System Safety within Laboratory Data Exchanges Report

September 25, 2023

Authors:
Prof. Nancy Leveson
Dr. John Thomas
Polly Harrington
Rodrigo Rose
Massachusetts Institute of Technology
Partnership for Systems Approaches to Safety and Security
https://mit.edu/psas

and

Dr. Stephen Powell
Alana Keller, PMP
Synensys, LLC
Contact: Dr. Stephen Powell
spowell@synensysglobal.com

DISCLAIMER

The opinions expressed in this report are those of the authors. They do not purport to reflect the opinions or views of the U.S. Food and Drug Administration (FDA), its affiliates, or the organizations included in the research. This report was completed under FDA Contract #75F40122C0012.

A System-Theoretic Process Analysis (STPA) of the U.S. Diagnostic Laboratory Data Ecosystem

Summary

Many studies have found large numbers of preventable medical errors in the U.S., despite significant efforts to reduce them. This project, a collaboration between Synensys and MIT, studied how the laboratory data ecosystem works today, identified weaknesses and sources of adverse events, and recommends changes to eliminate or reduce such events. We used System-Theoretic Process Analysis (STPA), a technique based on system theory that allows analysis and understanding of very complex, adaptive systems.

Using STPA we created a model of the healthcare laboratory data ecosystem by interviewing fifty stakeholder who represent components of the U.S. healthcare system. These components included departments across the U.S. Health and Human Services (FDA, CDC, National Library of Medicine, ONC, and CMS), standards development organizations, Health IT (HIT) vendors, regulators, public health agencies, clinical practitioners, device manufacturers, administrators, payors, accreditors, policymakers, patients, informaticists, and laboratorians.

The goal for the system model was to try to assist in understanding how the system works as a whole, that is, how the components work together to provide—or to not provide—needed diagnostic laboratory data. While we found that nobody seems to understand the entire U.S. laboratory data ecosystem in detail, we were able to combine the information elicited in the interviews to create a useful model to satisfy our analysis goals. We then used this model to identify the causal factors in common types of adverse events related to healthcare laboratory data. In this study, we concentrated on two hazards: (1) patients receiving less than acceptable care and (2) loss of reputation or trust in the laboratory data ecosystem.

Using the model, we identified unsafe actions and decision making in the system such as the healthcare provider ordering the wrong test, receiving incorrect test results, not receiving the test results at all, receiving test results after delays, or receiving test results for a different patient. Causal scenarios were then created for the identified unsafe events. We identified several hundred potential unsafe actions across the system and multiple causal scenarios/factors for each of those. The identified unsafe actions and scenarios were reviewed by participants in the system for their reasonableness and importance in the real-world operation of the system.

Based on our analysis of the system and the potential unsafe actions, we identified the following systemic flaws and propose recommendations to address them:

(1) Systemic factors and recommendations addressable by the SHIELD initiative

- *Decentralized and missing oversight*. The system is characterized by strong regulation in some parts of the system while the system as a whole is weakly regulated. There are very few regulations that address interactions between system components in a meaningful way. Gaps may arise partly because decentralization makes it unclear who has the ultimate jurisdiction over interactions. Each agency may have different goals and directives based on the responsibilities they were assigned by Congress or HHS leadership that limit what they can or cannot add to regulations.

  Another consequence of decentralized oversight is that regulatory agencies may not have access to the information they need to perform their regulatory duties. For example, an agency may need particular data elements to be shared in a certain format that is unobtainable if data requirements are not under their regulatory scope.

  In addition, financial incentives for adopting safer practices may differ among various groups. For example, there are no requirements for laboratory HIT to use more advanced standards like FHIR for communication with EHRs. The lack of requirements hinders adoption of new standards that might address problems arising from new and complex diagnostic tests being shared in unstructured formats.

  Furthermore, in some cases, information is not being collected about potential regulatory gaps, or no controller has any authority to ensure that a problem gets addressed. For example, there are insufficient mechanisms to ensure that providers adequately receive laboratory data, or to ensure that specimens collected outside of a laboratory are collected and transported appropriately. Insufficient studies are being conducted on identification of regulatory gaps in the ecosystem.

Recommendation 1: Assign responsibility for addressing gaps in the regulatory oversight of laboratory data exchanges between system components that are regulated by different agencies.

Recommendation 2: Identify the data and standards needs of regulatory agencies and ensure they have the ability to use them appropriately.

Recommendation 3: Encourage the identification of regulatory gaps in other areas of the laboratory ecosystem through additional systems-theory-based analyses.

- *Inadequacies and gaps in laboratory data standards, including standards that are loosely constrained, ambiguous, and outdated*. Laboratory data standards may not be tightly constrained because each implementer may possess their own set of requirements for each use of the standards and may thus want it to be implementable in different ways. Even if stakeholders' implementation goals are aligned, ambiguity in laboratory data standards may make different implementations still appear reasonable and fully compliant with regulation. The use of outdated or obsolete laboratory data standards may similarly raise challenges for patient safety and data interoperability.

  Recommendation 4: Reference libraries must develop a knowledge base that establishes a ground truth for naming, coding, and mapping of reference terminologies to particular laboratory tests, and stakeholders must be incentivized to use it.

  Recommendation 5: Appropriate groups must be assigned responsibility for identifying gaps and weaknesses in laboratory data standards and for establishing a reporting channel for problems related to them.

  Recommendation 6: SDOs must continuously support users by identifying and eliminating ambiguities in implementation guides for HIT standards.

(2) Systemic factors and recommendations addressable by the other components of the laboratory data ecosystem

- *Inaccurate perceptions of risks with respect to both laboratory data and the use of health information technology (HIT)*. A common theme observed in multiple scenarios is a flawed perception of risk in diagnostic healthcare. Many stakeholders in the ecosystem hold assumptions about the low safety-criticality of laboratory data and HIT that lead to flawed decision making across the system. An example is the effect on clinical decision making when there are data presentation problems or missing data: Errors are often blamed on the medical practitioners using HIT even if the software is counterintuitive or misleading.

  Causes of misperceived risk include beliefs that HIT is low risk in comparison with its potential benefits leading to less than rigorous oversight; limited proactive and reactive laboratory safety efforts, including investigating sources of diagnostic error; and a limited reporting system with no regulatory body keeping records on IVD (in vitro device) and lab errors. There also exist false assumptions about the ease of installing and maintaining HIT.

  One result of misperceived risk is that laboratory data and HIT problems are not prioritized when designing and implementing responses to adverse events. In general, misperceived risk is a common cause of accidents in all industries.

  Recommendation 7: Proactively and retroactively investigate systemic sources of diagnostic error.

  Recommendation 8: Create a consolidated national database for HIT safety reporting that can be used to identify trends and opportunities for improving patient safety outcomes. It should include information about HIT not behaving as users intended and allow understanding how features of HIT design may have contributed to "user errors."

- *Lack of a systems view by participants in the system*. Nearly all stakeholders in the U.S. healthcare system are trying to make locally optimal changes to reduce adverse events. However, without taking a systems' view, many changes made at the local level do not make the system significantly safer. Local or limited "fixes" may just shift the problem to a different part of the system or even make it worse. It may also cancel an improvement or change made by others.

After dozens of interviews, it became clear that no stakeholder holds a complete view of the entire ecosystem.

Recommendation 9: Educate the healthcare community on systems engineering and systemic approaches for solving problems, including tools to accomplish this goal.

One particular area in which customized "local solutions" were prevalent was in the design and maintenance of HIT systems and standards. Designing a new HIT or updating it without sufficient consideration of the system's connections to other systems can lead to broken connections. The difficulty of installing or maintaining HIT is often underestimated.

Recommendation 10: Establish appropriate control loops for updates to standards and HIT.

- *Inadequate regulatory emphasis on the safety involved in health system information technology*. Regulatory directives to the ONC have historically been driven by increasing the usage and capabilities of HIT without emphasizing safety. Designs that meet ONC certification requirements frequently have significant safety risks. Furthermore, no one is currently required to use certified HIT, as incentives for using certified IT are only available to facilities that are eligible for certain government programs.

  Recommendation 11: Assign regulatory oversight of HIT safety to ONC or another appropriate group. Include the explicit directive to develop and include safety-related certification criteria for HIT and the ability to limit the inclusion of "hold harmless" clauses in HIT contracts.

  Recommendation 12: Establish incentives for using certified HIT throughout the entire healthcare ecosystem.

- *Flawed communication and coordination*. A common causal factor identified is the lack of formal communication and coordination channels between those attempting to control diagnostic data safety. Many regulators do not have the information they need to change or update regulatory standards. Medical practitioners may also not be incentivized to report problems if previous reports have not been appropriately addressed. Following standards is often voluntary. While some requirements do exist to follow standards, they often refer to outdated standards without a strong process to change the standards to recognize best practices.

  Additionally, inadequate communication and coordination channels between data users may also contribute to patient harm. For example, medical practitioners are responsible for ordering tests to monitor and diagnose patients, but at the same time have a huge range of responsibilities and could benefit from better communication with laboratories. Laboratorians have up-to-date information on changes to the diagnostic testing environment, including new test options or how tests results should be interpreted. However, due to the way many interfaces are set up, laboratorians may not receive sufficient data to fully support practitioners. For example, a laboratory may not be able identify if a test result is critical and time-sensitive if they don't appropriately receive the patient's relevant clinical context.

  Recommendation 13: Develop formal processes for inclusion of laboratorians in the multidisciplinary teams responsible for decisions about laboratory data needs, representations, and interfaces at care facilities.

  See recommendations 5 and 8 as well.

Conclusions

Our goal in this study was not to focus on what individuals or even individual components of the system are doing wrong, but instead on why their actions make sense within the system as it exists today. Our recommendations are about how to change the overall system design to allow and encourage safe behavior by everyone. The causal scenarios for adverse events identified by STPA point clearly to actionable recommendations that can be linked to the related flaws in the system. A rationale for all the recommended changes to the system is provided by the links to the identified adverse event scenarios.

The problems we identified are not unknown within the healthcare community. What is not understood widely is how to get past the problems and effect changes to greatly increase healthcare safety. By formally analyzing the system and identifying why the problems are occurring, we were able to generate recommendations that have the potential to greatly decrease adverse events.

Perhaps the biggest takeaway from our effort and from the application of system theory is that the difficult problems in U.S. healthcare safety cannot be solved without applying a systems-theoretic approach: major improvements will require redesign of the system as a whole, not just small tweaks to parts of it. The problems are not so much in the individual system components, where everyone is trying to provide safe and effective care. The most serious and persistent problems are instead occurring in the interactions and interdependences between the system components. Only by redesigning the system to control these interactions will significant progress be made.

While the recommendations in this report represent large changes for the healthcare community, they are standard features in other industries that have highly successful safety records. For example, the U.S. has an incredibly safe aviation system, which is unparalleled compared to other types of transportation systems. One of the reasons is that aviation in the U.S. long ago instituted the systems approach to safety recommended for healthcare in this report.

Finally, changing the current system, as difficult as it will be, is not enough. There also needs to be action to control the foreseeable changes in the healthcare industry. One of these is the rapidly growing use of software and information technology. We can wait until the inevitable adverse events start to occur widely, or we can take action to ensure that new software and advanced automation is introduced from the beginning with acceptable controls over patient safety.

The types of structural changes recommended in this report may take some time to introduce into the U.S. healthcare system. In the meantime, near-term solutions will be required to provide adequate control over hazards. All the changes will require the participation of everyone in the healthcare community to ensure that the most effective controls are successfully created and used. Local optimization may in some cases have to be sacrificed for increases in overall healthcare safety, quality, and efficiency.

Table of Contents

A System-Theoretic Process Analysis (STPA) of the U.S. Diagnostic Laboratory Data Ecosystem

Abstract

This report presents the results of research conducted for the FDA by Synensys and researchers at MIT to investigate the causes of adverse events in the U.S. diagnostic laboratory data ecosystem. A relatively new approach to modeling and analyzing complex, adaptive systems was used to identify scenarios in the current laboratory system design that can lead to adverse events. The new approach is based on system theory and uses an analysis technique called System-Theoretic Process Analysis (STPA). The study identified many systemic flaws in the system design that can lead to adverse events. The causal factors identified were used to create recommendations for eliminating the causal factors and thus reducing adverse events.

1. The Problem and Research Goals

Preventable medical errors are now the third leading cause of death in the U.S. even though significant resources have been expended to improve patient safety [2]. Diagnostic errors account for 6-17% of all adverse patient events occurring in hospitals while at the same time resulting in most of the paid medical malpractice claims [3]. An estimated 800,000 Americans are seriously injured or die each year across multiple care settings due to misdiagnosis of dangerous diseases [4]. Another study of closed claim malpractice data found that 92% of diagnostic errors within the EHR occurred during laboratory testing [5].

During the recent COVID-19 pandemic, existing data deficiencies, including the lack of data interoperability, paralyzed the national pandemic response due to the inability to share data across public health agencies (State and Federal), health facilities, regulators, and laboratories. This inability to share and use real-world data hampered testing, prevention, regulation, resource management, and ultimately, led to preventable patient deaths. The U.S. was forced to use COVID response data from other countries to address testing efficacy, masking, virus characteristics, and treatment options.

To determine how to reduce diagnostic errors and increase safety, the FDA Center for Devices and Radiologic Health (CDRH) and the FDA Systemic Harmonization and Interoperability Enhancement for Laboratory Data (SHIELD) program office sponsored the research presented in this report. The goal was to conduct a system safety assessment across the laboratory data ecosystem in order to:

- understand how the system works today,
- identify weaknesses and sources of adverse events, and
- recommend changes to eliminate or reduce such events.

The research reported here was conducted by researchers at MIT (Prof. Nancy Leveson, Dr. John Thomas, Polly Harrington, and Rodrigo Lopes Rose) and Synensys (Dr. Stephen Powell and Alana Keller) over a period of a year, starting in September 2022. Interviews were conducted with 50 people from 9 groups within the laboratory data ecosystem in order to understand how the system works today. STPA (System Theoretic Process Analysis) [6] was used to model the results of the interviews and to analyze the model to identify scenarios that can lead to adverse events due to problems with laboratory data. Adverse events are defined here as any patient injury caused by medical care. STPA is a relatively new and powerful technique being used today to improve safety in some of the most complex, socio-technical systems [7].

This report presents the results of the research. The next section presents a short overview of the laboratory data ecosystem today followed by an introduction to system theory and the modeling and analysis method used to obtain the results.

Two basic categories of results are included: (1) specific scenarios that could lead to adverse events and (2) general systemic flaws in the overall laboratory system leading to adverse events. Section 4 presents final recommendations to improve the safety of the laboratory data system in the U.S.

Research planned for the next year includes expanding the boundary of the system to include point-of-care testing, over-the-counter test kits, and demonstration of a system-theoretic approach to the analysis of laboratory data adverse events called CAST (Causal Analysis based on System Theory).

2. Background

2.1 The Laboratory Data Ecosystem Today

The U.S. clinical laboratory data ecosystem is a highly complex network of people, organizations, processes, regulations, equipment, devices, policies, technology, and standards developed to collect, analyze, manage, report, and share test results. Laboratory test results are used to diagnose and treat patient conditions, manage public health responses during disease outbreaks such as COVID-19, support population health for chronic conditions such as diabetes, and conduct health research to improve patient outcomes. Additional laboratory ecosystem data is used for financial reimbursement, regulatory compliance, safety, efficacy, quality, privacy, and security.

Over 12 billion clinical laboratory tests are analyzed in the U.S. each year making laboratory tests the highest volume health service. Most laboratory testing performed on humans in the U.S. (except research) is regulated by the Centers for Medicare and Medicaid Services (CMS) through CLIA (Clinical Laboratory Improvement Amendments). CLIA covers about 320,000 laboratory entities. The objective of the CLIA program is to ensure quality laboratory testing. CMS is a division of the U.S. Health and Human Services (HHS) agency.

Most laboratory tests are ordered by medical providers using an electronic health record (EHR) that connects the order to a Laboratory Information System (LIS) via middleware or interface and ultimately to the test analyzer or in vitro diagnostic (IVD) device where the specimen is tested by a lab technician.

The test results are electronically returned to the LIS and the EHR using a variety of coded message standards. When a lab test is unavailable within a local hospital laboratory, the order will be transmitted to an outside or third-party laboratory. Point of care lab tests usually take place outside the hospital in an outpatient setting.

Additional laboratory ecosystem performance data is collected and shared with laboratory quality organizations such the College of American Pathologists (CAP) to assess ongoing laboratory testing proficiency against benchmark standards to support CLIA certification and quality assurance. The U.S. Food and Drug Administration (FDA) collects IVD device data as part of their post-market IVD surveillance to ensure devices are safe and effective. Laboratory test data is also reported to state and federal public health agencies such as the Centers for Disease Control and Prevention (CDC), disease registries, and health research agencies such as the National Institutes of Health (NIH) to enable tracking infectious diseases, guiding pandemic responses, supporting health equity, and developing medical innovations for better population health outcomes.

2.2 General Limitations and Problems in the Laboratory Data System

The current laboratory data ecosystem has many acknowledged drawbacks and limitations. As laboratory data is exchanged with outside organizations and aggregated with other data sources, laboratory data quality deficiencies and variation can cause preventable patient harm. In addition, slow policymaking creates health disparities, impedes research, and results in a lack of trust in the laboratory data ecosystem [8].

One of the major problems is interoperability. The system was designed for an individual patient undergoing laboratory tests within a single hospital or health system. Mobility of patients and the use of mobile data devices were not envisioned within the original system design [9]. The sharing of patient laboratory data or other electronic health information with other health facilities or public health agencies was considered to be secondary at the time.

As a result, HIT vendors and hospital customers created local (customized) HIT configurations that did not prioritize interoperability between non-affiliated systems or outside organizations. While standards development organizations (SDOs) have produced terminology, messaging, and naming standards aimed at increasing health data interoperability, implementation of these standards is mostly voluntary, incomplete, and difficult to maintain over time [10]. The naming and coding of laboratory tests is unique to each laboratory, requiring significant curation including complex mapping to minimize the loss of meaning when the data is exchanged with outside organizations.

Another set of problems arose because health policy and regulatory efforts of the laboratory data ecosystem prioritized health information digitization for primarily billing purposes over patient safety, data quality, and system interoperability. Laboratory test data is not standardized. For example, a positive result can be described as confirmed, detected, screen positive, and immunized. Other variation among common lab tests can include test names, test units, test ranges, and test codes leading to secondary data usability challenges and safety issues when data is transferred [11].

3. Research Method

Much of engineering involves building models of the system being created or studied and analyzing those models. When the system is a physical or natural system, the models often are composed of mathematical equations, primarily using differential calculus. The modeling and analysis of human or social systems, such as the diagnostic laboratory data system in this report, uses a very different type of engineering model and analysis method based on systems theory or systems thinking. The goal is to identify how the system could operate in a way that leads to adverse events. This information is then used to design or redesign the system to eliminate such events.

3.1 A Brief Introduction to Systems Theory

Systems theory can be traced back about 60 years ago to researchers studying biological systems [1], the designed aspects of social systems [12], and the relationship between man and machines [13]. The concepts in systems theory quickly spread to management [14], the social sciences, and system engineering. As one example, Margaret Mead is often credited with introducing systems theory in anthropology.

System engineers have learned that considering the aircraft or nuclear power plant as a whole or as an integrated system is necessary to ensure the safety of these systems. The same is true for any complex system, including healthcare.

Systems theory provides the scientific foundation for the study and design of complex systems, which have the following basic properties:

Goal-Oriented (Teleological)

Engineered (designed) systems, including social systems, are not just a set of connected components that interact with one another but have an *overall purpose or goal*.[1] The highest-level system purpose—providing healthcare, in this case—is achieved through the operation of the system as a whole. The overall system purpose or goal, in turn, is achieved through the operation of individual pieces of the system, each designed with a subgoal or purpose in mind that is part of the overall goal. A subgoal of the diagnostic lab subsystem is to provide accurate and timely laboratory test information for overall healthcare decisions in the larger healthcare system. The successful achievement of the subgoals is necessary to achieve the overall system purpose.

Interdependent and Interconnected

The world and the systems in it are interconnected and interdependent. Science and engineering have traditionally handled complexity by decomposing complex systems into components, analyzing the components separately for some property, and then combining the results. For example, problems in taking samples, data transfer between components, diagnostic problems within individual laboratories, and so on are solved in isolation from each other. An assumption is made that this combining process provides an accurate result for the system as a whole.

While useful to some extent, this focus on individual components of a complex system can lead to missing important problems that occur in the interactions among the components, such as the sharing of electronic data with other laboratories or healthcare facilities. The connections are usually not simple in a complex system because the components mutually interact with each other, with one impacting the behavior of the other(s). For example, a laboratory test order is initiated by a medical provider within an electronic health record (EHR), a uniquely coded message is sent to a laboratory information system (LIS) which in turn sends a uniquely coded message to an in vitro diagnostic (IVD) device where the test is performed by a lab technician. Once the test is complete, the lab results are returned to the LIS and EHR using a series of system interfaces and ultimately, to the provider, shared with the patient and sent to the billing system.

Interdependencies are common in the designed aspects of the healthcare system, which includes diagnostic data laboratory and healthcare facility operations and policies, diagnostic data formats, oversight by government agencies, policies and procedures, electronic health record systems, medical and diagnostic equipment, and so on. Interdependencies can lead to undesired effects when the design of one component is changed in isolation from the others. This phenomenon is called the *Law of Unintended Consequences*. As an example, changing data formats in one part of the system may have unintended consequences throughout the entire system.

[1] In contrast, *complexity theory*, created a few years after system theory, is most applicable to systems that do not necessarily have a purpose, such as weather.

Holistic

If we want to fix something or intentionally change the behavior of a complex system, we must first understand the system as a whole or we are very likely to not achieve our goals. In the worst case, we may increase the number or type of adverse events.

In addition, some system properties, such as safety, *emerge*, that is, are created, through the operation of the system as a whole. Diagnostic laboratory data safety emerges from the interaction and properties of multiple system components such as the way that samples are taken from patients, the mode of the transfer of required information to the laboratory facility and back, the calibration of instruments in the laboratory, the knowledge of laboratory workers, the consistent interpretation of data among the various groups involved, the implementation of accepted data standards, etc.

A common way of expressing this idea is by saying that the whole is greater than the sum of the parts, an idea that can be traced to Aristotle. For example, individual laboratory tests (i.e., serum glucose, hemoglobin AIC, oral glucose tolerance test) provide clinicians and patients with important information, but the combined results of a series of laboratory tests are required to diagnose diabetes. Laboratory data safety may depend on the way that diagnosis is performed in different laboratories, the expectations of those receiving the data, timing, adverse event reporting and handling, technological changes affecting different parts of the system, etc.

The concept of emergence means that properties of complex systems may "emerge" when the parts operate together that may not be visible when looking at the separate components in isolation. Understanding a system property such as safety requires looking at all the components as an integrated system, that is, as a whole.

Contextual

All behavior is affected by the context in which it occurs. We cannot understand, predict, or change the behavior of something without looking at the context in which that thing (or person) is operating. For example, the process of healthcare personnel taking a sample involves not only the ability of the individuals involved but also features of their environment such as the equipment available, patient compliance (i.e., "needle-phobia"), distractions, time stresses, etc. Leveson has suggested that human error is a symptom of a system design that needs to be changed [15].

Human behavior is not only driven by the context in which it occurs, but also indirectly by our mental models of that context. Our mental models impose a structure that allows us to deal with a "messy" world. For example, physicians believe that the data they receive has been processed in specific ways and will act on that belief. Perception is also affected by expectation, that is, we often interpret what we see through the lens of what we expect to see. If we expect to see the results from a diagnostic lab expressed in micrograms, we might not notice that the units reported differ from what we expected, even if the units used are noted somewhere on the lab results report.

Dynamically Complex and Adaptive

In dynamically complex systems, such as healthcare, cause and effect are not related in a simple way. Understanding and changing such systems is challenging as they are continually changing and adapting to the current conditions, both within the system and in its environment. As an example, a payor may try to reduce the number of potentially dangerous incidents of a particular type by creating financial incentives for hospitals having a low number of them. Hospital administrators may in turn create incentives for employees to reduce those types of incidents. The result may not be what the payors expected: Instead of reducing the incidents, the incentives may lead only to reduced reporting of them. As a result, adverse events may not decrease and may even increase. Or the attempts to reduce that particular type of incident may lead to increases in other types of incidents, perhaps leading to even worse adverse events. In general, attempts to reduce adverse events may not have the intended result because the system reacts and adapts in unexpected ways.

Constraints can be imposed in system design and operation to control the dynamics that prevent the system goals from being achieved but they are not simple to devise.

Non-Linear

Causality is sometimes simplified to assist in understanding and preventing adverse events. The most common simplification is to assume causality is linear. Linear causality means that each event is the cause of an event that directly preceded it. A common analogy used to understand linear causality is to think of adverse events as holes in Swiss cheese, with the holes lining up in a linear fashion to lead to the actual adverse event.

While this model can be imposed on any set of events preceding an adverse event, it omits important information such as the reasons *why* the events occurred—which are usually much more complicated than just the existence of a single preceding event. Looking only at the events leading to the final loss (i.e., the holes in the Swiss cheese and

the failure of protection systems) does not provide enough information to prevent large categories of adverse events most effectively.

In addition, in systems theory causality can be circular. Doing something successfully, that is, without an adverse event occurring, leads to complacency and an assumption that the process is and will always be safe. Doing A leads to success which leads to doing 'A' the same way again and again, reinforcing the appearance of the safety of doing A. This circular loop may continue until some feature of or change in the system or its environment is encountered where A leads to an adverse event. Another example of circular causality is the one mentioned above where financial incentives to reduce incidents and therefore adverse events lead to the same number of incidents or maybe an increased number.

To deal effectively with complex systems, our understanding of causality has to use models that include non-linear (non-sequential) behavior and identification of why the events occurred. Non-linear causality may include feedback and other types of communication between components and events. In general, goal-seeking behavior includes feedback and monitoring of information about the state of the system and the components in it. An example is provided in the next section.

3.2 The System-Theoretic Approach used in this Research

Engineers analyze a system for a particular property, such as safety, by building models and analyzing the models for the properties of interest. We use a model in this research that includes the properties of complex systems described in the previous section [7].

A Basic Feedback-Control Model

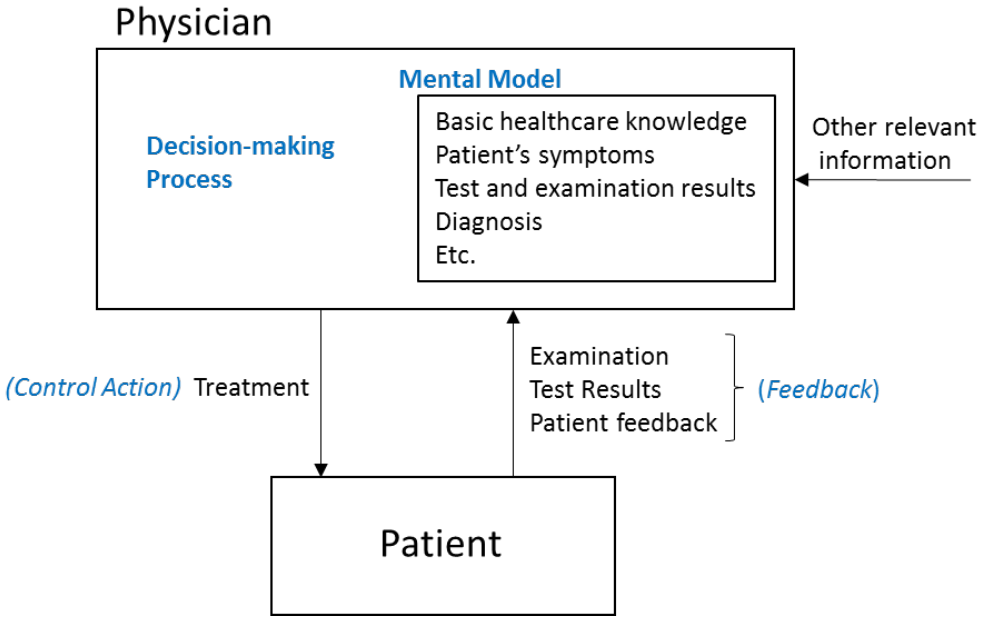

Figure 1. A basic Engineering Feedback Control Loop

Consider the model in Figure 1. In this model, the physician is treating a patient (shown by the downward arrow from the physician to the patient).

To decide about what treatment to prescribe, physicians use information in their mental models of the situation, such as basic healthcare knowledge, the patient's reported symptoms, diagnostic test and examination results, and the physician's current diagnosis (which may stem from the other information in the physician's mental model).

After treating the patient, the physician gets *feedback* about the effect of the treatment through perhaps an examination, test results, patient feedback about current symptoms after the treatment, etc. The physician then decides whether further treatment is necessary and, if so, what that might entail. This general type of model is called a *feedback-control loop*, where the downward arrow are the controls provided by the controller (in this case a physician) on the patient's health which is labeled "treatment" here. In more general terms, the label on the downward arrow is called a *control action*.

The physician may get additional information to be used in decision making about control actions from sources other than the patient, such as an EHR, consultation from other physicians, information about the current environment such as the existence of an epidemic, and so on.

Direct feedback and any additional information from other sources are used to update the physician's mental model. The current mental model is used in the decision-making process to identify a necessary control action.

In general, the controlled process may be a physical object such as IVD equipment, as well as processes that adapt and change over time. Note that the model is an adaptive model as the physician's behavior will change over time as well, in the simple case it will change as the physician learns from the response of this particular patient but in general by learning from overall experience and new information. Note that learning does not always imply improvement. For many reasons, learning may involve worse behavior or maladaptation.

The inclusion of adaptation and learning over time is an important difference between a systems approach and more simple conceptions using linear causality. Of course, the events resulting from the control loop process can be strung out on a timeline. The events are linear because time is linear. But the causality of the events may be circular or reflect complex causal relationships. Modeling causality as linear has limited use for complex systems.

Instead, in systems-theoretic modeling and analysis, the *process* of how the events are generated—*why* they occur—is the cause of the events on the timeline. Causality is thus a process rather than a chain of failure events. A new model of accident causality, called STAMP, is based on these concepts [7].[2] The analysis method to learn from (analyze) the models is called STPA (System-Theoretic Process Analysis) [6]. STPA is described later in the next section of this report.

Creating More Complex Models

The model in Figure 1 is too simple to provide much understanding of how the system works and what is involved when adverse events occur. Instead, more components put together into a *hierarchical control structure* are needed. Figure 2 shows an example with more system components included.

In Figure 2, a diagnostic lab is included along with administrative controls on physician behavior in a healthcare facility. Again, the model is too limited to handle many important causes related to adverse events in the diagnostic data arena. Where the boundaries are set for the model will affect the types of information that can be obtained by the model. In general, those creating and analyzing the model must decide where the boundaries of the model will be set and thus the extent of the information they want to obtain from the model.

[2] Another modeling language claimed to be based on systems theory is called FRAM. It was not used for this research because it is not a systems-theoretic model: Instead, it is a model of the linear sequence of events over time, like a flow chart. FRAM itself shows some aspects of control *flow* between the events (on a line called a control line) but there are no control loops (that is, no feedback control) and there are no mental models or decision-making processes described or used in an analysis of the model. Control flow models have been used for several decades in computer science for specifying the behavior of software, but do not allow identifying emergent behavior and analyzing the safety of a complex system like the U.S. laboratory data system.

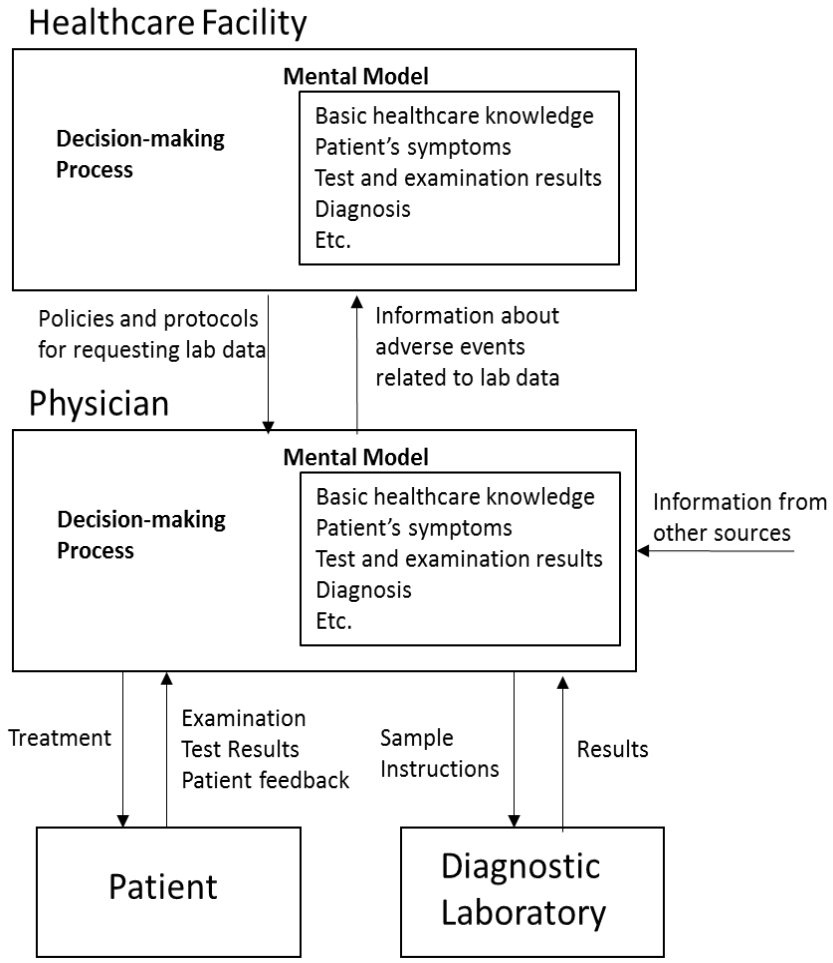

Figure 2. A model of the system more inclusive of laboratory data

3.3 The Process for Analyzing the Model: STPA

STPA is a technique used to analyze these control models. It has four steps:

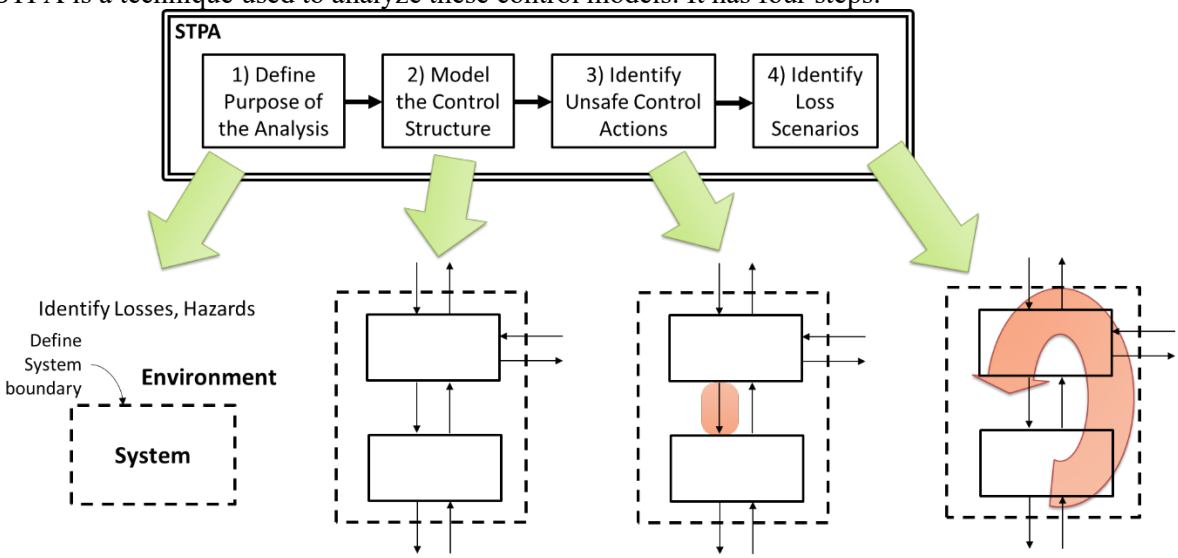

Figure 3. The four steps in STPA

First, the basic purpose of the analysis and the boundary of the system being analyzed are determined. Next, a control structure model of the system is created. In the third step, Unsafe Control Actions (UCAs) are identified by determining how each control action that is available to a controller in the system may become unsafe if performed under certain contexts. Finally, the fourth step identifies situations in which these UCAs resulting in hazards or adverse events can occur, called the *loss scenarios*. These loss scenarios can be used to determine how to redesign the system as a whole to eliminate them from the design or to minimize their impact if elimination is not feasible. Each step may cause the researchers to go back and add more to previous stages as the process continues. Results remain traceable through all four levels of analysis.

To create the models used in this research, interviews were conducted with 50 key stakeholders across the system. Interviewees or "key informants" were from regulatory agencies, medical practitioners, laboratory technicians, standard developers, payors, HIT professionals, health informaticists, and beyond. A list of key informants is included in Appendix A.

The laboratory data system in the United States is highly sociotechnical. Therefore, the interdisciplinary range of experts on the interview team was critical for the project's success. The interview team included STPA experts, informaticists, patient safety professionals, and other healthcare subject matter experts.

The STPA process in this research started with discussions with project stakeholders to identify the losses and hazards important to the project. Interviews then began to develop the control structure. Initially, the control structure modeling mapped the relationship between the FDA and IVD manufacturers. However, as we interviewed new stakeholders, our view of the system quickly expanded. It became quite clear that the laboratory data ecosystem was impacted by a broad range of controllers, and we had to expand the boundary of our model

Interviews revealed an ecosystem consisting of patients that undergo testing, practitioners who order and conduct the tests, data consumers who use the data for clinical decision-making and reimbursement, secondary users including data registries, public health agencies, regulators, accreditors, payors as well as information technology vendors, data standards professionals, and IT system support-personnel. Each interview was used to expand understanding of the system and to correct errors where needed. Each change to the control structure was informed by subsequent interviews in addition to literature analyses. As the process continued, a model that captured the critical relationships between controllers and that was generally agreed upon emerged.

With the losses, hazards, and control structure established, the research team began creating the list of unsafe control actions (UCAs). This stage of the project was meant to identify in what specific contexts the control actions available to each controller may become unsafe and lead to losses and hazards. Subsequent interviews were used both to identify new UCAs and to refine or edit already uncovered UCAs .

Finally, scenarios were generated from the list of UCAs. First, concrete examples of unsafe events (i.e., real accidents/incidents) from our interview recordings and literature were gathered. Then ways that UCAs could plausibly occur based on credible information were identified. Each scenario was constructed from discussions with the subject matter expert interviewees, as well as review of relevant literature. After being generated, scenarios were

validated by the subject matter experts. Some were augmented with real-world examples uncovered through parallel efforts of the SHIELD team.

The steps are explained further in the next section of this report, which presents the results of the laboratory data system research performed for this contract.

4. Research Results

This section presents the results of the analysis of the laboratory data ecosystem using the four steps of STPA described above.

4.1 Losses and Hazards

The first step of STPA involves defining the purpose of the analysis, which is done by identifying the losses and hazards of interest to the stakeholders of the system. The laboratory data ecosystem has a wide range of stakeholders including patients, providers, payors, and regulators, among others. Anything of value to any of these stakeholders may be treated as a loss in STPA. Preventing or mitigating losses is the ultimate goal of the recommendations generated in STPA. For practical reasons, this study is limited to two main losses:

L-1: Loss of life or injury to patient
L-2: Loss of reputation or trust in the laboratory data ecosystem

To explain how either of these losses may occur, the STPA analyst also generates a set of hazards, which are system states or sequences of actions that, together with a particular set of worst-case conditions, will lead to the loss. For example, one of the hazards related to L-1 might be that a patient receives less than the acceptable standard of care. That might not always lead to the patient being injured or losing their life, but in a worst-case environment (e.g., the patient has a particular pre-condition or allergy), it might. A complete list of the hazards identified, along with the losses they trace to, is shown in Table 1.

Table 1. Losses and Hazards for the Laboratory Data Ecosystem

Losses	Hazards
L-1: Loss of life or injury to patient	**H-1:** Patients receive less than acceptable standard of care (Associated with Loss-1)
L-2: Loss of reputation or trust in the laboratory ecosystem	**H-2:** Laboratory ecosystem stakeholders including patients (public) lose trust in the laboratory data being collected, shared, analyzed, and reported (Associated with Loss-2)

Several additional losses could be considered for the analysis, including financial losses or efficiency losses. Additional hazards related to L-1 and L-2 could also be considered. However, a deeper exploration of losses and hazards beyond those identified in Table 1 (such as a person being exposed to harm during the testing process or the specimen collection process itself) is outside the scope of this work and may be considered in future studies. The rest of the STPA results presented in sections 4.2, 4.3, and 4.4 are guided and prioritized based on the losses L-1 and L-2, and hazards H-1 through H-3.

4.2 Boundary of the System Considered

For practical considerations, the boundary of the system considered in the research, while extensive, needed to be limited simply to ensure finishing the work within the time constraints of the research contract period of performance. We included laboratory operations within hospitals, health systems, public health laboratories, specialty laboratories, and reference laboratories for specialized laboratory tests.

Laboratory data in these settings are initially generated from the in vitro diagnostic (IVD) device used for the test, the test result data is transferred to a laboratory information system (LIS) and then to an electronic health record (EHR) for clinical decision-making. The test results are sent to a portal for patient viewing. Laboratory test results that must be sent to outside organizations (public health agencies, health registries, non-affiliated health systems, payors, etc.) use health information exchanges (HIEs). All of these are included in our study. Other aspects of the system are also included but given less priority.

At this time, we have excluded laboratory data from point-of-care (POC) lab testing and over-the-counter (OTC) test kits in our research. Expansion of the analysis is planned for the next phase of this research study.

4.3 Modeling the Control Structure

Two models of the laboratory data system in the United States were generated. The first model, shown in Figure 4, uses a high level of abstraction in order to identify systemic factors leading to adverse events. The second model,

shown in Figure 5 uses a lower level of abstraction, which expands upon Figure 4. The more detailed model highlights the specific interactions that occur between components of the diagnostic data ecosystem in order to capture more nuances and identify places where responsibilities and control overlap. However, no model captures everything. The second model, while detailed, is not a complete representation of the system; it only explicitly includes the interactions that are relevant for the defined scope of the analysis.

Complete descriptions of all controllers listed in Figure 4 and Figure 5 are located in Appendix B. Table 2 below contains descriptions and clarifications regarding certain terms used in the control structure.

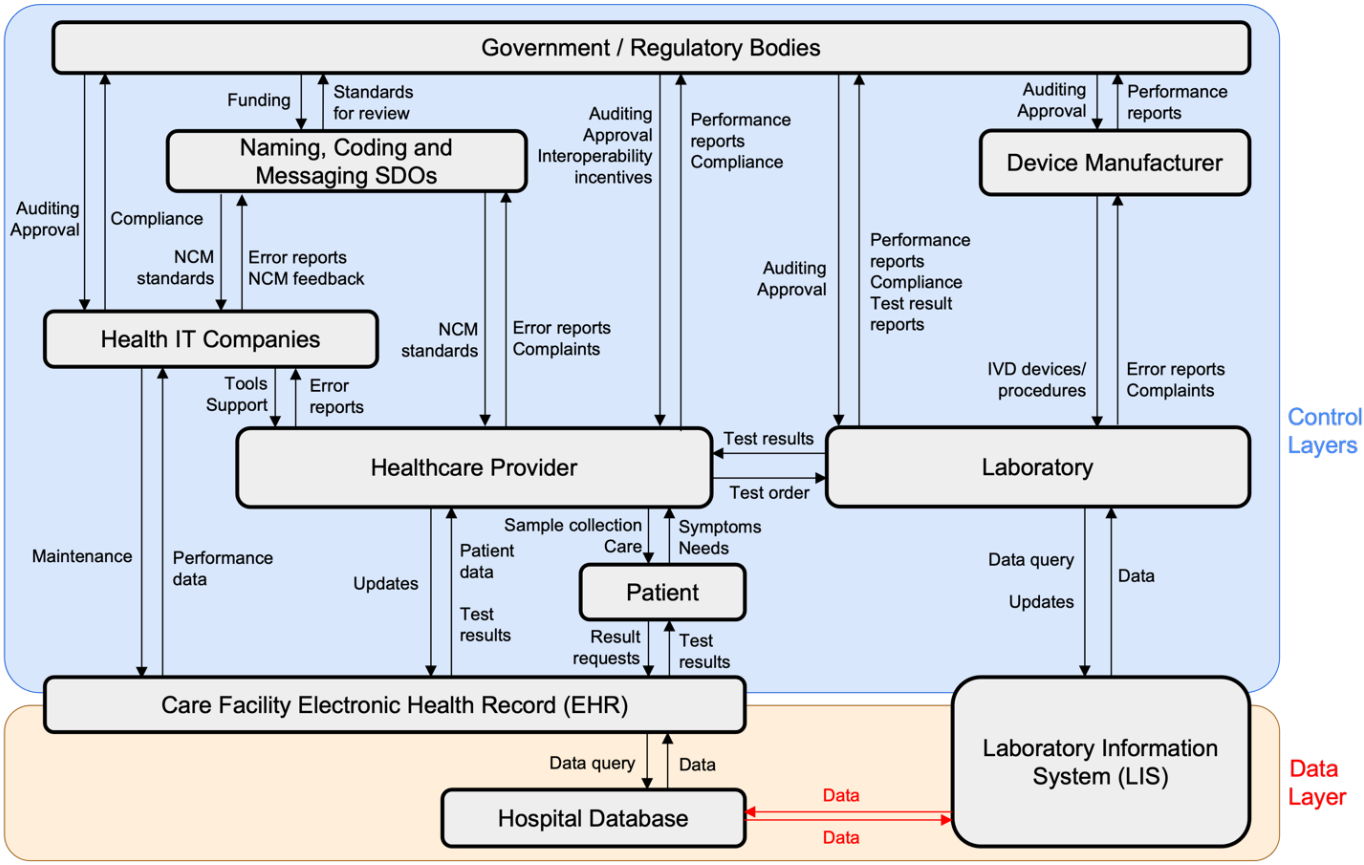

Figure 4. Abstract control structure for diagnostic laboratory ecosystem

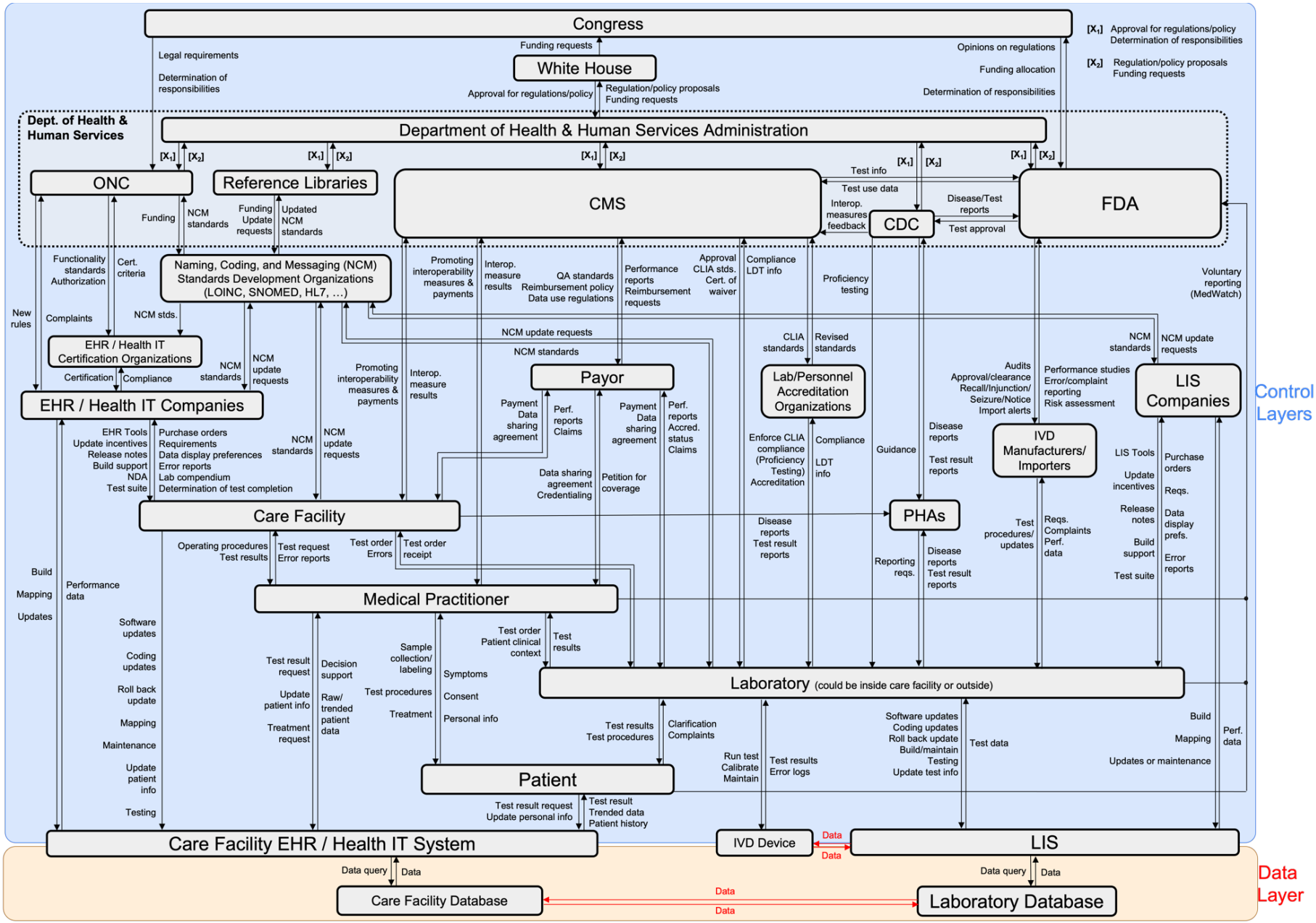

Figure 5. Detailed control structure for diagnostic laboratory data ecosystem

Table 2. Table. Clarifications on Key Terms Used in Figures 4 and 5

Term	Explanation
Medical Practitioner	The professionals (e.g., clinicians or nurses) who interact directly with patients in the form of consultations, ordering and interpreting diagnostic tests, collecting test samples, and providing treatment/care.
Care Facility	The institutions (e.g., hospitals or clinics) where patients go to receive medical care. Most of the interactions with care facilities modeled in the control structure involve the facilities' administrations or IT departments.
Laboratory/ Personnel Accreditation Organizations	Independent organizations that act on behalf of government agencies to provide certification and accreditation to different components of the laboratory data ecosystem. Examples include the College of American Pathologists (CAP), American Society for Clinical Pathology (ASCP), among others.
Naming, Coding and Messaging (NCM) Standards Development Organizations (SDOs)	Organizations that develop, release and update reference terminologies such as Logical Observation Identifiers Names and Codes (LOINC) and Systemized Nomenclature of Medicine – Clinical Terms (SNOMED CT), as well as messaging standards such Health Level 7 (HL7).
Reference Libraries	Agencies like the National Library of Medicine (NLM) or the National Cancer Institute (NCI), both under the National Institutes of Health (NIH), who curate and release compendia of healthcare terminology like the United Medical Language System (UMLS).
Department of Health and Human Services (HHS) Administration	The leadership structure within HHS determines, assigns, and enforces the responsibilities of the different operating divisions and offices within the department.
HIT Certification Organizations	Independent organizations that act on behalf of the Office of the National Coordinator for Health Information Technology (ONC) to provide certification of HIT systems. Officially known as ONC Authorized Certification Bodies (ONC-ACBs).
PHAs	Public health agencies at the state or county level

An important abstraction that appears in both models is the distinction between the data layer (represented at the bottom of the models in red) and the control layers (represented at the top of the models in blue). The data layer includes the physical devices and infrastructure used to send, transmit, and receive laboratory data. This includes IVD devices, which exchange test order and test result data with laboratory information systems (LISs), as well as electronic health record (EHR) systems managed by hospitals or clinics. When applying STPA to the laboratory data ecosystem, the data layer and the patient are the controlled processes.

The safety of the system emerges from interactions between the controllers in the layers above the data that use, share, and regulate it. For example, a potential loss scenario may occur because a test result transmitted from an LIS to an EHR in the data layer might be incomplete, which may result in a medical practitioner making an unsafe treatment decision. The data may, in turn, be incomplete because of configuration decisions made by various controllers, such as the care facility that manages the EHR system, the laboratory that manages the LIS, the vendors that implement these systems, or the regulatory authorities that oversee them. These types of loss scenarios are the

output from the STPA process. To emphasize the emergence of unsafe behavior from the control layer, the data and control layers are distinguished in both versions of the models.

In addition, the configuration of the laboratory data ecosystem is not static nor is it consistent across the entire country. For example, larger care facilities may possess their own laboratories, while smaller hospitals and clinics rely on external laboratories. Even in laboratories belonging to large care facilities, the LIS may be a module of their EHR system, or it may be a separate piece of software provided by a different vendor. Representing every possible configuration while maintaining the readability and usefulness of the models would be impossible, so Figure 4 and Figure 5 depict the most common configuration of the system and the one in which interoperability poses the greatest challenge. In the configuration selected, the laboratory and the care facility are different organizations and the laboratory's LIS was developed by a different vendor than the facility's EHR.

4.4 Identifying Controller Behaviors That May Lead to Adverse Events

The next step of STPA is to examine the control actions available to the controllers to determine the contexts in which those control actions could be unsafe. A control action becomes an *unsafe control action* (UCA) when it is used in a context that can lead to a hazard. For example, providing treatment to a patient may be unsafe if the patient does not need that treatment (the context). A complete list of all UCAs developed during this step is included in Appendix C.

Each UCA consists of four components: the controller performing the action, the control action itself, the type of UCA, and the context in which the action can be unsafe. Figure 6 shows a simple control loop between a medical practitioner and a patient, with four generic UCAs that may be derived from it. The example where the medical practitioner provides treatment that the patient does not need is highlighted in yellow. UCAs do not include the contributing factors that may have led to the UCA. The contributing factors are instead identified in the next step of STPA: causal scenario generation. For example, why might the medical practitioner provide treatment that the patient does not need? These causal scenarios are then used to identify the changes in the system design that can eliminate or mitigate the loss scenarios.

UCA Structure: <Controller> **<UCA Type>** <Control Action> *<Context>*

4 UCA Types	UCA
Not Provide	*UCA-1*: **Medical practitioner does not provide treatment** ***when the patient needs treatment***
Provide	*UCA-2*: **Medical practitioner provides treatment** ***when the patient does not need treatment***
Early / Late / Wrong Order	*UCA-3*: **Medical practitioner provides treatment too late** ***to address the patient's condition***
Apply too long / stop too short	*UCA-4*: **Medical practitioner stops providing treatment too soon** ***to address the patient's condition***

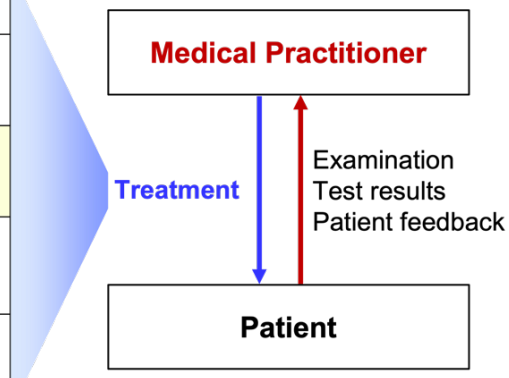

Figure 6. Example UCA for the medical practitioner

For each controller and identified control action, the 4 UCA types were analyzed to identify the contexts in which the control actions became unsafe.

Several hundred UCAs were identified across the system. All are included in Appendix C. Table 3 lists the 42 UCAs that provided the widest range of analytical results in the form of scenarios. In this study, it was found that many of the UCAs identified in step 3 of STPA share contributing factors and originate from the same (or very similar) scenarios identified in step 4. For instance, a medical practitioner might provide excessive treatment that a patient does not need for many of the same reasons that they might provide incorrect treatment for that patient. A detailed discussion of all UCAs is not included to limit the size of this report. The most important and representative ones are shown, however.

The 42 UCAs listed in Table 3 were selected based on those leading to the most distinct, unique, and helpful scenarios. These UCAs either came up frequently or were otherwise emphasized as important or urgent during a broad number of key informant interviews. UCAs that generated scenarios or recommendations that were already generated by other UCAs were excluded to reduce redundancy. The sharing of causal factors across multiple UCAs means that analysis of one UCA can generate recommendations that preclude or mitigate the risk of several others.

Each UCA is traceable to one or both of the hazards identified in Table 1. Some UCAs, like the example of the medical practitioner providing excessive treatment, are directly traceable to the hazard of a patient receiving less than the acceptable standard of care. Other UCAs, like a care facility not updating their EHR system, are further removed from the patient but are still traceable to the same hazard. Though the point of care is where patient harm primarily takes place, decisions made at the point of care are the result of unsafe decisions made throughout the system.

Note that neither this list nor the complete list available in Appendix C can be considered an exhaustive set of unsafe actions that may lead to the aforementioned hazards. Additional analysis within and beyond the scope of this work is required to generate a more exhaustive list. However, the ones shown do provide insight into the most important design problems in the laboratory data ecosystem.

Table 3. Consolidated List of Unsafe Control Actions

ID	Controller	Control Action	UCA	Hazard
1	Medical Practitioner	Provide treatment to patient	Medical practitioner provides treatment that does not match the patient's condition	H-1
2	Medical Practitioner	Provide treatment to patient	Medical practitioner provides treatment too late to avoid patient harm	H-1
3	Medical Practitioner	Order laboratory test	Medical practitioner orders laboratory test that is not the best/most appropriate test to diagnose a disorder/disease	H-1
4	Medical Practitioner	Order laboratory test	Medical practitioner orders laboratory test for patient that is not covered by patient's health insurance	H-1
5	Medical Practitioner	Order laboratory test	Medical practitioner orders laboratory test for patient that has already been done	H-1
6	Laboratory/ Care Facility	Update HIT system	Laboratory/care facility does not update HIT system when safety-critical HIT system update is released	H-1
7	Laboratory/ Care Facility	Update HIT system	Laboratory/care facility updates HIT system to version that is incompatible with other systems	H-1
8	Laboratory/ Care Facility	Update reference terminology in HIT system	Laboratory/care facility does not update reference terminology in HIT system when safety-critical reference terminology update is released	H-1
9	Laboratory/ Care Facility	Map local codes to reference terminology	Laboratory/care facility does not map local codes to reference terminology when safety-critical reference terminology update is released	H-1
10	Laboratory/ Care Facility	Map local codes to reference terminology	Laboratory/care facility maps local codes to reference terminology incorrectly/inconsistently	H-1

Table 3. Consolidated List of Unsafe Control Actions (continued)

ID	Controller	Control Action	UCA	Hazard
11	Laboratory/ Care Facility	Enable software feature in HIT system	Laboratory/care facility does not enable safety-critical software feature in HIT system	H-1
12	Care facility	Acquire an EHR system	Care facility does not acquire an EHR system when patient data needs to be shared electronically from other facilities or laboratories	H-1
13	HIT Company	Release HIT system update	HIT company does not release HIT system update following safety-critical reports from customers	H-1
14	HIT Company	Release HIT system update	HIT company releases HIT system update that has been insufficiently tested	H-1
15	HIT Company	Roll back HIT system update	HIT company rolls back HIT system update with safety-critical flaws too late after update is released	H-1
16	HIT Company	Provide build support and maintenance for HIT customers	HIT company does not provide build support or maintenance when customer does not have the resources to build or maintain HIT system	H-1
17	HIT Company	Select data standards to implement in HIT system	HIT company selects data standard that is not compatible with data standards used in HIT systems from competitors	H-1
18	CMS	Change requirements for "Promoting Interoperability" participants to avoid a negative payment adjustment	CMS changes requirements for "Promoting Interoperability" participants in a way that negatively impacts safety outcomes for program participants	H-1
19	CMS	Provide hardship exception for "Promoting Interoperability" program participant	CMS provides a hardship exception to a requirement that allows hospitals to operate EHRs with known safety risks [99].	H-1
20	CMS	Provide negative payment adjustment to care facility	CMS does not provide negative payment adjustment to care facility that did not meet funding requirements and is using systems that do not meet minimum safety requirements	H-1

Table 3. Consolidated List of Unsafe Control Actions (continued)

ID	Controller	Control Action	UCA	Hazard
21	ONC	Adopt technical standards in HIT certification criteria	ONC adopts technical standards in HIT certification criteria that are insufficient to create interoperable HIT systems	H-1
22	ONC	Adopt technical standards in HIT certification criteria	ONC adopts technical standards in HIT certification criteria too late after HIT systems are already deployed	H-1
23	ONC	Certify EHR as meeting current certification requirements	ONC certifies EHR that does not meet current certification requirements.	H-1, H-2
24	FDA	Approve IVD device	FDA approves an IVD device that does not perform to expected performance levels	H-1, H-2
25	FDA	Issue corrective action to IVD manufacturer	FDA issues corrective action to IVD manufacturer too late following a series of inappropriate results from IVD device	H-1
26	IVD Manufacturer	Associate IVD device output to reference terminology codes	IVD manufacturer does not associate device output to reference terminology codes when device output needs to be shared with external facilities	H-1
27	Payor	Provide coverage/reimbursement for laboratory test	Payor does not provide coverage/reimbursement for a laboratory test that may provide value to an individual patient's case	H-1
28	Payor	Provide additional preventative healthcare/well-being services to patients	Payor stops providing additional preventative healthcare/well-being services that patients are actively utilizing	H-1
29	NCM SDOs and Ref. Libraries	Create/release new reference terminology	SDO creates/releases new reference terminology too late after a new type of diagnostic test is developed or disease/condition is identified	H-1
30	NCM SDOs and Ref. Libraries	Create/release new reference terminology	SDO creates/releases reference terminology or messaging standard that does not sufficiently standardize communication between users	H-1
31	NCM SDOs and Ref. Libraries	Provide reference terminology mapping guidelines	SDO provides conflicting or ambiguous reference terminology mapping guidelines following safety-critical terminology release	H-1, H-2

Table 3. Consolidated List of Unsafe Control Actions (continued)

ID	Controller	Control Action	UCA	Hazard
32	NCM SDOs and Ref. Libraries	Provide messaging standard implementation guides	SDO provides conflicting or ambiguous implementation guides following safety-critical messaging standards update	H-1, H-2
33	Patient	Follow laboratory pre-test instructions or test procedures	Patient does not follow laboratory pre-test instructions or test procedures when procedures are necessary for validity of test results (e.g., does not fast, etc.)	H-1
34	Patient	Make/attend laboratory appointment	Patient does not make/attend lab appointment when lab results are necessary to inform care plan	H-1
35	CDC/PHAs	Set standards for reporting of diagnostic data from laboratories	CDC/PHAs set standards for reporting of diagnostic data that laboratories are unable to comply with	H-1
36	CDC/PHAs	Provide healthcare guidance	CDC/PHAs provide healthcare guidance that conflicts with current/previous guidance	H-1, H-2
37	Laboratory/ Personnel Accreditation Organizations	Provide accreditation to laboratory	Laboratory accreditation organization provides accreditation to laboratory without being able to enforce minimum interoperability requirements	H-1
38	HHS Administration	Determine responsibilities of component agencies	HHS does not assign any agency responsibility over safety-critical component of laboratory data ecosystem	H-1, H-2
39	HHS Administration	Determine responsibilities of component agencies	HHS assigns agencies overlapping responsibilities	H-1, H-2
40	Congress/ White House	Update Federal regulatory authority's statutory boundary	Congress/White House updates a Federal regulatory authority's statutory boundary in a way that removes components that were critical for safe control loop design	H-1, H-2
41	Congress/ White House	Expand Federal regulatory authorities' statutory boundaries	Congress/White House do not expand federal regulatory agencies' statutory boundary to cover technologies that have emerged or undergone significant changes since previous statutory boundaries were enacted	H-1, H-2
42	Congress/ White House	Expand Federal regulatory authority's statutory boundaries	Congress/White House expand regulatory authority's statutory boundaries in a way that diminishes the safety of the regulated industry	H-1, H-2

4.5 Causal Scenarios and Analysis

From the 42 UCAs listed in section 4.2, we generated approximately 200 causal scenarios. Scenarios describe the causal factors that can lead to the UCAs and to hazards. Assigning blame is not the goal of STPA. Instead, the goal is to understand why a controller might reasonably choose an action that was not safe. Frequently in complex systems, even when nobody is purposely trying to cause harm, well-trained individuals make decisions that are later identified to have been unsafe. For example, medical practitioners who receive an incorrect laboratory report and assume that they have received correct information may make an unsafe treatment decision.

Rather than trying to identify individuals who are doing the wrong thing, this approach instead tries to understand why people trying to do the right thing (which is the vast majority of people in the system) might be influenced by the design of the system in which they are working and do something that is unsafe. Using this framework, it becomes possible to identify ways to change the overall system that will increase safety and minimize hazards without blaming or punishing individuals trying their best while working in an imperfect system.

A complete list of generated scenarios is available in Appendix D. Similar to the list of UCAs, this list includes causal scenarios from the broader diagnostic healthcare ecosystem that were discovered during the interview process, even if they do not reflect problems specific to laboratory data quality and interoperability. Though these scenarios are outside the scope of this work and are not discussed in detail, they are included in the list for completeness. They may be used in further studies to improve the safety of the system even further.

To aid with scoping and clarity, the causal scenarios have been subdivided into three categories, denoted A, B, and C, based on how closely related they are to the direct scope of this study. These categories are outlined in Table 4 below.

Table 4. Scenario Categorization Scheme

Category	Description
A	In scope, directly related to issues of laboratory data, high explanatory power, worth a deep dive
B	Generally in scope, contain data-related contributions but are primarily driven by out-of-scope elements, data-related components likely addressed in recommendations for mitigating A-level scenarios
C	Out of research scope, do not contain data-related contributions, but worth a mention for research completeness

A-level scenarios are directly related to problems in laboratory data. Furthermore, A-level scenarios have high explanatory power with respect to uncovering and describing the systemic flaws that lead to the UCAs. Although these scenarios involve the data layer shown at the bottom of the control structures in Figures 4 and 5, the systemic factors in the scenarios stem from interactions between the controllers that oversee the data layer. For example, problems regarding medical practitioners not receiving test results due to inappropriate mapping of reference terminologies in LIS and EHR systems would be a component of an A-level scenario.

B-level scenarios contain data-related contributions and are thus generally within the scope of this study but are primarily driven by out-of-scope elements. An example scenario at the B-level could include a patient sample not being collected or stored appropriately because additional requirements were not communicated to the collecting nurse as part of a test order. Addressing the systemic factors that influence A-level scenarios is likely to address the data-related components of B-level scenarios as well.

C-level scenarios do not contain data-related contributions but were mentioned and emphasized by the subject matter expert interviewees and are worth including in the list of scenarios for completeness. An example at the C level might include a test result being skewed by a patient not having fasted before a test.

The following section of this report presents three example A-level scenarios from different controllers at different hierarchical levels of the control structure. These three scenarios were selected because of their high explanatory power, and because they highlight the kind of analysis that was performed for the other scenarios seen in Appendix D. Additionally, the systemic recommendations generated from these scenarios may preclude or mitigate not only them, but several other scenarios as well. Alongside some A-level scenarios is a visualization that traces the path of the scenario through the control structure and highlights the contributions of several controllers.

4.5.1 Scenario 1-14

Table 5. Scenario 1-14

Category	Scenario Information
Related UCA	**UCA 1-14:** Medical practitioner provides treatment that does not match the patient's condition
Controllers involved	• Medical practitioner • Laboratory • Care facility • SDOs • CMS • ONC
Scenario	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the EHR aggregated (e.g., placed in the same field) noncomparable test results that were derived using different methodologies that have not been harmonized to give comparable results. That may occur if two different tests that use the same or similar approaches for different conditions are mapped to the same reference terminology (i.e., LOINC code, etc.). It may also occur if two tests that use different methodologies for the same condition are mapped to the same reference terminology. This could happen because mapping different formats is a manual process, subject to the interpretation of the individual mapper, who may be an IT professional rather than a medical professional. It may also be the other way around, where a medical professional without reference terminology experience is tasked with mapping codes following an update. Tests using different methodologies and producing noncomparable results may also be *appropriately* mapped to the same reference terminology, as the terminology structure may not support sufficient granularity to distinguish results performed on different noncomparable instrumentation. On the other hand, there can be multiple appropriate codes for a given test, so different users may not always select the same code. Implementation/mapping guidelines cannot anticipate every system and source data upon which the terminology or messaging standards would be implemented. Therefore, guidelines cannot provide specific mapping of proprietary data to standards. Inconsistent mapping is more likely to occur if implementers are unable to access support resources to clarify ambiguities in implementation/mapping guidelines or standards themselves.
Causal Factors	• Decentralized oversight • Inadequacies and gaps in laboratory data standards (ambiguous standards) • Inaccurate perceptions of the risk of HIT

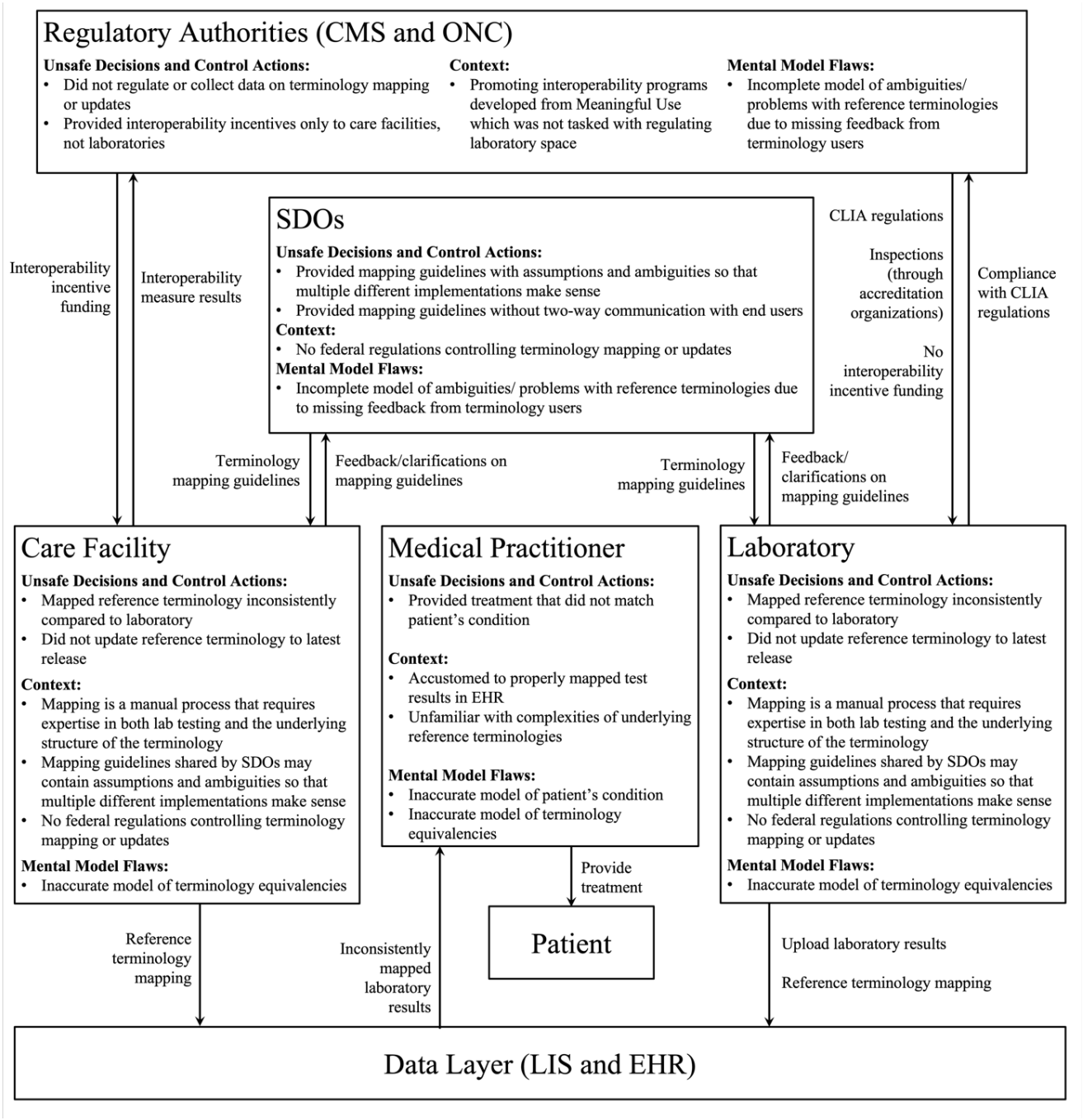

Figure 7. Visualization of Scenario 1-14

4.5.2. Scenario 6-2

Table 6. Scenario 6-2

Category	Scenario Information
Related UCA	**UCA 6-2:** Laboratory/care facility does not update HIT system when safety-critical HIT system update is released
Controllers involved	• Laboratory • Care facility • HIT Company • Regulatory Authorities
Scenario	A laboratory/care facility may not have updated their HIT system because they believed the update would interfere with other IT systems the laboratory/care facility uses. The laboratory/care facility may have this belief if prior system updates resulted in other IT systems encountering problems. They may also have received information from other facilities with the same software system that may have already taken the update and experienced problems. Some HIT system updates may have an impact on 3rd party HIT systems as well as downstream instruments. Software code changes may not be implemented successfully without thorough validation testing and coordination between HIT system vendors and users. Currently, regulatory or statutory incentives ensuring safety-critical updates do not affect other safety-critical functionality are inadequate. Maintaining up to date LIS systems depends on vendors working in partnership with users when new code releases are coming, which may not occur without dedicated maintenance contracts.
Causal Factors	• Decentralized oversight • Missing/inadequate feedback • Inaccurate perceptions of the risk of HIT

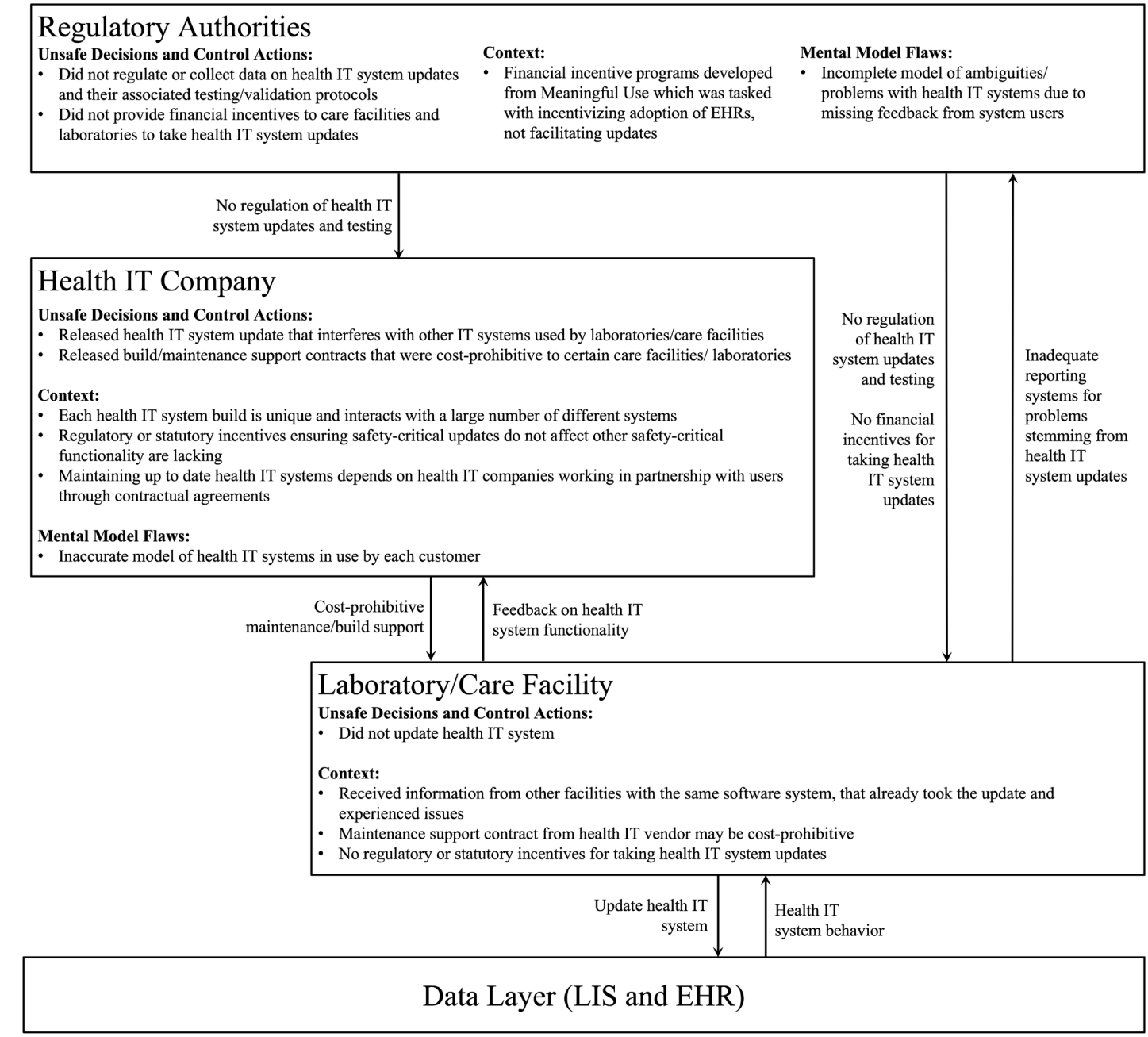

Figure 8. Visualization of Scenario 6-2

4.5.3. Scenario 30-1

Table 7. Scenario 30-1

Category	Scenario Information
Related UCA	**UCA 30-1:** SDO creates/releases reference terminology or messaging standard that does not sufficiently standardize communication between users.
Controllers involved	• SDO • Regulatory bodies • All other controllers in the system
Scenario	The SDO may release reference terminology that does not sufficiently standardize communication between users because their terminology does not capture enough information to adequately identify a test/disease. That may occur because the individual codes do not capture contextual information regarding a specific instance of a test/disease, such as the specific test kit used to perform one instance of a test, or the body site at which a condition has manifested. This may occur because reference terminology SDOs are not tasked with capturing all contextual information regarding a specific instance of a test/disease, as they operate under the assumption that HIT systems and their associated messaging standards will include additional fields for contextual information about a specific instance of a test/disease. SDOs are typically consensus organizations and ideally, clinical information is modeled in a manner that is most efficient for use by implementers for many different use cases with a wide range of requirements. Therefore, there is not a single model that is used, and clinical information may need to be available in multiple forms. Each member of the consensus organization may thus have goals that conflict with those of other members, and standards may be written loosely to compromise to each member's goals.
Causal Factors	• Missing/inadequate feedback • Decentralized oversight

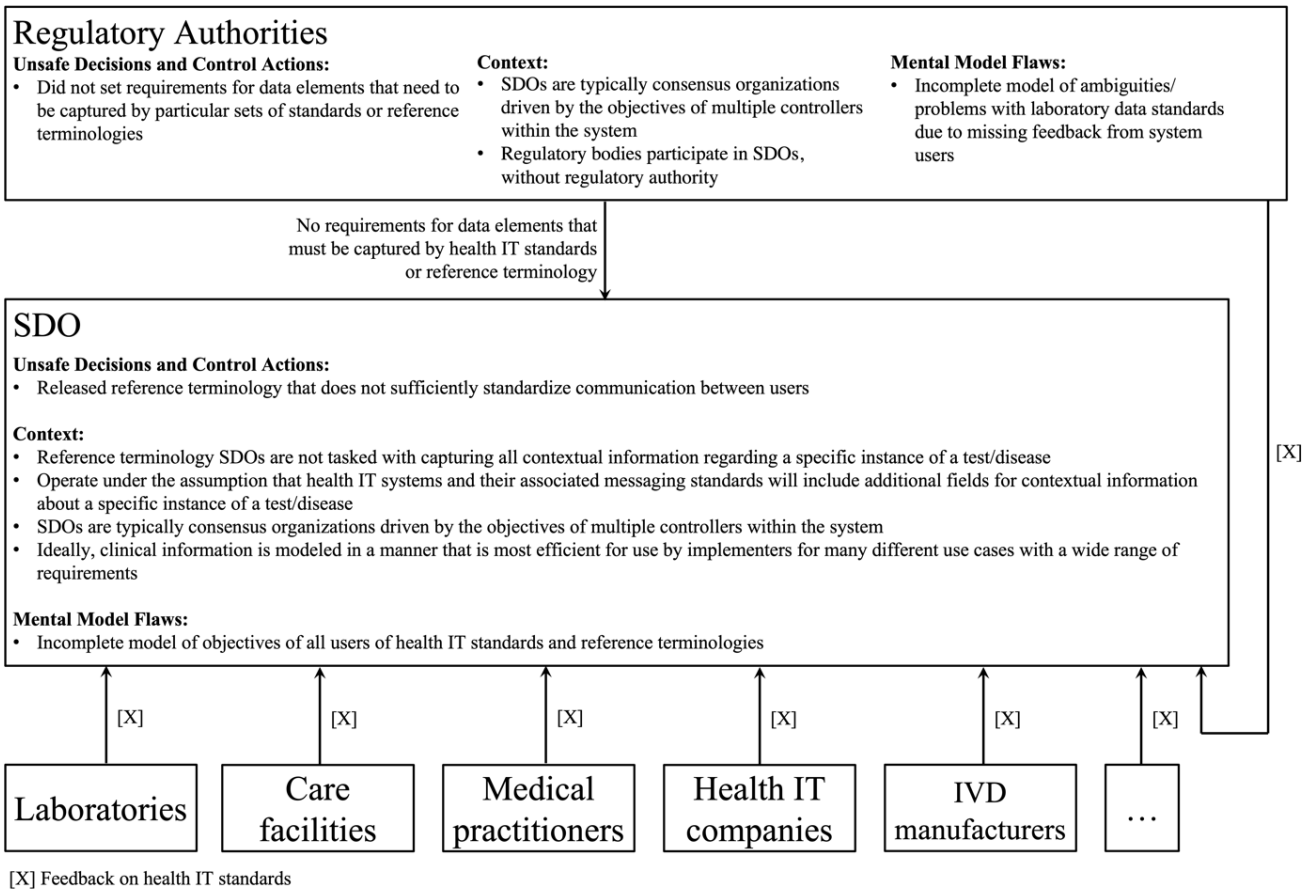

Figure 9. Visualization of Scenario 30-1

The next section of this report consolidates the analysis of the A-level scenarios presented above and in Appendix D into a set of systemic factors that permeate the laboratory data ecosystem.

5. Discussion and Recommendations

The scenarios outlined above highlight several key patterns and systemic flaws. These systemic causal factors are discussed here in detail, with examples and references to scenarios in Appendix D. Below each systemic factor are one or more recommendations to address that systemic factor, generated from analysis of the scenarios.

5.1. Decentralized Oversight

Another key causal factor observed across multiple scenarios is decentralized oversight of different components of the laboratory data ecosystem. Laboratories, IVD devices, laboratory HIT systems, and care facility HIT systems are each primarily regulated by different agencies within HHS and are regulated to different degrees. Some regulatory control loops are individually quite strong. For example, the oversight of laboratories provided by CMS and its approved accreditation organizations, or the approval of new IVD devices by the FDA. On the other hand, responsibility for oversight of HIT systems has been diluted across a multitude of HHS agencies based on each agency's original responsibilities and capabilities.

The branches of HHS are in constant communication with each other. and they attempt to collaborate to minimize regulatory burdens on healthcare providers, IVD manufacturers, HIT companies, and others. However, the decentralization of regulatory authority means that even solutions developed through partnerships across agencies are typically unable to affect the ecosystem beyond the jurisdiction of those particular agencies.

The result is a system in which *individual* regulatory control loops (like those on laboratories or devices) may be strongly enforced, while *collectively* the system is weakly regulated. There are very few regulations that address interactions among system components in a meaningful way, partly because decentralization makes it unclear who has the ultimate jurisdiction over interactions. Furthermore, agencies within HHS must receive direction from Congress before they can enact regulations on industry, especially industries commonly regulated by other agencies.

One example of inadequate coordination when regulating interactions appears in Scenario 1-13. As a reminder, this scenario deals with EHRs incorrectly trending laboratory data containing different units, reference ranges or test methodologies. CLIA does offer protections against missing units or reference ranges by requiring that a test result report indicate "if applicable, the units of measurement or interpretation, or both" [42 CFR 493.1291(c)(6)] as well as requiring that "pertinent 'reference intervals' or 'normal' values … be available to the authorized person who ordered the tests" [42 CFR 493.1291(d)]. However, upon arrival at the care facility EHR, test result data are no longer under the purview of CLIA's interface regulations, other than the requirement that data remain available to the laboratory or CMS upon request [42 CFR 493.1291(b)]. EHR systems are subject to the ONC's certification criteria, but how a certified EHR is implemented or used at individual care facilities is not.

In the EHR certification criteria from the ONC, there are no strong controls over the methods through which test result data are aggregated and shown to the medical practitioner. The ONC final rule only mandates the inclusion of "laboratory test(s)" and "laboratory value(s)/result(s)" as part of the "common clinical data set" required for several types of data exchanges. ONC's certification criteria require that clinical decision support interventions *can* be triggered based on laboratory test results [45 CFR 170.315(a)(9)], but they do not control how laboratory test data is presented within or outside of clinical decision support functionality. The decentralization of authority thus means that even a control that is strongly enforced on the laboratory side (CLIA) does not ensure that information actually makes it to the person that will use it (the medical practitioner) on the care facility side.

Ultimately, the different authorities enacting regulations on different components of the system often have different goals they have been assigned by Congress or the HHS leadership structure. For instance, CLIA and CAP certification of laboratories is designed to maintain and improve safety, while the ONC's EHR certification criteria included in the final rule of the 21st Century Cures Act is primarily concerned with ensuring that HIT systems possess certain capabilities in order to increase their usage. Without proper coordination, differing goals may lead some regulatory agencies to enact strong controls on certain elements of the system, then hand those elements off to other agencies that will not strongly control them, rendering the prior controls less effective.

Decentralization not only affects regulatory controls, but also the financial incentives that care facilities and others are offered to adopt safer practices. We see financial incentives coming up in scenarios like 1-1. Scenario 1-1 deals with data being shared between facilities in unstructured formats. The 21st Century Cures Act (Cures Act) regulates data sharing between care facilities. The Cures Act requires that certified HIT products adopt particular data standards for communicating laboratory data in order for their customers to receive financial incentives through CMS's Promoting Interoperability Program [23]. While laboratory HIT companies *could* certify their software to ONC standards and meet the requirements of the Cures Act, laboratories are not eligible for any financial incentives through the Promoting Interoperability Program [23]. As a result, there are no requirements for laboratory HIT systems to use more advanced standards like FHIR for communication with EHRs [24].

Decentralization creates environments where strong regulatory controls are not consistent among all components of a system. This ultimately hinders the adoption of new standards that might help address the problems stemming from the results of new and complex diagnostic tests results being shared in unstructured formats.

Another consequence of decentralized oversight is that regulatory agencies may not have access to critical information. An agency may need information from system components that affect their mission but do not fall under their regulatory scope. For example, in scenario 36-1 the CDC cannot provide appropriate guidance because they do not have access to the data necessary to perform a complete analysis. During the COVID-19 pandemic, HHS imposed regulatory requirements under the CARES Act that mandated reporting of COVID-19 laboratory test data to the federal government, including a particular set of data elements [25]. However, these provisions expired as of May 2023 and never included diseases outside of COVID-19.

While the Cures Act included standards for reporting to public health agencies, requirements for what data elements need to be shared for each particular test or condition are still lacking. The CDC does not have the regulatory authority to require particular data elements, so they must collaborate with CMS and ONC to establish new requirements and provide financial incentives for vendors and facilities to comply with them. However, each agency often possesses different goals and directives based on the responsibilities they were assigned by Congress or HHS leadership, and the agencies have their own limitations on what they can or cannot add to regulations.

Besides decentralized oversight of the laboratory data ecosystem, there are also a number of control loops that are missing entirely (i.e., there is no formal oversight occurring). A missing control loop is different from a weak or broken control loop, in that it is not just one component of the loop that is weakly enforced or missing, but the entire loop itself. Non-existent control loops can be identified when:

- No controller is collecting any information on a problem (missing feedback).
- No controller has any authority to ensure that a problem gets addressed (missing controls).

An example of a missing control loop involves ensuring that medical practitioners have properly received the information provided by laboratories. CLIA offers protections to ensure that data transmitted by the laboratory reaches the EHR system of the end user in the same format it was shared. However, that does not necessarily ensure that the medical practitioner themselves will know about and be able to access that data. As is seen in scenario [1-14], the data may reach the EHR and be placed in a different field than where the medical practitioner expects it to be and thus the data is likely to be missed.

Some scenarios in Appendix D highlight similar situations, in which test results get placed in a queue for manual review or end up in the wrong patient's medical record and are thus inaccessible to the practitioner. These situations can occur because there are no formal control mechanisms to ensure medical practitioners actually view test results that are shared with them. Furthermore, there are no feedback channels to the laboratory or care facility administration to inform them that test results were not seen. This control loop may exist as a matter of policy in individual care facilities and laboratories, but without any formal requirement that it exist, many facilities may not have such a control loop.

Another missing control loop exists between the laboratory and the medical practitioner or care facility collecting and storing patient specimens. CLIA requires that laboratories establish and follow written procedures for specimen collection, labeling, storage, preservation, transportation, processing, acceptability, and rejection. However, when specimens are collected and stored at facilities outside the laboratory, such as a physician's office, the laboratory may receive the specimen with no additional data about how it was collected or stored. Data representations associated with collected specimens may not have sufficient fields to record necessary information for making decisions about specimen quality. Without appropriate data on specimen collection, storage and transportation, the laboratory may not take the necessary control actions to ensure that test results are meaningful. Without any feedback or control, laboratories (and regulatory bodies overseeing them) may not even have a model of how often specimens are collected or stored inappropriately, which would help them in determining what requirements need to be changed.

Because centralizing oversight of the entire healthcare ecosystem into one agency is infeasible, recommendation 1 addresses the problem of decentralized oversight through increased coordination between existing regulatory agencies. This recommendation also helps address problems of flawed communication and coordination channels, discussed in section 5.6. Recommendation 2 addresses the problem of regulatory agencies not having access to information that is critical to performing their regulatory duties. Recommendation 3 encourages additional studies to be conducted to identify more instances of missing oversight.

Recommendation 1: Assign responsibility for addressing gaps in the regulatory oversight of laboratory data exchanges between system components that are regulated by different agencies.

A central entity must be assigned the responsibility of ensuring (or at least verifying) that the full set of data elements shared from a laboratory are received and seen by their end users. That central entity may not need to create additional regulations but must ensure that regulations on each end of any laboratory data handoff (e.g., data regulations on laboratories and data regulations on EHRs) are compatible.

As data travels through different organizations and HIT systems that are overseen by different regulatory authorities, any data elements that an end user needs must be preserved. Regulatory agencies that oversee part of the process for transmitting laboratory orders and results to and from medical practitioners and laboratory devices must ensure that the controls enacted on each component of the system complement and do not negate other controls.

For instance, in order to meet the CLIA requirement that a laboratory immediately notify the ordering physician of an abnormal test result, the laboratory may need additional contextual information about the patient to be shared by the physician. Thus, the EHR system used by the physician must be required to prompt them for contextual information when a test that requires it is ordered. Similarly, CLIA ensures that data is sent to the EHR with particular data elements that physicians need, but to ensure that physicians actually see those data elements, there must be additional data and display requirements on the EHR system.

Before regulations on components of the laboratory data pipeline are updated, the central entity must ensure that the regulatory agency proposing new regulations coordinates with other agencies to ensure the changes are compatible with their regulations. Such coordination is also meant to ensure that regulatory agencies are aware of other agencies' planned updates so that regulations stay compatible not only with current rules, but future ones as well.

Recommendation 2: Identify the data and standards needs of regulatory agencies and ensure the agencies have the ability to use them appropriately.

Ensuring that agencies like the FDA and CDC can perform their assigned tasks involves ensuring that they receive the appropriate data they need. Thus, one agency must be assigned the task of coordinating to ensure that all regulatory authorities overseeing the laboratory data ecosystem have access to the data elements needed to perform their regulatory duties.

To provide more effective regulatory guidance, different regulatory agencies must receive data in formats that are useful and actionable. For example, if the FDA is to leverage laboratory data to assess the post-market performance of IVD devices used across a wide range of laboratories, data from each facility must be transmitted with device identifiers so that they can be appropriately aggregated. Similarly, if CDC is utilizing laboratory results to track disease outbreaks, they may need particular contextual information about each patient to be shared with them in order to examine trends and provide appropriate guidance.

A single authority must be tasked with assessing the various data needs of regulatory agencies and establishing a set of data sharing requirements that laboratories (and their associated HIT systems) must comply with. This regulatory authority must also ensure requirements contain data elements that are necessary to appropriately send data from lab to physician and to aggregate data in EHRs. If each stakeholder continues requesting pieces of data in different formats, no single stakeholder will consistently receive the high-quality data they need.

Continuing to develop the USCDI standards (through the ONC) may help achieve this goal. However, if USCDI is to be truly effective, it must be used by more stakeholders in the healthcare ecosystem, and thus must capture more of the data elements that are relevant to each stakeholder. For example, USCDI requirements for laboratory test reporting must include at least the data elements required by CLIA, but should also include additional elements, such as IVD device identifiers. While USCDI is required for certified HIT, not everyone in the ecosystem is required or incentivized to use certified HIT. Even if they do not use certified HIT, incentivizing other agencies to adopt USCDI may help ensure that data is shareable in the format that each stakeholder needs. Appropriate groups such as ONC must incentivize or require broader usage of USCDI and other relevant standards.

Recommendation 3: Encourage the identification of regulatory gaps in other areas of the laboratory ecosystem through additional systems-theory-based analyses

Identifying instances of missing oversight like the examples provided above requires a systemic analysis of the laboratory ecosystem. While this study uncovered several critical gaps regarding the safety of laboratory data in particular, the scope did not cover the entire laboratory ecosystem and it is likely that additional gaps exist. To improve the safety of the laboratory data ecosystem, other stakeholders in the broader laboratory ecosystem must also work to identify and address existing gaps.

For the recommendations provided in this report to be most impactful, agencies responsible for the oversight of other components of the ecosystem should use systems-theory-based methodologies like the one utilized here to identify what changes not identified here must also be implemented. Laboratory data can only ever be as safe as the systems and processes that create and utilize it.

5.2. Inadequacies and gaps in laboratory data standards

Another set of systemic causal factors observed throughout the scenarios is the presence of laboratory data standards that are not tightly constrained, can be interpreted and implemented ambiguously by different users, or are not kept up to date. These standards represent controls over laboratory data. If these controls are enforced inconsistently across the system, data may be shared in ways that appear reasonable to the sender but are in fact difficult for the receiver to use appropriately in making treatment decisions.

5.2.1 Loosely constrained standards

One particularly clear example of loosely constrained standards affecting the safety of laboratory data is in scenario 1-A. New diagnostic tests may address gaps or challenges that medical practitioners face in diagnosing and treating patients. Therefore, laboratories and IVD manufacturers want to release tests for use as soon as possible, regardless of whether or not data sharing standards have caught up. In order to use new tests before tightly constrained standards are released and adopted, laboratories often share test results in unstructured formats. One popular unstructured format is PDF.

Rich text representations like PDF have some benefits, like the ability to format text and include hyperlinks[24]. However, data within such textual reports is difficult to consistently extract and map into a patient electronic record. Without appropriate association to fields in an EHR, such static data may not trigger clinical decision support resources [34]–[37]. As is shown in the scenario, practitioners providing treatment to the patients long after unstructured results were obtained may not be aware of additional information outside the mapped fields in an EHR [38].

Even after standards have begun being developed for reporting new laboratory tests, gaps may arise as a result of the development process itself, as is seen in scenario 30-1. Many SDOs are consensus organizations that contain representatives from different controllers within the control structures in Figures 4 and 5. Ideally, clinical information should be modeled in a manner that is most efficient for use by implementers for many different use cases. Each implementer may possess their own set of requirements for each use case of the standard. Therefore, clinical information may need to be available in multiple forms. Messaging standards and reference terminology codes may thus not be highly constrained due to pressures from various controllers, each of whom may have different uses for a specific laboratory test and may want it represented differently. When standards are not tightly constrained, this leaves room for ambiguity in the implementation of the standard.

Standards for reporting real-world data from IVD devices may also be loosely constrained and result in biases when aggregating data and studying trends in device performance, as seen in scenario 25-1. Though unique device identifiers (UDIs) have been implemented for IVD devices, they are unlikely to be included in databases that aggregate test result data nor required by the U.S. Core Data for Inoperability (USCDI). Reference terminologies are also often not designed to capture information about what manufacturer produced a device or assay, and whether laboratories have modified it for any particular use case [39], [40]. Test result data may have been aggregated at a care facility or laboratory for reimbursement purposes, and may not be coded to capture particular data elements that could make the data otherwise useful for clinical research or regulatory oversight [39], [41]. Though standards and implementation specifications for sharing IVD device data do exist, they are not federally mandated beyond COVID-19 result reporting and their adoption is not widespread [40], [42].

5.2.2. Ambiguous standards

Ambiguity in laboratory data standards allows controllers to implement them differently in ways that still appear reasonable and fully compliant with any regulation that might exist. One example of ambiguous standards potentially affecting patient safety involves the mapping of reference terminologies to local codes, which plays a crucial role in Scenario 1-14.

Before the inception of standardized reference terminologies for laboratory test orders and results, each laboratory possessed a set of local codes used to share information with other facilities, and interfaces had to be built to translate between each facility's codes [23], [43]–[45]. The introduction of reference terminologies allowed for smoother sharing of results across facilities, but still requires a lengthy and cumbersome process of mapping existing local codes to new reference terminologies. Furthermore, local codes may be necessary even in the presence

of adequate reference terminology if tests need to be differentiated based on managerial or logistical factors, such as whether they were performed at a laboratory's main facility or a subsidiary [23].

Individual laboratories and care facilities typically map local codes to reference terminologies according to their own best judgment, along with implementation guides and resources provided by the SDOs developing the terminology. Reference terminology mapping is often a manual process that requires expertise in the complexities of both laboratory testing and the underlying structure of the terminology [23], [45].

The task of mapping is often assigned to laboratorians without extensive knowledge of the terminology, or to IT professionals without a clinical background. This practice frequently results in different tests being assigned to the same code or equivalent tests being assigned to different codes.

However, even those with both IT and clinical experience do not always agree on mapping decisions, because inconsistent mappings may make logical sense in certain contexts. For example, because terminology codes are composed of multiple components like the property being measured, the specimen type and the test method, multiple codes might exist for the same test, some of which specify a particular component and others that generalize it [23], [46]. These ambiguities may ultimately lead reference terminology to be mapped inappropriately and medical practitioners to misinterpret test results.

In examining the regulatory authority of each controller, it becomes clear that there is no formal control loop when it comes to verifying that reference terminologies have been appropriately mapped. The 2015 final rule on HIT certification criteria issued by the ONC requires the use of at least version 2.52 of the LOINC standard for representing laboratory test orders and results [23], [45 CFR 170.207(c)], but there are no federal regulations pertaining to reference terminology mapping.

The main control that does exist comes in the form of implementation and mapping guidelines shared by SDOs, which are often complex and require a nontrivial amount of effort to process [47]. Developers of implementation and mapping guidelines cannot anticipate the nuances of every system that may adopt the standards. Therefore, guidelines must cater to all potential users of the standard and cannot provide individual users with detailed and unique mapping support. As a result, guides may contain ambiguities based on assumptions about what a "normal" implementation may look like [48]. Such ambiguities could allow different users to reasonably implement standards in vastly different ways. Furthermore, when guidelines are shared with laboratories and care facilities without explicit two-way communication channels, there may be a real (or perceived) difficulty in obtaining clarification or support to follow the guidance.

5.2.3. Outdated standards

Beyond the overall subjectivity of reference terminology mapping, the use of outdated or obsolete laboratory data standards may similarly raise challenges [23], [46], [49]–[51] that ultimately affect patient safety.

Addressing ambiguities within the standards will still not fully prevent patient harm if such standards are not widely implemented and used across the entire diagnostic healthcare ecosystem, or not constantly kept up to date. Laboratories often have a business incentive for adopting reporting standards, as care facilities are likely to want to use laboratories that can more seamlessly communicate with their own EHR systems. However, without regulatory guidelines coupled with financial incentives for implementing such standards, the high cost of implementation may not lead laboratories to see enough of a return on their investment to be worth updating their systems [52]

The consequence of standards being out of date can be seen in scenario 1-14. If an SDO releases a reference terminology update that changes an existing code or introduces a new code, and a facility does not update their HIT system, diagnostic data shared to or from other facilities may not be appropriately aggregated in either facility's system. Additionally, if facilities do not retroactively map historical data to updated reference terminologies, patients' clinical history may be obscured from practitioners. Outdated terminology may also not trigger clinical decision support resources as expected.

Several studies have proposed auditing schemes for both laboratories and SDOs in order to ensure consistency of reference terminology mapping and usage [23], [53], [54]. An additional control on reference terminology mapping was enforced by the FDA on IVD manufacturers as part of SHIELD's LOINC to IVD (LIVD) program, which aimed to ensure that all laboratories using the same IVD device detecting for SARS-CoV-2 describe the test and its result using the same reference terminology codes [55]. By having IVD manufacturers themselves map device outputs to reference terminologies under the supervision of the FDA, an additional layer of control is enforced by removing some of the burden and uncertainty of mapping from individual laboratories.

As with terminology mapping, there is no formal control loop when it comes to verifying that laboratory data standards are up-to-date at every facility. Laboratories typically rely on pressure from clients to adopt specific standards, which may not always provide particularly strong or consistent control.

Recommendations 4, 5, and 6 address the problems of loosely constrained, ambiguous and outdated standards by enforcing additional controls on how standards (and the HIT systems they rely on) are developed, implemented and maintained. The problem of outdated standards would also benefit from a stronger control loop as described later in recommendation 10.

Recommendation 4: Reference libraries must develop a knowledge base that establishes a ground truth for naming, coding, and mapping of reference terminologies to particular laboratory tests, and stakeholders must be incentivized to use it.

One component of eliminating ambiguities and more tightly constraining laboratory data standards is having an agreed-upon baseline with which to compare different implementations of a standard. Reference libraries must coordinate with standards development organizations to establish a universal and integrated knowledge management system that documents a set of ground truths when it comes to naming laboratory tests, assigning them codes, and mapping between different terminologies for test result reporting.

At a minimum this knowledge base should document the established mapping of test type to LOINC code. However, it would be most valuable for this knowledge base to establish the ground truth for mapping decisions for each data element in the standard as described in recommendation 2. For example, if a care facility receives a test result without a code or with an inappropriate or outdated code, the facility should be able to use a unique device identifier to consult the knowledge management system and identify the appropriate code for that test and device.

To further streamline the consolidation of reference terminology usage and ensure the database stays up to date, devices approved by the FDA should include pre-approved LOINC codes. Requiring that devices include LOINC codes that adhere to the established "ground truth" could help reduce mapping disagreements between the hundreds of laboratories across the country that utilize the same device to perform a particular test. This process was pioneered through the LIVD program and could be expanded beyond the program's original scope.

Incentivizing stakeholders to use the knowledge base could be done by first incentivizing IVD manufacturers to associate appropriate codes with their devices, which should be done in collaboration with the knowledge base developers. Once the program has matured, it should be included as a requirement in the device approval process. The approval for new devices should involve coordination between the IVD manufacturer, the FDA and reference libraries to determine what the most appropriate terminology code for the device would be, based on previously approved devices. Care facilities and laboratories must also be incentivized to use this knowledge base. Financial incentives could be used initially to increase usership and strengthen the program. However, once the program is well established, stakeholders should be required to use the knowledge base when mapping terminologies.

If efforts to improve mapping via a national knowledge base are successful, this tool could also be used to facilitate the normalization of test result reports across laboratories so that they are directly comparable regardless of the device or process used at each laboratory. An HL7 message with a device identifier, LOINC code, and normalized test result would thus become easier to collate and compare between patients across regions, devices, and time periods. Data from tests measuring the same value should be able to be charted together so medical practitioners and patients can assess laboratory values over time.

Recommendation 5: Assign responsibility to appropriate groups to identify gaps and weaknesses in laboratory data standards and establish a reporting channel for problems related to them.

A central entity must be assigned the responsibility to continuously identify potential gaps in laboratory data standards, inconsistencies between standards, or outdated standard usage. Reference libraries, who would manage the knowledge base proposed in recommendation 4, are a potential candidate to perform such a task, as it would aid them in curating the knowledge base and proactively addressing any identified problems.

The central entity must proactively seek to identify gaps through independent research, reports from standards users, collaboration with regulatory agencies, and SDOs themselves. This entity must not participate in the standards development process in the same way that other regulatory authorities do, such as CMS or ONC, but must operate independently to actively monitor the development of new standards, make safety-critical gaps publicly available, and evaluate that they are addressed appropriately by SDOs.

Recommendation 6: SDOs must continuously support users by identifying and eliminating ambiguities in implementation guides for HIT standards

Another element of removing ambiguities is ensuring that the guidance for implementing standards is consistent. SDOs must actively collect feedback on implementation guides and document any identified ambiguities or other problems. Future implementation guides should eliminate any ambiguities identified in previous guides and inform users of how to appropriately modify their systems if implemented incorrectly.

Additionally, SDOs must not release standards or implementation guides without formalized two-way communication channels between implementers of the standards and the SDOs. System hazards resulting from implementation guide optionality should be identified and eliminated whenever possible.

5.3. Inaccurate perceptions of risk

A common causal factor observed in multiple scenarios is a flawed perception of risk in diagnostic healthcare. Many stakeholders in the ecosystem hold assumptions about the safety-criticality of laboratory data and HIT that affect decisions made across the system. As a result, laboratory data and HIT problems are not prioritized when designing and implementing solutions. In fact, misperceived risk is a common cause of accidents in all industries.

Misconceptions regarding the laboratory data and the HIT software are distinct. Each is directly addressed in the following sections.

5.3.1. Inaccurate perceptions of risk involving laboratory data

Most preventable harm patients experience occurs at the point of care. As a result, in-vitro diagnostic testing is generally viewed as low-risk and not a significant contributor to safety-related events (beyond harm to patients during specimen collection). A common argument used to defend this position is that treatment decisions are ultimately made by medical practitioners, and diagnostic data is only one component in the decision-making process. However, taking a systems-theoretic approach reveals that control actions and feedback are closely linked, and it is unreasonable to criticize the action without also considering the information available and used to inform that action.

This nuance is particularly clear in scenarios 1-1, 1-13 and 1-14, which deal with medical practitioners providing treatment that does not match a patient's condition. Though it is ultimately the treatment decision that harms the patient, feedback in the form of diagnostic data is what informs that decision. In scenario 1-1, that feedback is missing entirely. In that case, the medical practitioner is unaware of results shared in an unstructured format and does not have sufficient information to make a safe decision. In scenarios 1-13 and 1-14, the diagnostic data is inaccurate or misleading because it is presented poorly. Poor data presentation can easily cause an incorrect interpretation to appear perfectly reasonable to a practitioner. Medical practitioners operate in fast-paced and high-stress environments [16] where missing or inadequate data may not be recognized or questioned.

Missing data can be particularly difficult to identify and is thus a particular risk to patient safety [17]. For example, if a physician is expecting a particular test result but they do not see it displayed in a patient's profile. Recognizing the missing data, they may expend additional time to try to identify hidden information (like unmapped PDF reports). However, if the test was ordered by another physician or was shared a long time ago, the physician may have no reason to expect that the structured data they see is incomplete.

Thus, the contents and presentation of laboratory data plays a significant role in the decision-making process for medical practitioners, even if test results themselves do not harm patients directly. However, the minimized perception of the safety of diagnostic data means that many care facilities lack either proactive or reactive safety teams that focus on investigating sources of diagnostic error [16].

Furthermore, reporting structures for problems involving laboratory data are not well established. CLIA does require that laboratories have procedures in place to collect and address complaints submitted by medical practitioners. However, such complaints do not need to be reported anywhere outside of the laboratory or to the provider whose test result report was affected by a problem. As a result, there is no regulatory body that keeps records of problems involving laboratory data in order to determine whether regulatory requirements need to be changed or added.

Gaps in reporting of laboratory data-related problems are also shown particularly clearly in scenario 25-1. In this scenario, the FDA does not issue corrective action to device manufacturers providing diagnostic equipment with safety flaws because of inadequate reporting of these flaws. Many existing reporting structures only require that events involving direct patient harm get reported to regulatory bodies. When IVD devices and laboratory data

as a whole are not considered safety-critical, their contributions to adverse events may go underreported in favor of placing responsibility on the providers at the point of care.

Additionally, under section 522 of the Federal Food, Drug, and Cosmetic Act, the FDA can only require post-market surveillance studies of class II and III medical devices. Post-market studies that have been performed on devices beyond just IVDs, have been found to produce little clinical data on device performance, with many devices being weeded out before the studies could be completed and published [18]. Until feedback in the form of laboratory data is recognized as an important contributor to unsafe decisions at the point of care and is included in reporting requirements, regulatory bodies will not have sufficient information on the ways in which data impacts the safety of the healthcare system.

Recommendation 7 addresses inaccurate perceptions of risk involving laboratory data by considering the role of laboratory data more explicitly in adverse event investigation.

Recommendation 7*:* Proactively and retroactively investigate systemic sources of diagnostic error.

To address inaccurate perceptions of risk involving laboratory data, care facilities must proactively and retroactively investigate potential systemic sources of diagnostic error, including laboratory data.

When patient harm occurs, care facilities must have the responsibility to explicitly consider whether diagnostic error was a contributing factor to the adverse event. Often, care decisions made by clinicians, laboratorians, or other controllers may have appeared reasonable despite being unsafe in hindsight. It is unreasonable to criticize an inappropriate decision by a medical practitioner without considering what information was available to inform that decision.

Care facilities must either create investigation teams that are particularly focused on sources of diagnostic error or incorporate consideration of diagnostic error into existing adverse event investigation processes. Particular focus should be given to systemic sources of diagnostic error (i.e., ways through which the design of systems and processes that practitioners use may have contributed to an incorrect decision).

Teams investigating adverse events must understand and acknowledge the significance of laboratory data in the medical decision-making process by framing it as a critical piece of feedback used by clinicians. In particular, the teams must consider what pieces of feedback would have been necessary to make a more appropriate decision, and why medical practitioners did not appropriately receive them. For example, laboratory data may have been hidden, presented in a misleading manner, or missing altogether. Care facilities must also establish a structure of accountability, to ensure that teams conducting adverse event investigation have truly considered all potential sources of diagnostic error.

Investigating inappropriate diagnostic decisions by scrutinizing what information was or was not available to inform practitioners' mental models facilitates the creation of recommendations that will improve outcomes across the care facility as opposed to focusing on individual practitioners' aptitude or training. To ensure that sources of diagnostic error are identified beyond the actions of just one component of the system, the teams must include investigators with clinical, laboratory and informatics backgrounds. Considering the contributions of every element in the system that may have contributed to an inappropriate decision also aids in eliminating blame from the process and thus encouraging further frontline reporting of safety concerns.

Care facilities also must ensure there are employees with the responsibility to proactively identifying possible sources of diagnostic error by continuously monitoring any updates and changes to care facility systems, particularly those that are relevant to the sharing and presentation of laboratory data. Adverse events often follow changes and managing change is a basic management function for any organization.

5.3.2. Inaccurate perceptions of risk involving HIT

Software in general is subject to several inaccurate assumptions and perceptions. HIT software is no different. Common incorrect assumptions about HIT include that HIT systems are not safety-critical and that they are easier to implement and maintain than they actually are.

The assumption that HIT systems are not safety-critical is apparent in how HIT systems are sold and regulated. EHRs and LIS systems are labeled as "health management" [19] tools by the FDA and ONC. This view of EHRs and LISs as "health management" tools asserts that medical practitioners are supposed to act as "learned intermediaries" between the systems and their patients [20]. Medical practitioners are then seen ultimately responsible for patient care decisions regardless of the feedback provided (or not provided) by the system. Treating HIT as simple health management tools has consequences for customers (especially clinicians) and patients.

One consequence is the pervasiveness of "hold harmless clauses" in contracts between HIT vendors and their customers. "Hold harmless" clauses ensure that vendors are not held responsible for errors resulting from usage of their systems, even if the company was aware of the potential risk[20]. Another consequence is how HHS agencies treat EHRs. For example, The FDASIA report (a 2014 report by the FDA, ONC, and FCC) concluded that "We believe the potential safety risks posed by health management HIT functionality are generally low compared to the potential benefits." [19] This low risk-rating enables HIT to escape rigorous oversight regarding safety concerns and belies the role of software in adverse events in healthcare (and most every other industry).

Scenario 13-1 is a good example of how the belief that the physician is ultimately responsible for safe decisions can lead to unsafe outcomes. In that scenario, a HIT company does not release updates to address potentially safety-critical flaws because of the belief that the flaw emerged from the clinician not using the system as designed, even if the software design was counterintuitive or misleading.

In addition to the assumptions about safety, HIT suffers from assumptions about the ease of maintainability. Frequently, care facility management and others have the idea that HIT software packages are "turnkey," and are easily implementable in new contexts.

Unfortunately, the process of implementing a new EHR in a care facility is often much more difficult, time consuming, and expensive than expected. HIT vendors benefit from these assumptions. HIT vendors and care facilities often push aggressive timelines for EHR implementation, which often create situations where groups in charge of implementing HIT systems select inaccurate or inadequate options or settings. One example of an unsafe implementation selection, detailed in Scenario 2-10, is implementing a test order menu in a care facility EHR that shows more or fewer tests available than the partner laboratory offers. An additional example could include a care facility accidentally not turning on a setting that is important for safety critical functionality.

Recommendation 8 addresses inaccurate perceptions of risk involving HIT by establishing clear mechanisms for collecting feedback on HIT safety concerns.

Recommendation 8: Create a consolidated national database for HIT safety reporting that can be used to identify trends and opportunities for improving patient safety outcomes. It should include information about HIT not behaving as users intended and allow understanding how features of HIT design may have contributed to "user errors."

Rectifying inaccurate perceptions of risk involving HIT requires gaining a better awareness of the specific risks generated by usage of HIT products. All reports of HIT and data related safety concerns must be consolidated by one organization at the national level to effectively identify trends and opportunities for improving patient safety outcomes.

Users of HIT must have one consolidated platform through which they can report safety concerns involving HIT functionality or data. Medical practitioners should not be required to report some HIT problems to care facility management, others to HIT vendors, others to ONC-ACBs, and others to the FDA.

A national repository for HIT and data related problems would allow and require users and care facilities to send reports of safety problems they experience to a single authority. As the leading regulatory body overseeing HIT systems, ONC is a potential candidate for creating and operating such a repository. The operator of such a repository would be responsible for facilitating the capture of information, analyzing it, disseminating information from or about the repository, and allowing access to those with legitimate needs for the information.

Appropriate responsibility, authority, and accountability for a useful and effective repository should be assigned throughout the control structure. For example, medical practitioners associated with a particular care facility should be responsible to report HIT and data related problems to the care facility administration, who would in turn be required to submit every report to the national repository regardless of whether or not they believe "user error" was primarily responsible. This repository should be separate from existing pathways for reporting concerns to HIT vendors, but care facilities should also transmit all reports of EHR-related problems submitted by medical practitioners to HIT vendors.

HIT companies should develop a safety culture in which both customers and developers are encouraged to ask questions about system design, usability, and safety. Healthcare facilities must develop a complementary culture where they encourage IT performance reports from medical practitioners. However, the agency that is monitoring the repository must ensure that reports are consistently followed up, and the necessary changes are made to affected HIT systems.

The reporting process should allow medical practitioners to describe the observed problem (including screenshots if available) and should require the care facility administration to fill in information regarding the particular system involved and associated vendor/version information. Instances of HIT systems not behaving as users intended must also be included in the reports submitted to the database, and the procedure for addressing each report must explicitly consider how features of the HIT system design contributed to "user errors."

The repository should be openly accessible to the public after deidentification of all reports and removal of sensitive patient information. Additionally, the organization tasked with managing the repository should have active monitoring programs in place that allow for research into trends in HIT or data safety. The managers of the repository should also have the responsibility to further investigate any report that is received or transmit reports to other agencies that may have structures in place to investigate them.

For example, the repository could transmit batches of reports to the ONC's HIT certification branch that describe certified HIT products not meeting certification standards. They might also transmit reports to the CMS that describe laboratory HIT systems not meeting data sharing requirements imposed by CLIA.

The point of this database should not be to identify who to "blame" in any incident or report. Analysis should be focused on uncovering industry-wide trends as opposed to identifying whether punishments should be doled out to individual vendors or facilities. A similar recommendation was made in 2014 by the FDASIA report and is still relevant today. Similar national databases exist in other industries. For example, the NASA ASRS database collects de-identified information about safety-related incidents. Although the first reports in ASRS were submitted by pilots in both commercial and general aviation, the success of the program led to its extension to include reports from almost all participants in the industry.

5.4. Lack of a Systems view

In conversations with stakeholders from across the system, it became evident that nearly everyone is trying to make changes to reduce adverse events. However, without taking a systems' view, many changes made at the local level do not make the system significantly safer. Local "fixes" may just shift the problem to a different part of the system or make it worse. It may also cancel an improvement or change made by a different controller.

In most of the scenarios identified, each controller makes reasonable decisions based on how they believe the system or process they are controlling is designed, and on the information available to them. For example, medical practitioners are usually making the best treatment decisions they can, given the available information. However, after dozens of interviews it became clear that no stakeholder holds a complete view of the entire system and may hold assumptions about other components of the system that later we found to be either outdated or mistaken.

Laboratories are trying to share information that providers can interpret and in ways that conform to regulatory requirements. In these situations, making a local change (like adding more physician training) is unlikely to fix anything.

The impact of "locally optimal" solutions is seen particularly clearly in scenario 2-10, where each controller behaves in a way that appears optimal to them. The patient's safety, however, could still be jeopardized. In that scenario, the medical practitioner uses the EHR to order a test as specified by procedures and orders the most appropriate test to assess the patient's condition. The laboratory, which did not offer the test that was ordered, makes the most reasonable decision as well: to reject the test order and inform the practitioner. The HIT vendor who develops the EHR interface also acts reasonably, by installing a "model system" with a default list of available tests: the presence of defaults has been shown to improve medical practitioner decision-making. Finally, the care facility administration, who may be under resource constraints or may not have enough qualified IT staff, also acts reasonably in not requiring further customization that might be expensive or difficult to maintain. Each of these locally optimal decisions turns out to be less optimal at the system level. The unintended consequences do not become clear unless the decision-makers have a more holistic view of the consequences of local decisions.

Another scenario where local "fixes" create new problems is scenario 6-2, in which a laboratory or care facility does not update their HIT system out of concerns that it will break connections to other safety-critical systems. Upgrades to HIT systems may sometimes not be sufficiently tested by the vendor, especially in the many different implementation contexts that exist at each individual facility. Therefore, a solution that might appear optimal for a "model" HIT system, may actually break connections or disable functionality in a customized system.

Additionally, many HIT updates do not necessarily come with labels or descriptions of the implications of not implementing the update. Most updates are discussed internally and the decision to proceed with the update or not is made in the context of available resources and competing priorities. Also, many update decisions are made by administrative teams with varying input from the medical practitioners and laboratorians who will be the end users of the system. Particularly if systems have been in place for a long time in a facility with rapid staff turnaround, many stakeholders may be unaware of how an update will impact their tools and workflows [21].

Without a wide-ranging, systemic view of the consequences of installing or not installing a system update, a facility may install a fix that creates more problems or may not address an existing problem out of fear of creating more. Note that this same general causal factor, that is, problems in updating software, has led to accidents in aviation [22] and other high-risk industries.

Because the laboratory data ecosystem is so complex, each controller may have a hard time understanding the system as a whole. The problems identified here can be addressed by educating the healthcare community on system engineering approaches to problem-solving (recommendation 9), as well as by strengthening controls on particular processes that often result in local solutions being developed (recommendation 10). Recommendation 10 specifically addresses the issue of HIT updates affecting other systems. This recommendation also addresses the problem of outdated systems and standards, discussed in section 5.2.3.

Recommendation 9: Educate the healthcare community on systems engineering and systemic approaches for solving problems, including tools to accomplish this goal.

Healthcare education must adapt their curricula to utilize and teach more advanced hazard analysis techniques developed in systems engineering. Healthcare management must have the skills to proactively and retroactively assess the performance of systems and to identify areas for potential improvement.

Healthcare professionals must be educated to treat their surroundings as engineered systems that may not be perfectly designed. Systems engineering must be utilized in the process of designing healthcare systems and processes, as well as evaluating them to identify and address safety concerns. Many healthcare organizations are attempting to incorporate "just culture" principles, but without incorporating systems engineering principles as well, it will be difficult to productively move beyond blame when identifying areas that need to be improved.

These educational programs should also teach healthcare professionals about tools for incorporating systems engineering principles into processes like hazard analysis and system design. Different organizations throughout the healthcare ecosystem could be responsible for developing and disseminating educational programs, including patient safety organizations, professional associations, and quality organizations (e.g., Institute for Healthcare Improvement, CAP, etc.).

Recommendation 10: Establish appropriate control loops for updates to standards and HIT systems.

Fixing the problem of HIT updates breaking other systems also requires gaining a better awareness of the specific risks posed by updates. Regulatory authorities (for example, ONC) must collect feedback on the prevalence and safety effects of using outdated laboratory data standards and HIT systems. Corresponding control mechanisms to increase adoption of updated standards and systems must also be developed.

The HHS administration must determine the most appropriate agency to collect data on the updates to certified HIT systems that are released and whether care facilities or other HIT users are implementing these updates in a timely manner.

With this information, further research should be undertaken to identify whether additional regulatory action must be taken to encourage HIT users to update their systems on a regular basis. Further research is also needed to identify barriers to updating beyond those identified in this report, as well as the implications for not installing particular updates.

In the interim, within care facilities, there should be clear assignment of roles and responsibilities regarding updating both HIT systems and laboratory data standards. Organizations releasing updates must provide two-way support in addition to clearly indicating the safety-criticality of an update and any known implications of not updating a system in a timely manner.

5.5. Inadequate regulatory emphasis on the safety of HIT

Beyond gaps stemming from decentralization, gaps in the regulatory environment also stem from a historical deemphasis on safety within HIT certification. Regulatory directives to the ONC have historically been driven by increasing the usage and capabilities of HIT. Therefore, the ONC has focused on certifying the functionality of EHR systems, not their safety. There were assumptions made that safety would automatically follow from high EHR usage without specific regulatory oversight. However, this assumption has not proven to be the case in practice [26].

Designs that meet ONC certification requirements frequently have significant safety risks. For example, EHRs often merge test results that used different test methods within a patient's record. However, test results from different methods may not be directly comparable [27], [28]. This is particularly hazardous in situations where EHRs merge test results that have different units of measure or different reference ranges, as seen in scenario 1-13. Inappropriately merged test results presented together may cause the physician to draw incorrect conclusions about a patient's condition. For example, the physician may see a graph that appears to show that a measure is trending downward, when in reality it is flat.

Another example of an unsafe EHR design that passes ONC certification is how units of measure are displayed to a physician. Units of measure are often transmitted ambiguously and get misinterpreted by EHRs when they automatically aggregate patient data. Despite standards such as the unified code for units of measure (UCUM) establishing a code system for electronic communication of units, laboratories may use unit terminologies as provided by IVD manufacturers as opposed to UCUM specifications [9]. It becomes difficult for medical practitioners to uncover these discrepancies themselves when the visual interfaces that they use to access patient data within EHRs do not explicitly display units or reference ranges [29], or require additional steps/clicks to access them [27].

Furthermore, no one is currently required to use certified HIT. Use of certified HIT is promoted through the Medicare "Promoting Interoperability" (previously "Meaningful Use") programs where participants only get full funding if they use certified HIT. However, not everyone in the system is eligible to participate in that program or does so.

Recommendations 11 and 12 call for additional safety controls to be enacted on HIT systems. Their goal is to address existing safety concerns within HIT systems, as well as to further adjust users' and developers' perceptions of the safety-criticality of these systems.

Recommendation 11: Assign regulatory oversight of HIT safety to ONC or another appropriate group. Include the explicit directive to develop and include safety-related certification criteria for HIT and the ability to limit the inclusion of "hold harmless" clauses in HIT contracts.

ONC must be assigned additional regulatory authority regarding oversight of HIT safety, including the explicit directive to create and enforce safety-related certification criteria for HIT systems and the ability to limit the inclusion of "hold harmless" clauses in HIT contracts. Ensuring that HIT systems are viewed in the same way as other safety-critical components of the healthcare ecosystem requires enforcing safety controls on HIT systems that is similar to the way they are enforced on devices and processes.

The perception that HIT systems do not play a significant role in adverse events must be changed. These systems have evolved from electronic analogs of paper records to complex software implementations that aid practitioners in medical decision making. As the leading regulatory body currently overseeing HIT systems, ONC must be given additional responsibilities regarding control of HIT safety.

Certification criteria for HIT systems, which have historically been driven by a need to increase usage of HIT, must include safety criteria as well. Some of the information for generating such criteria could come from the repository of HIT safety incidents in recommendation 8. Sophisticated and modern hazard analysis techniques are also important to include in the certification process.

The mistaken perception that HIT is not safety-critical should not be instantiated by "hold harmless" clauses in HIT contracts. ONC must include limits on "hold harmless" clauses in its certification programs. Additionally, ONC must be given the authority to require HIT companies to address problems that are identified as safety-critical, regardless of maintenance contracts between HIT companies and customers.

Recommendation 12: Establish incentives for using certified HIT throughout the entire healthcare ecosystem

If more HIT systems are subject to the controls proposed in recommendation 11, safety constraints on HIT in general can be better enforced. Therefore, a wider range of users of HIT must be required or incentivized to use certified HIT products.

Usage of certified HIT systems should be required or incentivized beyond the subset of care facilities, clinicians, and critical access hospitals that are currently participating in the Medicare "Promoting Interoperability" programs. For example, laboratories that operate outside of care facilities must be incentivized to use certified HIT systems. Without requirements or incentives to use certified HIT, any improvements to the certification will not be adopted ecosystem wide.

More stakeholders in the healthcare ecosystem could be required to use certified HIT by expanding existing regulatory frameworks (e.g., CLIA) or accreditation programs (e.g., CAP accreditation). Additionally, adoption of certified HIT could be encouraged by private institutions such as professional societies. Payors, both public and private, could also require or incentivize users to adopt certified technology in order to receive payments.

However, usage of certified HIT will only increase patient safety if certification criteria place patient safety as a priority, as recommendation 11 suggests.

5.6. Flawed Communication and Coordination

One of the most common causal factors observed throughout the system is the lack of formal communication and coordination channels between controllers. Many regulators do not have the information they need to change or update regulatory standards.

Even between medical practitioners and care facilities, safety concerns regarding HIT systems are often underreported [56], [57]. Medical practitioners may be reluctant to report occurrences out of fear of not being considered knowledgeable or competent [16] in operating the system, or because of fear of being punished [58]. Additionally, filling out error reports may be time consuming. A medical practitioner may not know what errors are reportable and may not trust that reporting will be worth the effort.

Without strong feedback, care facility administrations may not attribute particular importance or priority to HIT related usability or safety concerns when they do arise. Instead, care facilities may believe that the systems were operated incorrectly by the practitioners. Given the high cost and effort expended to implement or customize HIT systems, it is not unreasonable for management to be reluctant to uncover and acknowledge problems that would require significant resources to address. Care facilities may not have maintenance contracts with their HIT vendor so they may use workarounds that are more immediately cost-efficient, such as trying to change a medical practitioners use of a system rather than the system itself [59]. Furthermore, if HIT related safety concerns are not identified at the care facility level, they will never reach the vendors or regulatory authorities that could enact further controls on the systems.

Even if a care facility has good internal records of safety problems with HIT, there is no federal repository for this data. The ONC directs care facilities and medical practitioners to send reports of problems involving HIT to the HIT company, then to the ONC-Authorized Certification Bodies and then finally to the ONC if they do not get a response from the other two parties. The ONC, however, is only looking for information on whether or not certified HIT products are meeting certification standards in the field. Some reports get sent to the FDA Maude database, but as HIT is not under their purview, they get few results and cannot take much action on them. The 2014 FDASIA report recommended the creation of an agency under the ONC for this purpose, but it was never created.

Lack of quality feedback also contributes to a positivity bias for scientific publications surrounding HIT [55], [60]. The positivity bias might influence decisions made by care facility administrations when it comes to acquiring and utilizing HIT. Positivity bias is a good example of circular causality in accidents, where lack of feedback leads to weak controls, leading in turn to even less feedback. Because of widespread assumptions regarding the safety of HIT, real problems are underreported and assigned low priorities. As a result, few safety controls are enacted on HIT systems and stronger controls are enforced on medical practitioners that operate these systems. This circular causality perpetuates the idea that practitioners should be responsible for compensating for flaws in HIT and leads them to report these flaws less often.

Inadequate communication and coordination channels between data users may also contribute to patient harm. Many unsafe situations arise because physicians and laboratorians are expected to perfectly execute tasks that require data that is not consistently provided in many current systems.

For example, as described in scenario 2-21, laboratories are typically responsible for communicating quickly and directly to the physician when a notable result is identified. This notification allows physicians to be alerted to results that require an immediate response. Without the notification, physicians may be unaware that a critical and time-sensitive result was obtained until the next time they open that patient's record. Unfortunately, laboratorians may not have sufficient clinical context to identify all critical results.

Reference ranges, the numerical bounds that determine if a lab value is "normal" or "out of range," are essential elements for interpreting a test result. Reference ranges may vary based on demographic factors like age and sex, as well as specific preconditions patients might have [30], [31]. The laboratory often does not receive sufficient clinical context to know which reference range is most applicable to a patient, and therefore whether a diagnostic test result is critical or time-sensitive [32]. For example, orders sent from a medical practitioner to a lab may not include the age, gender, weight, or previous diagnosis of a patient. An oncology patient may need a transfusion for a higher platelet test value, whereas, for an otherwise healthy individual, the critical platelet value may be much lower [33].

If medical practitioners are not prompted to enter relevant clinical context—through automatic prompts in the lab order process or by other means—laboratorians will not consistently receive the required information. Medical practitioners cannot be expected to remember what clinical context is needed for every single test they may order. Often the only way for the lab to obtain missing information is to contact the ordering provider, which may be difficult under time or resource constraints. Furthermore, physicians may not have access to the information the laboratorian needs if the call comes after the patient has left the care environment.

One reason both parties may not have access to necessary data is because HIT implementation teams may have made decisions regarding needs, representations, and interfaces for laboratory data without sufficient input from laboratorians.

Recommendations 5 and 8, described earlier, address the flawed communication and coordination channels in the laboratory data ecosystem through creating the infrastructure needed to collect reports on HIT safety and gaps in laboratory data standards. Recommendation 13, below, aims to address the problem of inclusion of laboratorians in decisions regarding laboratory data infrastructure.

Recommendation 13: Develop formal processes for inclusion of laboratorians in the multidisciplinary teams responsible for decisions about laboratory data needs, representations, and interfaces at care facilities.

Care facilities, especially those with integrated laboratories, may consider opportunities for laboratorians to support decision making regarding laboratory data components in HIT. Laboratorians should help support decision making in the initial implementation, utilization, and maintenance of relevant HIT.

Determining what specific form that support should take is beyond the scope of this study, but one potential example could include ensuring laboratorians are part of the multidisciplinary teams that determine how laboratory tests are presented to practitioners both on the test order and test result views.

6. Conclusions

This study used a system-theoretic modeling and analysis approach to understanding the causes of healthcare adverse events related to diagnostic data. Our modeling was aided by interviews with participants in all parts of the healthcare system. In our interviews, the participants told us about many, if not most, of the problems that we also identified by our formal hazard analysis process. The problems and adverse event causal scenarios we identified are not unknown within the healthcare community. What is not understood widely is how to get past the problems and effect changes to greatly increase healthcare safety. Our recommendations address potential solutions.

Once again, we emphasize that our goal was not to focus on what individuals or even individual components of the system are doing wrong, but instead on why their actions make sense within the system as it exists today. Our recommendations are about how to change the overall system design to allow and encourage safe behavior by everyone. The causal scenarios for adverse events identified by STPA point clearly to actionable recommendations that can be linked to the related flaws in the system. A rationale for all the recommended changes to the system is provided by the links to adverse events.

Perhaps the biggest takeaway from our effort and from the application of system theory is that the difficult problems in healthcare safety cannot be solved without applying a systems-theoretic approach: major improvements will require the system as a whole to be redesigned, not just small tweaks to parts of it. The problems are not so much in the individual components of the U.S. healthcare system, where everyone is trying to provide safe and effective care. The most serious and persistent problems are instead occurring in the interactions and interdependences between the system components. Only by redesigning the system to control these interactions will great progress be made.

This redesign will require, as found in every other industry, some introduction of centralized or governmental controls. Local changes, though well meaning, are usually not enough to solve global problems. Local changes may have unintended consequences on other parts of the system that result in no overall increase in safety. Sometimes local improvement can even lead to decreases in healthcare safety in the system as a whole. Most industries that have dealt successfully with ensuring system safety (not just occupational or workplace safety) have found that some centralized controls over the behavior of system components and the interactions among components and over the collection of the information needed to improve safety is required. The goal should be to introduce the most effective and necessary safety controls without eliminating the local autonomy necessary to ensure productivity and efficacy.

While the recommendations in this report represent large changes for the healthcare community, they are standard features in other industries that have highly successful safety records. For example, the U.S. has an incredibly safe aviation system, which is unparalleled compared to other types of transportation systems. One of the reasons is that aviation in the U.S. long ago instituted the type of systemic control of safety recommended for healthcare in this report. They do not depend on just one type of control (for example, checklists, information collection, or accident investigation), but instead have created a safety management system that emphasizes a set of complementary controls to proactively manage hazards. Hazards, including those arising between the different system components, are eliminated, or controlled through changes to the national airspace system *as a whole* and to the interactions among the many system components.

As one example, each airline would like to optimize their schedules to fly whenever they want and wherever they want. The problem is that local autonomy leads to accidents and a “wild west” approach where some win but more lose because everyone wants to fly direct routes to the most popular airports at the same time. The Air Traffic Control System (ATC) was introduced after tragic accidents. The result has been near elimination of collisions for the aircraft in the ATC system despite large increases in flights as well as ensuring optimization of overall system throughput.

Finally, changing the current system, as difficult as it will be, is not enough. There also needs to be action to control the foreseeable changes in the healthcare industry. One of these is the rapidly growing use of software and information technology. We can wait until the inevitable adverse events start to occur widely, or we can take action to ensure that new software and advanced automation is introduced from the beginning with acceptable controls over patient safety. Other industries, for example automobiles, are rapidly introducing software into their products and systems. The automotive industry, however, is simultaneously developing the standards and methodologies required to control the new hazards. Healthcare must do the same.

The types of structural changes recommended in this report may take some time to introduce into the U.S. healthcare system. In the meantime, near-term solutions will be required to provide adequate control over hazards.

All the changes will require the participation of everyone in the healthcare community to ensure that the most effective controls are successfully created and used. Local optimization may in some cases have to be sacrificed for overall increases in healthcare safety, quality, and efficiency.

References

[1] L. von Bertalanffy, *General system theory: foundations, development, applications*, Rev. ed., 17. paperback print. New York, NY: Braziller, 2009.

[2] M. A. Makary and M. Daniel, "Medical error—the third leading cause of death in the US," *BMJ*, p. i2139, May 2016, doi: 10.1136/bmj.i2139.

[3] Committee on Diagnostic Error in Health Care, Board on Health Care Services, Institute of Medicine, and The National Academies of Sciences, Engineering, and Medicine, *Improving Diagnosis in Health Care*. Washington, D.C.: National Academies Press, 2015, p. 21794. doi: 10.17226/21794.

[4] D. E. Newman-Toker *et al.*, "Burden of serious harms from diagnostic error in the USA," *BMJ Qual Saf*, Jul. 2023, doi: 10.1136/bmjqs-2021-014130.

[5] S. A. Krevat *et al.*, "Identifying Electronic Health Record Contributions to Diagnostic Error in Ambulatory Settings Through Legal Claims Analysis," *JAMA Netw Open*, vol. 6, no. 4, p. e238399, Apr. 2023, doi: 10.1001/jamanetworkopen.2023.8399.

[6] N. Leveson and J. P. Thomas, "STPA Handbook," 2018. Accessed: Feb. 24, 2023. [Online]. Available: psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[7] N. Leveson, *Engineering a safer world: systems thinking applied to safety*. in Engineering systems. Cambridge, Mass: MIT Press, 2011.

[8] B. E. Dixon, J. J. McGowan, and S. J. Grannis, "Electronic laboratory data quality and the value of a health information exchange to support public health reporting processes," *AMIA Annu Symp Proc*, vol. 2011, pp. 322–330, 2011.

[9] J. Rychert, "In support of interoperability: A laboratory perspective," *Int J Lab Hematology*, vol. 45, no. 4, pp. 436–441, Aug. 2023, doi: 10.1111/ijlh.14113.

[10] J. D'Amore *et al.*, "Interoperability Progress and Remaining Data Quality Barriers of Certified Health Information Technologies," *AMIA Annu Symp Proc*, vol. 2018, pp. 358–367, 2018.

[11] R. G. Hauser, D. B. Quine, and A. Ryder, "LabRS: A Rosetta stone for retrospective standardization of clinical laboratory test results," *J Am Med Inform Assoc*, vol. 25, no. 2, pp. 121–126, Feb. 2018, doi: 10.1093/jamia/ocx046.

[12] P. Checkland, *Systems thinking, systems practice*. Chichester [Sussex] ; New York: J. Wiley, 1981.

[13] E. Wiener, "Human Factors of Advanced Technology ('Glass Cockpit') Transport Authority," NASA, 177528, Jun. 1989.

[14] J. D. Sterman, *Business dynamics: systems thinking and modeling for a complex world*, Nachdr. Boston: Irwin/McGraw-Hill, 2009.

[15] N. G. Leveson, "CAST Handbook: How to Learn More from Incidents and Accidents," 2019.

[16] T. D. Giardina, U. Shahid, U. Mushtaq, D. K. Upadhyay, A. Marinez, and H. Singh, "Creating a Learning Health System for Improving Diagnostic Safety: Pragmatic Insights from US Health Care Organizations," *J GEN INTERN MED*, vol. 37, no. 15, pp. 3965–3972, Nov. 2022, doi: 10.1007/s11606-022-07554-w.

[17] E. Li, O. Lounsbury, J. Clarke, H. Ashrafian, A. Darzi, and A. L. Neves, "Perceptions of chief clinical information officers on the state of electronic health records systems interoperability in NHS England: a qualitative interview study," *BMC Med Inform Decis Mak*, vol. 23, no. 1, p. 158, Aug. 2023, doi: 10.1186/s12911-023-02255-8.

[18] C. Iwaishi and K. Iwasaki, "A Comprehensive Analysis of Postmarket Surveillance Study Orders: Device Characteristics, Study Statuses, Outcomes, and Potential Contributions," *Ther Innov Regul Sci*, vol. 54, no. 4, pp. 953–963, Jul. 2020, doi: 10.1007/s43441-020-00113-7.

[19] FDA, FCC, and ONC, "FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework," Feb. 2014. [Online]. Available: https://www.fda.gov/media/87886/download

[20] R. Koppel, "Uses of the Legal System That Attenuate Patient Safety," De Paul Law Review, Law Review, 2019. [Online]. Available: https://via.library.depaul.edu/cgi/viewcontent.cgi?article=4081&context=law-review

[21] D. W. Meeks, M. W. Smith, L. Taylor, D. F. Sittig, J. M. Scott, and H. Singh, "An analysis of electronic health record-related patient safety concerns," *J Am Med Inform Assoc*, vol. 21, no. 6, pp. 1053–1059, Nov. 2014, doi: 10.1136/amiajnl-2013-002578.

[22] V. L. Foreman, F. M. Favaró, J. H. Saleh, and C. W. Johnson, "Software in military aviation and drone mishaps: Analysis and recommendations for the investigation process," *Reliability Engineering & System Safety*, vol. 137, pp. 101–111, May 2015, doi: 10.1016/j.ress.2015.01.006.

[23] M. Stram *et al.*, "Logical Observation Identifiers Names and Codes for Laboratorians," *Archives of Pathology & Laboratory Medicine*, vol. 144, no. 2, pp. 229–239, Feb. 2020, doi: 10.5858/arpa.2018-0477-RA.

[24] A. B. Carter *et al.*, "Electronic Health Records and Genomics," *The Journal of Molecular Diagnostics*, vol. 24, no. 1, pp. 1–17, Jan. 2022, doi: 10.1016/j.jmoldx.2021.09.009.
[25] Centers for Disease Control and Prevention (CDC), "COVID-19 Pandemic Response, Laboratory Data Reporting: CARES Act Section 18115."
[26] S. Vanderhook and J. Abraham, "Unintended Consequences of EHR Systems: A Narrative Review," *Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care*, vol. 6, no. 1, pp. 218–225, Jun. 2017, doi: 10.1177/2327857917061048.
[27] Anne Paxton, "Skirting the pitfalls of merging lab results," *CAP Today*, May 2018. [Online]. Available: https://www.captodayonline.com/skirting-pitfalls-merging-lab-results/
[28] D. Armbruster and J. Donnelly, "Harmonization of Clinical Laboratory Test Results: The Role of the IVD Industry," *EJIFCC*, vol. 27, no. 1, pp. 37–47, Feb. 2016.
[29] D. F. Sittig, D. R. Murphy, M. W. Smith, E. Russo, A. Wright, and H. Singh, "Graphical display of diagnostic test results in electronic health Records: a comparison of 8 systems," *Journal of the American Medical Informatics Association*, vol. 22, no. 4, pp. 900–904, Jul. 2015, doi: 10.1093/jamia/ocv013.
[30] S. Sabutsch, A. Mense, and S. Sauermann, "Development of a nationwide harmonized interoperable laboratory report based on CDA for the Austrian Electronic Health Record System," *Journal on Information Technology in Healthcare*, vol. 7, pp. 353–362, Oct. 2009.
[31] G. Koerbin, K. A. Sikaris, G. R. D. Jones, J. Ryan, M. Reed, and J. Tate, "Evidence-based approach to harmonised reference intervals," *Clinica Chimica Acta*, vol. 432, pp. 99–107, May 2014, doi: 10.1016/j.cca.2013.10.021.
[32] G. H. White, C. A. Campbell, and A. R. Horvath, "Is This a Critical, Panic, Alarm, Urgent, or Markedly Abnormal Result?," *Clinical Chemistry*, vol. 60, no. 12, pp. 1569–1570, Dec. 2014, doi: 10.1373/clinchem.2014.227645.
[33] H. Singh and D. F. Sittig, "Toward Electronic Medical Record Alerts That Consume Less Physician Time—Reply," *JAMA Internal Medicine*, vol. 173, no. 18, p. 1756, Oct. 2013, doi: 10.1001/jamainternmed.2013.9317.
[34] K. S. Lau-Min *et al.*, "Real-world integration of genomic data into the electronic health record: the PennChart Genomics Initiative," *Genetics in Medicine*, vol. 23, no. 4, pp. 603–605, Apr. 2021, doi: 10.1038/s41436-020-01056-y.
[35] M. S. Williams *et al.*, "Genomic Information for Clinicians in the Electronic Health Record: Lessons Learned From the Clinical Genome Resource Project and the Electronic Medical Records and Genomics Network," *Front. Genet.*, vol. 10, p. 1059, Oct. 2019, doi: 10.3389/fgene.2019.01059.
[36] N. Walton, B. Heale, and C. Formea, "Clinical decision support methods and infrastructure," in *Clinical Decision Support for Pharmacogenomic Precision Medicine*, Elsevier, 2022, pp. 109–130. doi: 10.1016/B978-0-12-824453-1.00001-4.
[37] M. Murugan *et al.*, "Genomic considerations for FHIR®; eMERGE implementation lessons," *Journal of Biomedical Informatics*, vol. 118, p. 103795, Jun. 2021, doi: 10.1016/j.jbi.2021.103795.
[38] R. S. Gammal, L. A. Berenbrok, P. E. Empey, and M. B. Massart, "Documenting Pharmacogenomic Test Results in Electronic Health Records: Practical Considerations for Primary Care Teams," *JPM*, vol. 11, no. 12, p. 1296, Dec. 2021, doi: 10.3390/jpm11121296.
[39] T. O'Neill *et al.*, "ISPOR, the FDA, and the Evolving Regulatory Science of Medical Device Products," *Value in Health*, vol. 22, no. 7, pp. 754–761, Jul. 2019, doi: 10.1016/j.jval.2019.03.020.
[40] E. Baumfeld Andre *et al.*, "The Current Landscape and Emerging Applications for Real-World Data in Diagnostics and Clinical Decision Support and its Impact on Regulatory Decision Making," *Clin Pharma and Therapeutics*, vol. 112, no. 6, pp. 1172–1182, Dec. 2022, doi: 10.1002/cpt.2565.
[41] Forum on Drug Discovery, Development, and Translation, Board on Health Sciences Policy, Health and Medicine Division, and National Academies of Sciences, Engineering, and Medicine, *Real-World Evidence Generation and Evaluation of Therapeutics: Proceedings of a Workshop*. Washington, D.C.: National Academies Press, 2017, p. 24685. doi: 10.17226/24685.
[42] Interoperability Standards Advisory, "Exchange InVitro Diagnostics (IVD) Orders and Results." ONC. [Online]. Available: https://www.healthit.gov/isa/exchange-invitro-diagnostics-ivd-orders-and-resultshttps://www.healthit.gov/isa/exchange-invitro-diagnostics-ivd-orders-and-results
[43] I. S. Kohane *et al.*, "What Every Reader Should Know About Studies Using Electronic Health Record Data but May Be Afraid to Ask," *J Med Internet Res*, vol. 23, no. 3, p. e22219, Mar. 2021, doi: 10.2196/22219.

[44] C. Uchegbu and X. Jing, "The potential adoption benefits and challenges of LOINC codes in a laboratory department: a case study," *Health Inf Sci Syst*, vol. 5, no. 1, p. 6, Dec. 2017, doi: 10.1007/s13755-017-0027-8.

[45] M.-C. Lin, D. J. Vreeman, C. J. McDonald, and S. M. Huff, "Correctness of Voluntary LOINC Mapping for Laboratory Tests in Three Large Institutions," *AMIA Annu Symp Proc*, vol. 2010, pp. 447–451, Nov. 2010.

[46] A. Bhargava, T. Kim, D. B. Quine, and R. G. Hauser, "A 20-Year Evaluation of LOINC in the United States' Largest Integrated Health System," *Archives of Pathology & Laboratory Medicine*, vol. 144, no. 4, pp. 478–484, Apr. 2020, doi: 10.5858/arpa.2019-0055-OA.

[47] A. Metke-Jimenez, J. Steel, D. Hansen, and M. Lawley, "Ontoserver: a syndicated terminology server," *J Biomed Semant*, vol. 9, no. 1, p. 24, Dec. 2018, doi: 10.1186/s13326-018-0191-z.

[48] J. Shivers, J. Amlung, N. Ratanaprayul, B. Rhodes, and P. Biondich, "Enhancing narrative clinical guidance with computer-readable artifacts: Authoring FHIR implementation guides based on WHO recommendations," *Journal of Biomedical Informatics*, vol. 122, p. 103891, Oct. 2021, doi: 10.1016/j.jbi.2021.103891.

[49] A. K. Sari, "Identification and Formal Representation of Change Operations in LOINC Evolution," *ijacsa*, vol. 10, no. 1, 2019, doi: 10.14569/IJACSA.2019.0100170.

[50] A. K. Sari, W. Rahayu, and M. Bhatt, "An approach for sub-ontology evolution in a distributed health care enterprise," *Information Systems*, vol. 38, no. 5, pp. 727–744, Jul. 2013, doi: 10.1016/j.is.2012.03.006.

[51] A. B. Carter, M. E. De Baca, H. S. Luu, W. S. Campbell, and M. N. Stram, "Use of LOINC for interoperability between organisations poses a risk to safety," *The Lancet Digital Health*, vol. 2, no. 11, p. e569, Nov. 2020, doi: 10.1016/S2589-7500(20)30244-2.

[52] A. Khalifa *et al.*, "A qualitative investigation of biomedical informatics interoperability standards for genetic test reporting: benefits, challenges, and motivations from the testing laboratory's perspective," *Genetics in Medicine*, vol. 23, no. 11, pp. 2178–2185, Nov. 2021, doi: 10.1038/s41436-021-01301-y.

[53] M. C. Lin, D. J. Vreeman, C. J. McDonald, and S. M. Huff, "Auditing consistency and usefulness of LOINC use among three large institutions – Using version spaces for grouping LOINC codes," *Journal of Biomedical Informatics*, vol. 45, no. 4, pp. 658–666, Aug. 2012, doi: 10.1016/j.jbi.2012.01.008.

[54] X. Zhu, J.-W. Fan, D. M. Baorto, C. Weng, and J. J. Cimino, "A review of auditing methods applied to the content of controlled biomedical terminologies," *Journal of Biomedical Informatics*, vol. 42, no. 3, pp. 413–425, Jun. 2009, doi: 10.1016/j.jbi.2009.03.003.

[55] R. A. Cholan *et al.*, "Encoding laboratory testing data: case studies of the national implementation of HHS requirements and related standards in five laboratories," *Journal of the American Medical Informatics Association*, vol. 29, no. 8, pp. 1372–1380, Jul. 2022, doi: 10.1093/jamia/ocac072.

[56] S. Palojoki, T. Pajunen, K. Saranto, and L. Lehtonen, "Electronic Health Record-Related Safety Concerns: A Cross-Sectional Survey of Electronic Health Record Users," *JMIR Med Inform*, vol. 4, no. 2, p. e13, May 2016, doi: 10.2196/medinform.5238.

[57] S. Menon, H. Singh, A. N. D. Meyer, E. Belmont, and D. F. Sittig, "Electronic health record-related safety concerns: A cross-sectional survey," *Journal of Healthcare Risk Management*, vol. 34, no. 1, pp. 14–26, Jul. 2014, doi: 10.1002/jhrm.21146.

[58] C. Robichaux, M. Tietze, F. Stokes, and S. McBride, "Reconceptualizing the Electronic Health Record for a New Decade: A Caring Technology?," *Advances in Nursing Science*, vol. 42, no. 3, pp. 193–205, Jul. 2019, doi: 10.1097/ANS.0000000000000282.

[59] K. T. Adams, T. C. Kim, A. Fong, J. L. Howe, K. M. Kellogg, and R. M. Ratwani, "Responding to health information technology reported safety events: Insights from patient safety event reports," *Journal of Patient Safety and Risk Management*, vol. 24, no. 3, pp. 118–124, Jun. 2019, doi: 10.1177/2516043519847330.

[60] D. K. Vawdrey and G. Hripcsak, "Publication bias in clinical trials of electronic health records," *Journal of Biomedical Informatics*, vol. 46, no. 1, pp. 139–141, Feb. 2013, doi: 10.1016/j.jbi.2012.08.007.

[61] "About The ONC Health IT Certification Program," *Office of the National Coordinator for Health IT*, Nov. 09, 2021. https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program (accessed Aug. 29, 2023).

[62] D. Raths, "LOINC-SNOMED Collaboration Called 'Major Breakthrough,'" *Healthcare Innovation*, Nov. 01, 2022. https://www.hcinnovationgroup.com/interoperability-hie/standards/news/21285785/loincsnomed-collaboration-called-major-breakthrough (accessed Aug. 29, 2023).

[63] "What is HL7 and why does healthcare need it? - Orion Health." https://orionhealth.com/global/blog/what-is-hl7-and-why-does-healthcare-need-it (accessed Aug. 29, 2023).

[64] Office of the Commissioner, "What does FDA regulate?," *FDA*, Oct. 07, 2022. https://www.fda.gov/about-fda/fda-basics/what-does-fda-regulate (accessed Aug. 29, 2023).

[65] "FDA Fundamentals," *FDA*, Jun. 28, 2021. https://www.fda.gov/about-fda/fda-basics/fda-fundamentals (accessed Aug. 29, 2023).
[66] "510(k) Clearances," *FDA*, Aug. 16, 2023. https://www.fda.gov/medical-devices/device-approvals-denials-and-clearances/510k-clearances (accessed Aug. 29, 2023).
[67] C. for D. and R. Health, "FDA's Role in Regulating Medical Devices," *FDA*, Aug. 18, 2023. https://www.fda.gov/medical-devices/home-use-devices/fdas-role-regulating-medical-devices (accessed Aug. 29, 2023).
[68] "About the Digital Health Center of Excellence," *Center for Devices and Radiological Health*, Sep. 22, 2020. https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence (accessed Aug. 29, 2023).
[69] "CDC Organization," *CDC*, Feb. 21, 2023. https://www.cdc.gov/about/organization/cio.htm (accessed Aug. 29, 2023).
[70] "How CDC Laboratories Protect Americans," *Centers for Disease Control and Prevention*, Apr. 07, 2022. https://www.cdc.gov/labs/protecting-america.html (accessed Aug. 29, 2023).
[71] "What is the Data Modernization Initiative?," *CDC*, Feb. 23, 2023. https://www.cdc.gov/surveillance/data-modernization/basics/what-is-dmi.html (accessed Aug. 29, 2023).
[72] Office of Public Health Scientific Services, "Informatics and Data Science," *CDC*, Nov. 2018. https://www.cdc.gov/csels/dls/informaticsdatascience.html (accessed Aug. 29, 2023).
[73] "Newborn Screening Quality Assurance Program (NSQAP)," *CDC*, Mar. 08, 2023. https://www.cdc.gov/labstandards/nsqap.html (accessed Aug. 29, 2023).
[74] "What are respective roles of ONC and OCR regarding privacy and security?," *Office of the National Coordinator for Health IT*, Jul. 07, 2023. https://www.healthit.gov/faq/what-are-respective-roles-onc-and-ocr-regarding-privacy-and-security (accessed Aug. 29, 2023).
[75] "ONC HITECH Programs | HealthIT.gov," *Office of the National Coordinator for Health IT*. https://www.healthit.gov/topic/onc-hitech-programs (accessed Aug. 29, 2023).
[76] "Centers for Medicare and Medicaid Services (CMS)," *USAGov*. https://www.usa.gov/agencies/centers-for-medicare-and-medicaid-services (accessed Aug. 29, 2023).
[77] A. Baker, "New CMS Rules Advancing Interoperability," *Health IT Buzz*, Feb. 27, 2023. https://www.healthit.gov/buzz-blog/health-it-policy/new-cms-rules-advancing-interoperability (accessed Aug. 29, 2023).
[78] "Clinical Laboratory Improvement Amendments (CLIA)," *CMS*, May 11, 2023. https://www.cms.gov/regulations-and-guidance/legislation/clia (accessed Aug. 29, 2023).
[79] "NIH Almanac," *National Institutes of Health (NIH)*, Jul. 09, 2015. https://www.nih.gov/about-nih/what-we-do/nih-almanac/national-library-medicine-nlm (accessed Aug. 29, 2023).
[80] "The Executive Branch," *The White House*. https://www.whitehouse.gov/about-the-white-house/our-government/the-executive-branch/ (accessed Aug. 29, 2023).
[81] Assistant Secretary for Public Affairs, "About HHS," *HHS.gov*, Feb. 03, 2015. https://www.hhs.gov/about/index.html (accessed Aug. 29, 2023).
[82] Digital Communications Division, "HHS Organizational Charts Office of Secretary and Divisions," *HHS*, Oct. 24, 2008. https://www.hhs.gov/about/agencies/orgchart/index.html (accessed Aug. 29, 2023).
[83] "Federal Budgeting." https://www.gao.gov/federal-budgeting (accessed Sept. 25, 2023).
[84] "Information and Regulatory Affairs," *The White House*. https://www.whitehouse.gov/omb/information-regulatory-affairs/ (accessed Aug. 29, 2023).
[85] FDA, "FDA Human Drug Review and Approval Basics Unit List: Introduction to FDA Human Drug Review and Approval Basics," *CDER World*. https://www.accessdata.fda.gov/scripts/cderworld/index.cfm?action=humandrugreview:main&unit=1&lesson=1&topic=4 (accessed Aug. 29, 2023).
[86] "MEDICARE PROMOTING INTEROPERABILITY PROGRAM HARDSHIP EXCEPTION FACT SHEET," CMS, 2022. [Online]. Available: https://www.cms.gov/files/document/medicare-pi-program-hardship-exception-fact-sheet-2023-04-06.pdf
[87] M. Quinn *et al.*, "Electronic Health Records, Communication, and Data Sharing: Cchallenges and Opportunities for improving the diagnostic process," *Diagnosis (Berl)*, vol. 6, no. 3, pp. 241–248, Aug. 2019, doi: 10.1515/dx-2018-0036.
[88] A. Gupta *et al.*, "Mind the overlap: how system problems contribute to cognitive failure and diagnostic errors," *Diagnosis*, vol. 5, no. 3, pp. 151–156, Sep. 2018, doi: 10.1515/dx-2018-0014.

[89] H. Singh *et al.*, "Timely Follow-Up of Abnormal Diagnostic Imaging Test Results in an Outpatient Setting: Are Electronic Medical Records Achieving Their Potential?," *Arch Intern Med*, vol. 169, no. 17, pp. 1578–1586, Sep. 2009, doi: 10.1001/archinternmed.2009.263.
[90] "Wrong-Record, Wrong-Data Errors with Health IT Systems," ECRI Institute, 2015. [Online]. Available: Wrong-Record, Wrong-Data Errors with Health IT Systems
[91] H. Singh *et al.*, "Improving follow-up of abnormal cancer screens using electronic health records: trust but verify test result communication," *BMC Med Inform Decis Mak*, vol. 9, p. 49, Dec. 2009, doi: 10.1186/1472-6947-9-49.
[92] J. L. Howe, K. T. Adams, A. Z. Hettinger, and R. M. Ratwani, "Electronic Health Record Usability Issues and Potential Contribution to Patient Harm," *JAMA*, vol. 319, no. 12, pp. 1276–1278, Mar. 2018, doi: 10.1001/jama.2018.1171.
[93] C. S. Caldwell and S. C. Denne, "Rigorous and consistent evaluation of diagnostic tests in children: another unmet need," *Pediatr Res*, vol. 88, no. 4, Art. no. 4, Oct. 2020, doi: 10.1038/s41390-020-01110-0.
[94] S. Posnack and E. S. Anthony, "Certification Program Updates to Support Efficiency & Reduce Burden," *Health IT Buzz*, Sep. 21, 2017. https://www.healthit.gov/buzz-blog/healthit-certification/certification-program-updates-support-efficiency-reduce-burden (accessed Jul. 18, 2023).
[95] D. F. Sittig, J. S. Ash, and H. Singh, "The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records," *Am J Manag Care*, vol. 20, no. 5, pp. 418–423, May 2014.
[96] J. Ash, H. Singh, and D. Sittig, "Test Results Reporting and Follow-Up SAFER Guide," ONC, Nov. 2016. [Online]. Available: https://www.healthit.gov/sites/default/files/safer_test_results_reporting.pdf
[97] "2022 ONC Report to Congress," ONC, 2022. [Online]. Available: https://www.healthit.gov/sites/default/files/page/2023-02/2022_ONC_Report_to_Congress.pdf
[98] "Medicare EHR Incentive Program Attestation Patterns | HealthIT.gov." https://www.healthit.gov/data/quickstats/medicare-ehr-incentive-program-attestation-patterns (accessed Jul. 19, 2023).
[99] "Medicare Promoting Interoperability Program Frequently Asked Questions (FAQs)."
[100] "Management Challenge 6: The Meaningful and Secure Exchange and Use of Electronic Health Information." https://oig.hhs.gov/reports-and-publications/top-challenges/2014/challenge06.asp (accessed Jul. 20, 2023).

Appendix A - List of Key Informants

We would like to thank the regulators, laboratorians, medical practitioners, health IT analysts, terminologists, payors, medical device industry subject matter experts, patient safety advocates, and accrediting agency representatives who have participated in this research, including, but not limited to:

W. Scott Campbell, PhD, MBA
Associate Professor
Peter C. Hinrichs Endowed Chair of Informatics
Director of Public Health Laboratory Informatics & Pathology Laboratory Informatics
Dept of Pathology/Microbiology
University of Nebraska Medical Center

James T. Case, MS, DVM, PhD, FACMI
Chief Terminologist
SNOMED International

Raja Cholan, MS
Health Informaticist
Deloitte Consulting, LLP

Andrea Englund, MBA, MSN, RN
Bioinformatics Research Manager, Dept. of Microbiology & Pathology
University of Nebraska Medical Center

Carol Geary, PhD, MBA, RN

Aaron Green, PhD
General Manager, North America
Labgnostic, Inc.

Eza Hafeza, MD
Director, Terminology Services and Operations
LOINC & Health Data Standards
Regenstrief Institute

Jason Hall, BS
Public Health Informaticist
Deloitte Consulting, LLP

Ross Koppel, PhD, FACMI, FAIHSI
Professor of Biomedical Informatics
University of Pennsylvania and University at Buffalo (SUNY)

S.J. Lange, Caregiver and Patient Advocate

Chris LeMaster, MD, MPH
Emergency Physician
Hospital Patient Safety Lead

Riki Merrick, MPH
Terminologist

Sandra Mitchell, RPh, MSIS, FASHP, FAMIA

Viet Nguyen, MD
Chief Standards Implementation Officer
HL7® International

Andrea Pitkus, PhD, MLS(ASCP)CM, FAMIA
Medical Laboratory Professional

Steven Posnack, MS, MHS
Deputy National Coordinator for Health IT
Office of the National Coordinator for Health Information Technology

Marjorie Rallins, DPM
Executive Director
LOINC & Health Data Standards
Regenstrief Institute

Paul Seville, MD, MBI, CPHIMS
Physician, Biomedical Information
Deloitte Consulting, LLP

Walter Sujansky, MD, PhD
Informatics consultant and subject matter expert for FDA SHIELD Program

Tina Vitale-McDowell, RN
Director, Emergency Department

Steven Wagers
Associate Director, Technical Services and Operations
LOINC & Health Data Standards
Regenstrief Institute

Greg Watkins, Jr., BSc
Senior HL7 Interoperability SME
GPS / CBO / Health Technology
Deloitte Consulting, LLP

Susan Winckler, RPh, Esq.
CEO, Reagan-Udall Foundation for the FDA

Dan Wyman, MD, MPH
Chief Medical Officer, Synensys, LLC

Appendix B – Controller Descriptions

- **Data Layer:** The data layer includes the physical devices and infrastructure used to send, transmit, and receive laboratory data. This includes IVD devices, which exchange test order and test result data with laboratory information systems (LISs). The LIS typically contains a database that stores the data, as well as a user interface that a laboratorian uses to access the data. Data stored within the LIS can be transmitted to other health information technology (HIT) systems, such as an electronic health record (EHR) system belonging to a care facility. The care facility EHR/HIT system also contains a database and a user interface through which a medical practitioner can insert or access health data.
- **Patient:** The patient is the individual receiving care, for whom the laboratory tests are conducted. Patients receive information about procedures they must follow for diagnostic testing from medical practitioners or laboratories, and may contact them to provide personal information, report new symptoms, or ask for clarification about testing procedures or treatment. Patients may directly provide the laboratory with the sample for laboratory testing, or the sample may be collected by a medical practitioner. Once the laboratory test is conducted, patients may be able to directly access their test results within a care facility's EHR/HIT system through a patient portal, and those results may be shown to them in a raw or processed (trended) format. Patients can also update their own personal information through the portal, as well as make or modify appointments for consultation, treatment, or diagnostic testing. Patients interacting directly with IVD devices (such as at-home test kits) can also voluntarily report issues with the devices to the FDA through the MedWatch platform.
- **Medical Practitioner:** Medical practitioners (e.g., clinicians) interact directly with patients in the form of consultations, ordering and interpreting diagnostic tests, collecting test samples, and providing treatment/care. Medical practitioners provide instructions to patients about the procedures they must follow to ensure accurate results of a laboratory test, and to ensure their treatment progresses as intended. In turn, they collect information from patients, including their clinical history or symptoms observed. Practitioners may operate independently, or as part of a larger care facility, and are typically subject to the procedures and policies in place at that facility. Practitioners usually interact with an EHR/HIT system to input patient information, order tests, and access test results. That EHR/HIT system may also provide clinical decision support (CDS) to aid the practitioner in providing the best care for the patient. Though policies differ at different institutions, medical practitioners encountering errors or adverse events may report those instances to the care facility administration, or directly to the FDA through the MedWatch platform. Practitioners are also credentialed by payors and may receive additional coverage from the Centers for Medicare and Medicaid Services (CMS) for having achieved a set of interoperability metrics when it comes to using EHRs/HIT systems.
- **Laboratory:** Laboratories are the facilities where the diagnostic testing within scope of this study takes place. Laboratories acquire and maintain in vitro diagnostic (IVD) devices, which they use to analyze the samples collected by medical practitioners for diagnostic testing. Though policies also differ at different institutions, laboratories encountering issues with IVD devices may report those issues to the manufacturer, or directly to the FDA through the MedWatch platform. Laboratories also acquire and maintain laboratory information systems, through which they receive, process, and store test orders from care facilities and medical practitioners, and share test results back to them. Laboratories update LISs following releases of new reference terminologies, messaging standards, or software functionality provided by the LIS vendor. Laboratories are also responsible for testing their LISs following updates and after the initial installation. Laboratory operations are regulated by CMS through the Clinical Laboratory Improvement Amendments (CLIA), whose requirements are typically enforced and expanded upon by accreditation and quality organizations like the College of American Pathologists (CAP). Laboratories are also required to report diagnostic data to public health agencies (PHAs) according to standards provided by those agencies.
- **Care Facility:** Care facilities are the institutions (e.g., hospitals or clinics) where patients go to receive medical care. Care facilities acquire and maintain EHR systems, through which they store and access patient clinical and billing data, as well as submit diagnostic test orders and receive the associated test results. Care facility IT teams update EHRs following releases of new reference terminologies, messaging standards, or software functionality provided by the EHR vendor. Part of the responsibilities of maintaining EHR systems include mapping local codes to reference terminologies for processing of diagnostic test orders and results. Care facilities are also responsible for testing their EHRs following updates and after the initial installation. The care facility administration provides instructions and procedures to the medical practitioners that work there, as well as process any reports about errors or adverse events observed and reported. Those reports can be addressed

internally or escalated to regulatory bodies or EHR vendors. Like laboratories, care facilities are also required to report diagnostic data to PHAs according to standards provided by those agencies.

- **EHR/HIT Companies and LIS Companies:** EHR/HIT companies, along with LIS companies, provide software resources that care facilities and laboratories use to manage healthcare data. These companies provide software tools to their customers, as well as support for building, maintaining, and testing the tools. Customers may share particular needs or requirements with HIT companies, who then work with the customer to modify the default implementation of a software tool (known as the "model system") to fit the customer's particular use case. Customers may also report problems with HIT systems to HIT companies, who may address the issue directly or require the customer to address it themselves. HIT companies developing systems for use in care facilities (like EHRs) may have their systems certified according to the ONC's certification criteria outlined in the final rule of the 21st Century Cures Act. Utilization of certified EHR systems is required in order for care facilities to receive certain funding incentives from CMS.
- **IVD Manufacturers/Importers:** IVD manufacturers develop and market in vitro diagnostic devices that laboratories use to run tests. IVD manufacturers must obtain approval for all IVD devices from the FDA through one of several pathways before a device may be used in a commercial laboratory. Manufacturers are also subject to quality control mechanisms from the FDA and are required to report to the FDA any complaints they may have received of device malfunctions, serious injuries or deaths associated with medical devices. In such cases, the FDA may issue corrective action to the manufacturer, or the manufacturer may voluntarily recall products that present a risk of injury. When laboratories acquire IVD devices, manufacturers also provide instructions on how the devices should be used. IVD importers act as representatives of IVD manufacturers that are based outside the United States. Manufacturers based outside the United States must still meet applicable U.S. regulations in order to import devices into the country. IVD importers are also required to report to the FDA any complaints they may have received of device malfunctions, serious injuries or deaths associated with medical devices.
- **Laboratory/Personnel Accreditation Organizations:** Laboratory and personnel accreditation organizations are independent organizations that act on behalf of government agencies to provide certification and accreditation to different components of the laboratory data ecosystem. Examples include the College of American Pathologists (CAP), American Society for Clinical Pathology (ASCP), among others. These organizations accredit laboratories and laboratory personnel based on requirements imposed by regulation, such as the Clinical Laboratory Improvement Amendments (CLIA). Requirements imposed by laboratory and personnel accreditation organizations must be at least equivalent to regulatory requirements but are often more stringent.
- **EHR/HIT Certification Organizations:** EHR/HIT certification organizations are third-party entities that work under the purview of the ONC to test and certify electronic health record (EHR) and health information technology (IT) products and services [61]. These organizations, known as ONC-Authorized Certification Bodies (ONC-ACBs), are authorized by the ONC to make certification decisions and conduct surveillance on HIT companies. HIT certification organizations may also receive reports from users of HIT systems regarding potential safety risks or violations of certification criteria.
- **Naming, Coding, and Messaging Standards Development Organizations (LOINC, SNOMED, HL7, etc.):** Naming, coding, and messaging (NCM) standards development organizations (SDOs) create standards to support interoperability of electronic data between healthcare systems. Each organization has a different focus. Organizations like the Regenstrief Institute and SNOMED International develop particular terminology standards for representing medical concepts, like LOINC (Logical Observation Identifiers Names and Codes) and SNOMED CT (Systemized Nomenclature of Medicine-Clinical Terms). These organizations may collaborate to further standardize terminologies, such as a recent agreement to develop a LOINC extension that will create both LOINC and SNOMED CT codes for all concepts that are shared between the terminologies [62]. HL7 (Health Level Seven) provides a common language around content and structures for clinical data classes (e.g. diagnoses, allergies, procedures) [63]. There are many other naming, coding, and messaging organizations, but this report will focus on LOINC, SNOMED, and HL7. These organizations periodically release updates of their standards, to be utilized by HIT companies, care facilities and laboratories. Users of laboratory data standards may request new reference terminology codes through the standards organization's website portals.
- **Payors:** Payors in the U.S. laboratory data ecosystem include Preferred Provider Organizations (PPOs), Health Maintenance Organizations (HMOs), healthcare service contractors, state insurance agencies, claim handlers,

and others. Payors enter into data sharing agreements with care facilities, medical practitioners, and laboratories (recipients). For the payors to send payments, the recipients (care facilities, medical practitioners, and laboratories) need to send petitions for coverage, claims, performance reports, and accreditation status. Recipients are required to be accredited to receive payment. Based on what they decide to pay, Payors influence the access to care that a patient will receive. CMS is the largest payor for healthcare in the U.S. and may provide additional funding to payors that meet a set of quality criteria imposed by CMS.

- **Public Health Agencies:** Public health agencies (PHAs) are official agencies established by a state or local government for the purpose of maintaining the health of their population by providing certain environmental health, medical, and sometimes therapeutic services. PHAs impose particular requirements on laboratories within their jurisdiction to report test results and disease patterns.
- **FDA:** The Food and Drug Administration (FDA) is an operating division of HHS. It consists of the Office of the Commissioner and four directorates overseeing the core functions of the agency. The FDA regulates foods, drugs, biologics, medical devices, electronic products that give off radiation, cosmetics, veterinary products, and tobacco products [64]. The FDA interprets laws given by Congress and carries out (regulates) the intent of those laws. The FDA will sometimes send out guidance to the industry to clarify certain aspects of the laws. FDA guidance is not legally binding [65]. The FDA approves medical devices through the 510(k) clearance process before manufacturers can sell them in the U.S [66]. The FDA monitors the ongoing safety and efficacy of regulated medical devices through MedWatch, the FDA Safety Information and Adverse Event Reporting Program [67]. They also conduct audits on approved devices and require recalls, injunctions, and seizure notices on devices that are discovered to be unsafe or ineffective. They also send out import alerts on devices that are manufactured outside the U.S. when necessary. The FDA's Digital Health Center of Excellence (DHCoE) provides regulatory advice and support to the FDA's regulatory review of digital health technology [68].
- **CDC:** The Centers for Disease Control and Prevention (CDC) is an Operating division of the HHS. The CDC fights disease and supports communities and citizens to do the same. The CDC is the United States government's health protection agency. It CDC conducts critical science and provides health information to protect the U.S. against health threats and responds when threats arise [69]. The CDC has over 200 laboratories across the U.S. that specialize in research, surveillance, and reference diagnostic testing [70]. The CDC launched the Data Modernization Initiative in 2020 [71]. CDC's Division of Laboratory Systems Informatics and Data Science Branch develops, maintains, and evaluates informatics and data science approaches to strengthening laboratory information systems for improved clinical and public health outcomes. This includes coordination of regional and national systems, reporting of laboratory diagnostic information to electronic health records, decision-making tools for healthcare providers, research and application of laboratory-related data, and informatics solutions for improved laboratory management, practice, and emergency preparedness [72]. The CDC may also serve as a reference laboratory for particular tests, and may conduct proficiency testing on laboratories to maintain the quality and accuracy of particular types of results, such as newborn screening [73].
- **ONC:** The Office of the National Coordinator for Health Information Technology (ONC) operates under the Office of the Secretary of HHS, to support the adoption of health information technology and the promotion of nationwide, standards-based health information exchange to improve healthcare. ONC develops regulations for the certification of HIT systems, engages public input, and implements grant programs, such as those to initiate state health information exchanges and the Regional Extension Centers that provide technical assistance to reach meaningful use of EHRs [74], [75]. The ONC authorizes ONC-ACBs to make certification decisions and conduct surveillance on HIT companies. The ONC may also receive reports from users of HIT systems regarding potential safety risks or violations of certification criteria.
- **CMS:** The Centers for Medicare and Medicaid Services (CMS) is an Operating division of the HHS. The CMS provides health coverage to more than 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace. CMS seeks to strengthen and modernize the United States' healthcare system, to provide access to high quality care and improved health at lower costs [76]. CMS works closely with the Office of the National Coordinator for HIT (ONC) for the purpose of health data interoperability with the Medicare Promoting Interoperability Program [77]. CMS regulates all laboratory testing (except research) performed on humans in the U.S. through the Clinical Laboratory Improvement Amendments (CLIA) to ensure quality laboratory testing [78]. The CMS authorizes laboratory accreditation organizations to perform inspections and accredit laboratories according to their own set of requirements, as long as those requirements are equivalent or more stringent than those imposed by CLIA. The CMS also sets

particular quality assurance standards, which other payors must meet in order to receive additional funding from CMS.

- **Reference Libraries:** Reference libraries are government agencies who curate and release compendia of healthcare terminology, including the National Library of Medicine (NLM) or the National Cancer Institute (NCI), both a part of the National Institutes of Health (NIH). NLM is the world's largest biomedical library and aims to make biomedical data and information more accessible. NLM enables researchers, clinicians, and the public to use the vast wealth of biomedical data to improve health [79]. NLM publishes the Unified Medical Language System (UMLS), which integrates and distributes key terminology, classification and coding standards, and associated resources to promote creation of more effective and interoperable biomedical information systems and services, including electronic health records.
- **Department of Health and Human Services (HHS) Administration:** HHS is responsible for the day-to-day enforcement and administration of federal health laws [80]. The mission of the U.S. Department of Health and Human Services (HHS) is to enhance the health and well-being of all Americans by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services [81]. The HHS has twelve Operating divisions, including the Centers for Disease Control and Prevention (CDC), the Centers for Medicare and Medicaid Services (CMS), the Food and Drug Administration (FDA), and the National Institutes of Health. The Office of the National Coordinator for HIT (ONC) is also under the authority of the HHS, listed under the Office of the Secretary [82]. HHS provides administrative oversight of the FDA and other HHS divisions. The leadership structure within HHS determines, assigns, and enforces the responsibilities of the different operating divisions and offices within the department.
- **The White House:** The White House is responsible for implementing and enforcing the laws written by Congress. The White House also appoints the Cabinet, which is composed of the heads of the 15 federal agencies, including HHS. The President submits to Congress the recommended budget for the federal agencies [83]. The White House Office of Information and Regulatory Affairs (OIRA), an agency within the Executive Office of the President, reviews draft proposed and final regulations [84].
- **Congress:** Congress creates and passes the laws that give the Department of Health and Human Services (HHS), the Food and Drug Administration (FDA), and other healthcare-associated federal regulatory agencies their authority [85]. Congress may pass down legal requirements, funding allocations, and determinations of responsibilities to regulatory agencies (such as those under HHS) and their affiliates. Congress also provides its opinion on healthcare-associated regulations.

Appendix C – Complete list of UCAs

This list of unsafe control actions includes all UCAs identified during the course of this study. The 42 UCAs shown in Table 3 are indicated with a number, an asterisk and are highlighted.

Controller: Medical Practitioner

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide treatment to patient	**UCA:** Medical practitioner does not provide treatment when patient needs treatment to avoid harm	**UCA:** Medical practitioner provides treatment when patient does not need any treatment **UCA-1*:** Medical practitioner provides treatment that does not match the patient's condition	**UCA-2*:** Medical practitioner provides treatment too late to avoid patient harm **UCA:** Medical practitioner provides treatment too early before patient condition has been identified	**UCA:** Medical practitioner stops providing treatment too early before patient condition has been resolved **UCA:** Medical practitioner provides treatment for too long after patient condition has been resolved
Communicate laboratory pre-test instructions or test procedures to patient	**UCA:** Medical practitioner does not communicate laboratory pre-test instructions or test procedures to patient when specific actions are required from patient and patient has not already received that information	**UCA:** Medical practitioner communicates laboratory pre-test instructions or test procedures to patient in a language/terminology patient does not understand **UCA:** Medical practitioner communicates laboratory pre-test instructions or test procedures in a way that is not repeatedly accessible to patient (not in writing, etc.)	**UCA:** Medical practitioner communicates laboratory pre-test instructions or test procedures to patient too early before test will be conducted **UCA:** Medical practitioner communicates laboratory pre-test instructions or test procedures too close to when test is being conducted	N/A

Medical Practitioner (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Communicate laboratory pre-test instructions or test procedures to patient (continued)		**UCA:** Medical practitioner communicates laboratory pre-test instructions or test procedures that patient is incapable of following **UCA:** Medical practitioner communicates incorrect laboratory pre-test instructions or test procedures to patient **UCA:** Medical practitioner communicates incomplete laboratory pre-test instructions or test procedures to patient **UCA:** Multiple medical practitioners communicate conflicting laboratory pre-test instructions or test procedures to patient		
Collect patient specimen	**UCA:** Medical practitioner does not collect patient specimen that is needed for a test	**UCA:** Medical practitioner collects incorrect patient specimen that is needed for a test **UCA:** Medical practitioner collects specimen from incorrect patient	**UCA:** Medical practitioner collects patient specimen too soon before test needs to be run **UCA:** Medical practitioner collects patient specimen too late after sample was requested	**UCA:** Medical practitioner stops collecting patient specimen too soon before full specimen has been collected **UCA:** Medical practitioner continues collecting patient specimen for too long after full specimen has been collected

Medical Practitioner (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Collect patient specimen (continued)		**UCA:** Medical practitioner follows incorrect procedure in collecting patient specimen **UCA:** Medical practitioner collects patient specimen when patient has not followed test requirements **UCA:** Medical practitioner harms patient during specimen collection	**UCA:** Medical practitioner collects patient sample too late after patient conditions change **UCA:** Medical practitioner collects patient specimen too early before patient conditions change	
Label patient specimen	**UCA:** Medical practitioner does not label patient specimen that is needed for a test	**UCA:** Medical practitioner labels patient specimen with incorrect description of sample **UCA:** Medical practitioner labels specimen with one patient's name when sample belongs to another patient **UCA:** Medical practitioner labels specimen without following proper labeling procedure	**UCA:** Medical practitioner labels patient specimen too late after specimen has been collected	N/A
Enter patient data into HIT system	**UCA:** Medical practitioner does not enter new patient data into HIT system when patient communicates new data with them	**UCA:** Medical practitioner enters incorrect patient data into HIT system	**UCA:** Medical practitioner enters patient data into HIT system too late after data has been obtained	**UCA:** Medical practitioner stops entering patient data in HIT system too soon before full set of data has been entered

Medical Practitioner (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Enter patient data into HIT system (continued)	**UCA:** Medical practitioner does not enter new patient data into HIT system when patient condition has changed	**UCA:** Medical practitioner enters incomplete patient data into HIT system **UCA:** Medical practitioner enters patient data into HIT system under one patient's name when data belongs to another patient		
Order laboratory test	**UCA:** Medical practitioner does not order laboratory test when patient needs that test to diagnose/monitor a condition	**UCA:** Medical practitioner orders laboratory test when patient does not need that test to diagnose/monitor a condition **UCA-3*:** Medical practitioner orders laboratory test that is not the best/most appropriate test to diagnose a disorder/disease **UCA-4*:** Medical practitioner orders laboratory test that is not covered by patient's health insurance **UCA-5*:** Medical practitioner orders laboratory test for patient that has already been done	**UCA:** Medical practitioner orders laboratory test too late after it is determined that patient needs that test to diagnose/monitor a condition **UCA:** Medical practitioner orders laboratory test too early before it is determined that patient needs that test to diagnose/monitor a condition	**UCA:** Medical practitioner stops ordering laboratory test too soon before order has been completed

Medical Practitioner (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Order laboratory test (continued)		**UCA:** Medical practitioner orders laboratory test without providing necessary clinical context (e.g., ask at order entry questions) about patient **UCA:** Medical practitioner orders test from laboratory when laboratory does not offer that test **UCA:** Medical practitioner orders test that patient cannot complete		

Controller: Laboratory/Care Facility

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Update HIT system	**UCA-6*:** Laboratory/care facility does not update HIT system when safety-critical HIT system update is released	**UCA:** Laboratory/care facility updates HIT system without following correct update procedures **UCA-7*:** Laboratory/care facility updates HIT system to version that is incompatible with other systems **UCA:** Laboratory/care facility updates only one of multiple modules of a HIT system that depend on each other **UCA:** Laboratory/care facility updates HIT system without directly informing system users of implications of update	**UCA:** Laboratory/care facility updates HIT system too late after update is released **UCA:** Laboratory/care facility initiates HIT system update outside of scheduled timeslot	**UCA:** Laboratory/care facility stops HIT system update too soon before update is complete
Update reference terminology in HIT system	**UCA-8*:** Laboratory/care facility does not update reference terminology in HIT system when safety-critical reference terminology update is released.	**UCA:** Laboratory/care facility updates reference terminology in HIT system without following correct update procedures **UCA:** Laboratory/care facility updates reference terminology in HIT system to version that is incompatible with other systems	**UCA:** Laboratory/care facility updates reference terminology in HIT system too late after update is released	N/A

Laboratory/Care Facility (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Update reference terminology in HIT system (continued)		**UCA:** Laboratory/care facility updates reference terminology in HIT system without directly informing system users of implications of update		
Map local codes to reference terminology	**UCA-9*:** Laboratory/care facility does not map local codes to reference terminology when safety-critical reference terminology update is released	**UCA-10*:** Laboratory/care facility maps local codes to reference terminology incorrectly/ inconsistently	**UCA:** Laboratory maps local codes to reference terminology too late after reference terminology is released and local codes are already in use	N/A
Enable software feature in HIT system	**UCA-11*:** Laboratory/care facility does not enable safety-critical software feature on HIT system	**UCA:** Laboratory/care facility enables only one of multiple modules of a HIT system that depend on each other **UCA:** Laboratory/care facility enables functionality in a HIT system that overrides safety controls **UCA:** Laboratory/care facility enables functionality in a HIT system that is not meant to be used in a specific context	N/A	N/A

Controller: Laboratory

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Calibrate IVD devices	**UCA:** Laboratory does not calibrate IVD devices when they lose calibration	**UCA:** Laboratory calibrates IVD devices to incorrect setting	**UCA:** Laboratory calibrates IVD devices while time critical samples are waiting to be processed **UCA:** Laboratory calibrates IVD devices before device update is complete	**UCA:** Laboratory stops calibration routine on IVD devices before routine is complete
Transfer laboratory results to ordering practitioner's HIT system	**UCA:** Laboratory does not transfer laboratory results to ordering practitioner's HIT system	**UCA:** Laboratory transfers laboratory result to ordering practitioner's HIT system without necessary data elements **UCA:** Laboratory transfers laboratory result to ordering practitioner's HIT system using invalid/ inconsistent message structure **UCA:** Laboratory transfers laboratory result to ordering practitioner's HIT system using invalid/ inconsistent reference terminology **UCA:** Laboratory transfers laboratory result to ordering practitioner's HIT system in unstructured format (e.g., as a PDF)	**UCA:** Laboratory transfers laboratory result to ordering practitioner's HIT system too soon before realizing test results contained inaccuracies	N/A

Laboratory (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Run laboratory test	**UCA:** Laboratory does not run test ordered by physician	**UCA:** Laboratory runs test without following appropriate test procedures **UCA:** Laboratory runs test on inadequate specimen **UCA:** Laboratory runs test on uncalibrated IVD device **UCA:** Laboratory runs test that does not match test ordered	**UCA:** Laboratory runs test too late after test order is received **UCA:** Laboratory runs test too late after specimen is received **UCA:** Laboratory runs test too early before necessary patient information is received **UCA:** Laboratory runs test too early before calibration routine is complete	**UCA:** Laboratory stops running test before results are obtained

Controller: Care Facility

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Acquire an EHR system	**UCA-12*:** Care facility does not acquire an EHR system when patient data needs to be shared electronically from other facilities or laboratories	**UCA:** Care facility acquires a non-certified EHR system	**UCA:** Care facility does not acquire an EHR system too late after patient data would have needed to be shared electronically from other facilities or laboratories	N/A
Provide operational procedures/ policies to medical practitioners	**UCA:** Care facility does not provide updated procedures/policies to medical practitioners following a HIT system update **UCA:** Care facility does not provide updated procedures/policies to medical practitioners following change in facility operations/logistics **UCA:** Care facility does not provide updated procedures/policies to medical practitioners following change in test availability or protocol (ref. ranges, etc.)	**UCA:** Care facility provides incorrect procedures/policies to medical practitioners following an HIT system update, change in facility operations/logistics, or change in test availability/ protocol **UCA:** Care facility provides incomplete procedures/ policies to medical practitioners following an HIT system update, change in facility operations/logistics, or change in test availability/ protocol	**UCA:** Care facility provides procedures/ guidelines to medical practitioners too late following an HIT system update, change in facility operations/ logistics, or change in test availability/ protocol	N/A
Assign laboratory result messages for manual review	**UCA:** Care facility team does not assign laboratory result messages for manual review that cannot be automatically interpreted by HIT systems	**UCA:** Care facility team assigns laboratory result messages for manual review without informing the appropriate stakeholders that need to review the results	**UCA:** Care facility team assigns laboratory result messages for manual review too late after receiving message	N/A

Care Facility (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Assign laboratory result messages for manual review (continued))		**UCA:** Care facility team assigns laboratory result messages for manual review in a system that is inaccessible to the people assigned to review it		

Controller: HIT Company

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Release HIT system update	**UCA-13*:** HIT company does not release HIT system update following safety-critical reports from customers	**UCA:** HIT company releases HIT system update that does not sufficiently address error reports from customers **UCA-14*:** HIT company releases HIT system update that has been insufficiently tested **UCA:** HIT company releases HIT system update without providing sufficient build support for customers **UCA:** HIT company releases HIT system update without informing customers of the implications of updating or not updating	**UCA:** HIT company releases HIT system update too late after receiving error reports from customers	N/A
Provide build support and maintenance for HIT system customers	**UCA-15*:** HIT company does not provide sufficient build support or maintenance when customer does not have the resources to build or maintain HIT System	**UCA:** HIT company provides incomplete build support or maintenance to customers	**UCA:** HIT company provides build support and maintenance for HIT system customers too late after systems would need to be built/maintained (e.g., after hospital has already done it themselves)	**UCA:** HIT company stops providing build support and maintenance to customer before system is operating as intended

HIT Company (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Roll back HIT system update	**UCA:** HIT company does not roll back HIT system update that included safety-critical flaws	**UCA:** HIT company rolls back HIT system update that included safety-critical functionality without providing alternatives to enforce safety controls	**UCA-16*:** HIT company rolls back HIT system update with safety-critical flaws too late after update is released	N/A
Require non-disclosure agreement from HIT system customers	**UCA:** HIT company does not require non-disclosure agreement to customers regarding patient data stored in HIT system (potential for patient privacy concerns)	**UCA:** HIT company requires non-disclosure agreement to customers regarding safety outcomes of HIT systems	N/A	**UCA:** HIT company requires non-disclosure agreement to customers regarding safety outcomes of HIT systems for too long after safety concerns have been identified by customers
Select data standards to implement in HIT system	**UCA:** HIT company does not select a particular set of data standards to implement in HIT system	**UCA-17*:** HIT company selects data standard that is not compatible with data standards used in HIT systems from competitors	N/A	N/A

Controller: CMS

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Set laboratory safety and certification requirements (CLIA)	**UCA:** CMS does not set requirement for preventing a particular safety-critical issue in laboratory ecosystem	**UCA:** CMS sets laboratory safety and certification requirements that are too stringent for laboratories to realistically comply with (e.g., requiring electronic reporting even for labs that do not possess electronic reporting systems) **UCA:** CMS sets laboratory safety and certification requirements that do not consider safety-critical issues (e.g., test naming conventions, test context)	**UCA:** CMS sets laboratory safety and certification requirements too late after laboratories are already performing a particular practice	N/A
Provide approval for laboratory based on CLIA criteria	**UCA:** CMS does not approve laboratory that is compliant with CLIA criteria at the requested level	**UCA:** CMS approves laboratory that is not compliant with CLIA criteria at the requested level **UCA:** CMS approves laboratory without performing appropriate inspections or delegating it to an approved body	**UCA:** CMS approves laboratory that is compliant with CLIA criteria too late after compliance is demonstrated **UCA:** CMS approves laboratory too early before compliance with CLIA criteria is demonstrated	**UCA:** CMS maintains approval for laboratory for too long after non-compliance with CLIA criteria has been discovered
Inspect/audit laboratory	**UCA:** CMS does not inspect/audit laboratory that is not complying with CLIA requirements	**UCA:** CMS selects only a limited subset of test cases for which to inspects/audits laboratory	**UCA:** CMS inspects/audits laboratory too late after scheduled inspection/audit date	N/A

CMS (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Inspect/audit laboratory (continued)	**UCA:** CMS does not inspect/audit laboratory that is not being inspected/ audited by a CMS-approved accreditation program		**UCA:** CMS inspects/audits laboratory too late after significant change in laboratory equipment/ procedures	
Provide approval for laboratory /personnel accreditation organizations	**UCA:** CMS does not approve an accreditation organization whose capabilities are equal or greater than those of CMS	**UCA:** CMS approves an accreditation organization whose capabilities are not equal or greater than those of CMS **UCA:** CMS approves an accreditation organization whose individual criteria do not satisfy CLIA criteria	N/A	N/A
Change requirements for "Promoting Interoperability" participants to avoid a negative payment adjustment	**UCA:** CMS does not change requirements that are no longer relevant for current HIT systems	**UCA-18*:** CMS changes requirements for "Promoting Interoperability" participants in a way that negatively impacts safety outcomes for program participants	**UCA:** CMS changes requirements too early before users can adopt necessary changes **UCA:** CMS changes requirements too late after funding requirements that no longer become relevant for current HIT systems	N/A
Provide hardship exception for "Promoting Interoperability" program participant	**UCA:** CMS does not provide a hardship exception for a requirement that has been deemed too stringent for care facilities to comply with	**UCA-19*:** CMS provides a hardship exception for a requirement that allows hospitals to operate EHRs with known safety risks [86].	**UCA:** CMS provides a hardship exception for a requirement too late after the requirement is deemed too stringent for care facilities to comply with	N/A

CMS (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide negative payment adjustment to care facility	**UCA-20*:** CMS does not provide negative payment adjustment to care facility that did not meet funding requirements and is using systems that do not meet minimum safety requirements	**UCA:** CMS provides negative payment adjustment to care facility that meets all funding requirements	N/A	**UCA:** CMS provides interoperability incentive funding for too long to care facility that did not meet funding requirements

Controller: ONC

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Adopt technical standards in HIT certification criteria	**UCA:** ONC does not adopt technical standards in HIT certification criteria when standards would be useful for sharing of laboratory data	**UCA:** ONC adopts technical standards in HIT certification criteria that are too stringent for HIT systems to realistically comply with **UCA:** ONC adopts technical standards in HIT certification criteria that do not fulfill needs of HIT system customers **UCA-21*:** ONC adopts technical standards in HIT certification criteria that are insufficient to create interoperable HIT systems	**UCA-22*:** ONC adopts technical standards in HIT certification criteria too late after HIT systems are already deployed	N/A
Certify EHR as meeting current certification requirements	**UCA:** ONC does not certify EHR that meets current certification requirements	**UCA-23*:** ONC certifies EHR that does not meet current certification requirements	N/A	**UCA:** ONC maintains certification for too long for an EHR that no longer meets current certification requirements

Controller: FDA

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Approve IVD device	**UCA:** FDA does approve an IVD device that is adequate or better than other IVD devices available on the market	**UCA-24*:** FDA approves an IVD device that does not perform to expected performance levels	**UCA:** FDA takes too long to give approval for a device for which there is no adequate replacement in the market	**UCA:** FDA maintains approval for too long of an IVD device that does not perform to expected performance levels
Issue corrective action to IVD manufacturer	**UCA:** FDA does not issue corrective action to IVD manufacturer following a series of inappropriate results from IVD device	**UCA:** FDA issues corrective action to IVD manufacturer whose device is performing according to regulation	**UCA-25*:** FDA issues corrective action to IVD manufacturer too late following a series of inappropriate results from IVD device	**UCA:** FDA issues corrective action to IVD manufacturer for too long following the resolution of a problem with an IVD device
Audit/inspect IVD manufacturer	**UCA:** FDA does not audit an IVD manufacturer whose IVD devices do not perform to expected performance levels	**UCA:** FDA audits a manufacturer that has safe practices (wastes time on FDA and lab)	**UCA:** FDA audits an IVD manufacturer too late after significant changes have occurred in IVD regulation	N/A
Require post-market performance study on IVD device	**UCA:** FDA does not require a post-market performance study of an IVD device whose results are used for high-risk diagnoses	**UCA:** FDA requires excessive post-market performance study of IVD devices whose results are not used for high-risk diagnoses	**UCA:** FDA requires a post-market performance study of an IVD device too late after the device's results have begun being used for high-risk diagnoses	**UCA:** FDA does not complete a post-market performance study of an IVD device whose results are used for high-risk diagnoses

Controller: IVD Manufacturer/Importer

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Issue recall of IVD device	**UCA:** IVD manufacturer does not issue recall of IVD device that does not perform to expected performance levels	**UCA:** IVD manufacturer issues recall on device that performs to expected performance levels and for which there is no adequate replacement in the market	**UCA:** IVD manufacturer does issues recall of IVD device that does not perform to expected performance levels too late after performance problems are detected	**UCA:** IVD manufacturer lifts recall of IVD device too soon before the resolution of a problem with the device **UCA:** IVD manufacturer does not lift recall of IVD device following the resolution of a problem with the device
Release IVD device and associated procedures	**UCA:** IVD manufacturer does not release IVD test to laboratories for which there is no adequate replacement in the market	**UCA:** IVD manufacturer releases device that has been insufficiently tested on particular demographics (e.g., children) **UCA:** IVD manufacturer releases device that was approved with inadequate validation data	**UCA:** IVD manufacturer releases device too soon before sufficient testing has been performed on particular demographics (e.g., children)	N/A
Release IVD device updates	**UCA:** IVD manufacturer does not release IVD device update following safety-critical reports from device users	**UCA:** IVD manufacturer releases IVD device updates that renders device incompatible with other systems or procedures in place at a laboratory **UCA:** IVD manufacturer releases IVD device updates that do not sufficiently address safety-critical reports from device users	**UCA:** IVD manufacturer provides IVD device updates too frequently such that device users cannot keep up to date **UCA:** IVD manufacturer releases IVD device updates too late after receiving safety-critical reports from device users	N/A

IVD Manufacturer/Importer (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Associate IVD device output to reference terminology codes	**UCA-26*:** IVD manufacturer does not associate device output to reference terminology codes when device output needs to be shared with external facilities	**UCA:** IVD manufacturer associates device output to reference terminology codes incorrectly or inconsistently as compared to manufacturers of equivalent devices	**UCA:** IVD manufacturer associates device output to reference terminology codes too late after device output would need to be shared with external facilities	N/A

Controller: Payor

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide coverage/ reimbursement for laboratory test	**UCA-27*:** Payor does not provide coverage for a laboratory test that may provide value to an individual patient's case	N/A	**UCA:** Payor provides coverage for diagnostic test that is needed to diagnose a patient's condition too late after coverage is requested	**UCA:** Payor stops providing coverage for a series of diagnostic tests that is needed to diagnose a patient's condition before all necessary results are obtained
Provide data sharing agreement to provider/ laboratory	**UCA:** Payor does not provide data sharing agreement to provider/laboratory that shares patient data with them	**UCA:** Payor provides data sharing agreement that does not include all data that payor needs to meet quality criteria **UCA:** Payor provides data sharing agreement to provider/ laboratory that provider/ laboratory cannot fulfill	N/A	N/A
Provide additional preventative healthcare/well-being services to patients	**UCA:** Payor does not provide additional preventative healthcare/well-being services that may provide value to an individual patient's case	N/A	N/A	**UCA-28*:** Payor stops providing additional preventative healthcare/well-being services that patients are actively utilizing

Controller: Naming/Coding/Messaging (NCM) Standards Development Organizations (SDOs) & Reference Libraries

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Create/release new reference terminology	**UCA:** SDO does not create/release new reference terminology after a new type of diagnostic test is developed **UCA:** SDO does not create/release new reference terminology after a new disease/ condition is identified **UCA:** SDO does not create/release new reference terminology when requested by stakeholder (lab, practitioner, etc.)	**UCA-30*:** SDO creates/releases reference terminology or messaging standard that does not sufficiently standardize communication between users. **UCA:** SDO creates/releases reference terminology that conflicts or overlaps with existing terminology **UCA:** SDO creates/releases reference terminology without appropriate implementation documentation	**UCA-29*:** SDO creates/releases new reference terminology too late after a new type of diagnostic test is developed or disease/ condition is identified	**UCA:** SDO stops providing updates for outdated reference terminology standard when some facilities still utilize the standard
Create new data messaging standards	**UCA:** SDO does not create a new data messaging standard format when the current standard format is insufficient to capture results from new laboratory tests	**UCA:** SDO creates additional data messaging standard formats when the current standard format is sufficient to capture results from laboratory tests **UCA:** SDO creates additional data messaging standard formats when a different SDO has already created a sufficient standard	**UCA:** SDO creates a new data messaging standard format too late after safety-critical changes in the laboratory data ecosystem are released	
Provide release notes for reference terminology update	**UCA:** SDO does not provide release notes for safety-critical reference terminology update	**UCA:** SDO provides incomplete or ambiguous release notes for safety-critical reference terminology update	**UCA:** SDO provides release notes too late after releasing safety-critical reference terminology update	N/A

Naming/Coding/Messaging (NCM) Standards Development Organizations (SDOs) and Reference Libraries (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide release notes for reference terminology update (continued)		**UCA:** SDO provides release notes that do not emphasize safety-criticality of reference terminology update **UCA:** SDO provides release notes without guidelines for how to perform safety-critical reference terminology update **UCA:** SDO provides release notes without informing customers of the implications of adopting or not adopting a reference terminology update		
Provide reference terminology mapping guidelines	**UCA:** SDO does not provide reference terminology mapping guidelines following safety-critical terminology release	**UCA-31*:** SDO provides conflicting or ambiguous reference terminology mapping guidelines following safety-critical terminology release **UCA:** SDO provides incomplete reference terminology mapping guidelines following safety-critical terminology release	**UCA:** SDO provides reference terminology mapping guidelines too late after safety-critical terminology release	N/A
Provide messaging standard implementation guides	**UCA:** SDO does not provide messaging standards implementation guides following safety-critical messaging standards update	**UCA-32*:** SDO provides conflicting or ambiguous implementation guides following safety-critical messaging standards update	**UCA:** SDO provides messaging standards implementation guides too late after safety-critical messaging standards update	N/A

Naming/Coding/Messaging (NCM) Standards Development Organizations (SDOs) and Reference Libraries (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
		UCA: SDO provides implementation guides without two-way communication with implementers following safety-critical messaging standards update		

Controller: Patient

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Follow laboratory pre-test instructions or test procedures	**UCA-33*:** Patient does not follow laboratory pre-test instructions or test procedures when procedures are necessary for validity of test results (e.g., does not fast, etc.)	**UCA:** Patient follows incorrect laboratory pre-test instructions or test procedures when procedures are necessary for validity of test results **UCA:** Patient follows laboratory pre-test instructions or test procedures when those procedures can harm their health	**UCA:** Patient follows laboratory pre-test instructions or test procedures too soon before test is to be conducted, when timing of procedures is crucial for validity of test results **UCA:** Patient follows laboratory pre-test instructions or test procedures too late before test is to be conducted, when timing of procedures is crucial for validity of test results	**UCA:** Patient stops following laboratory pre-test instructions or test procedures too soon before test is to be conducted, when timing of procedures is crucial for validity of test results
Access test results	**UCA:** Patient does not access test results when test results are not directly communicated to them by their medical practitioner	**UCA:** Patient accesses wrong person's test results **UCA:** Patient accesses wrong test result (e.g. test from the wrong date, etc.)	**UCA:** Patient accesses test results too late after their condition has changed	N/A
Make/attend laboratory appointment	**UCA-34*:** Patient does not make/attend laboratory appointment when laboratory results are necessary to inform care plan	**UCA:** Patient makes/attends laboratory appointment for wrong test	**UCA:** Patient makes/ attends laboratory appointment too late after laboratory results would be necessary to inform care plan	N/A

Controller: CDC/PHAs

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Set standards for reporting of diagnostic data from laboratories	**UCA:** CDC/PHAs do not set standards for reporting diagnostic data from laboratories when data needs to be aggregated for use by the agencies	**UCA-35*:** CDC/PHAs set standards for reporting of diagnostic data that laboratories are unable to comply with **UCA:** CDC and different PHAs set conflicting standards for reporting of diagnostic data from laboratories	**UCA:** CDC/PHAs do set standards for reporting diagnostic data too late after laboratories have already implemented other standards	N/A
Provide healthcare guidance	**UCA:** CDC/PHAs do not provide healthcare guidance that may provide value to patients' cases	**UCA-36*:** CDC/PHAs provide healthcare guidance that conflicts with current/previous guidance **UCA:** CDC/PHAs provide health guidance that is too stringent for institutions or individuals to follow	**UCA:** CDC/PHAs do provide healthcare guidance too late after data is received **UCA:** CDC/PHAs do provide healthcare guidance too early before sufficient data is received	**UCA:** CDC/PHAs remove healthcare guidance when the guidance is still relevant for patient safety outcomes **UCA:** CDC/PHAs maintain healthcare guidance when it is no longer relevant for patient safety outcomes

Controller: Laboratory/Personnel Accreditation Organization

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Provide accreditation to laboratory	**UCA:** Laboratory accreditation organization does not accredit laboratory that is compliant with CLIA criteria at the requested level **UCA:** Laboratory accreditation organization does not accredit laboratory when that laboratory is the only facility capable of performing a necessary test	**UCA:** Laboratory accreditation organization accredits laboratory that is not compliant with CLIA criteria at the requested level **UCA:** Laboratory accreditation organization accredits laboratory without performing appropriate inspections or delegating it to an approved body **UCA-37*:** Laboratory accreditation organization provides accreditation to laboratory without being able to enforce minimum interoperability requirements	**UCA:** Laboratory accreditation organization accredits laboratory that is compliant with CLIA criteria too late after compliance is demonstrated **UCA:** Laboratory accreditation organization accredits laboratory too early before compliance with CLIA criteria is demonstrated	**UCA:** Laboratory accreditation organization maintains accreditation for laboratory for too long after non-compliance with CLIA criteria has been discovered
Inspect/audit laboratory	**UCA:** Laboratory accreditation organization does not inspect/audit laboratory that is not complying with CLIA requirements **UCA:** Laboratory accreditation organization does not inspect/audit laboratory that is not being inspected/ audited by a CMS-approved accreditation program	**UCA:** Laboratory accreditation organization inspects/audits laboratory for compliance with incomplete set of CLIA requirements	**UCA:** Laboratory accreditation organization inspects/audits laboratory too late after scheduled inspection/audit date **UCA:** Laboratory accreditation organization inspects/audits laboratory too late after change in laboratory equipment/procedures	**UCA:** Audit ends too early to collect sufficient information

***Controller*: Department of Health and Human Services (HHS) Administration**

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Determine responsibilities of component agencies	**UCA-38*:** HHS does not give any agency responsibility over safety-critical component of laboratory data ecosystem **UCA:** HHS does not assign responsibility to a new agency when regulatory need is outside the scope of an existing agency	**UCA-39*:** HHS assigns agencies overlapping regulatory responsibilities **UCA:** HHS assigns responsibility to a new agency when regulatory need is within the scope of an existing agency	N/A	**UCA:** HHS removes safety-critical responsibility from agency without reassigning it **UCA:** HHS assigns a responsibility for longer than is relevant and helpful (resource waste)

Controller: Congress/White House

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Update Federal regulatory authority's statutory boundary	**UCA:** Congress/ White House do not update a Federal regulatory authority's statutory boundary when it is insufficient to enforce safety control loops	**UCA-40*:** Congress/White House update a Federal regulatory authority's statutory boundary in a way that removes components that were critical for safe control loop design **UCA:** Congress/ White House update a Federal regulatory authority's statutory boundary too frequently, causing confusion regarding regulatory scope	**UCA:** Congress/ White House update a Federal regulatory authority's statutory boundary too soon after another regulatory boundary change **UCA:** Congress/ White House update a Federal regulatory authority's statutory boundary too late after it is deemed insufficient to enforce safety control loops	N/A
Expand Federal regulatory authorities' statutory boundaries	**UCA-41*:** Congress/the White House do not expand federal regulatory agencies' statutory boundary to cover technologies that have emerged or undergone significant changes since previous statutory boundaries were enacted.	**UCA:** Congress/ White House expand the statutory boundary of multiple regulatory agencies to cover the same regulatory gap in a way that is not meaningfully different **UCA-42*:** Congress/White House expands regulatory authority's statutory boundaries in a way that diminishes the safety of the regulated industry	**UCA:** Congress/the White House expand federal regulatory agencies' statutory boundary too late after technologies have emerged or undergone significant changes since previous statutory boundaries were enacted	N/A
Allocate funding to HHS and component agencies	**UCA:** Congress/White House do not allocate sufficient funding to agencies whose services support safety-critical processes (or their oversight)	N/A	N/A	**UCA:** Congress stops issuing funding to agencies whose services support safety-critical processes (or their oversight)

Congress/White House (continued)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Allocate funding to HHS and component agencies (continued)	**UCA:** Congress/White House do not issue sufficient funding for agencies to address safety-critical reports			

Appendix D – Complete list of Loss Scenarios

This list of loss scenarios is categorized as A, B, and C, and are color-coded as follows:

Category	Explanation
A*	In scope, directly related to issues of laboratory data, high explanatory power, worth a deep dive
B	Generally in scope, contain data-related contributions but are primarily driven by out-of-scope elements, data-related components likely addressed in recommendations for mitigating A-level scenarios
C	Out of research scope, do not contain data-related contributions, but worth a mention for research completeness

*Some A-level scenarios include a visualization that traces the path of the scenario through the control structure and highlights the contributions of several controllers.

Controller: Medical Practitioner

Category/ Scenario #	Scenario Description
Control Action:	**Provide treatment to patient**
UCA Type:	**Providing causes hazard**
UCA:	**Medical practitioner provides treatment that does not match the patient's condition**
Scenario 1-1: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they did not have the diagnostic information to inform their mental model of the patient's condition. The diagnostic information may not be observed by the medical practitioner because they may be accustomed to using their routine process to access results in the EHR, which only displays laboratory data that has been previously mapped to the care facility's EHR system (e.g., mapped to a LOINC code or local code representation). In some cases, additional unmapped test results are shared by the laboratory as a PDF and the physician may not notice the PDF due to its lack of salience in the EHR process flow. Physicians who are not expecting and looking for the test results may not know to look for additional, unmapped information in a patient profile, particularly if the unmapped results were ordered by another physician or a long time ago. The results may have been shared as a PDF because they pertained to a new or uncommon test whose format could not be represented in the messaging standard available to that laboratory-care facility pair. Standards for new and complex tests (e.g., genomics) are not yet tightly constrained. See scenario 30-1 for a discussion of this. The results are able to be shared as PDFs because CLIA only requires that the data that is sent gets received, and it does not specify the method of transmission nor impose any requirement or confirmation that the information is observed by the medical practitioner. CLIA was drafted and approved in 1988, before EHRs were widely adopted and modifications to CLIA require Congressional approval.
Scenario 1-2: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the medical practitioner uses test result data that has been mapped incorrectly to the care facility's EHR system.

Category/ Scenario #	Scenario Description
	The practitioner may have ordered the test from the standard laboratory available to the care facility, but the test may actually have been conducted at a more specialized reference laboratory. The result may have been mapped incorrectly if the test was new and did not yet possess appropriate reference terminology, so the results were shared by the reference laboratory to the standard laboratory using local codes, and the local codes were mapped to the closest reference terminology available for transmission to the care facility. Standards for new and complex tests (e.g., genomics) are not yet tightly constrained. See scenario 31-1 for a discussion of this.
Scenario 1-3: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had insufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are not transferred into that patient's medical record. This may occur if the patient was unable to be associated with their medical record upon arrival at a care facility, such as if the patient is obtunded, cannot be identified, and a new medical record must be created for them. The patient's test results may be logged in a temporary record that is not later merged with the patient's permanent record.
Scenario 1-4: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had incorrect diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test result was influenced by the procedure used to conduct the diagnostic test on the laboratory and provider side. That may occur if the specimen was not collected or stored using the appropriate procedure/equipment. This may occur if the medical practitioner collecting and storing the patient specimen is unaware of additional restrictions beyond standard protocol at the facility, if the specimen collection facility does not have the package insert for diagnostic devices that will be used in the laboratory. This is able to occur because although CLIA does require that laboratories establish and follow procedures for specimen collection and transport [42 CFR 493.1242], laboratories often receive specimens with little information about how they were collected or stored.
Scenario 1-5: (C)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had incorrect diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test result was entered manually into the LIS, and this was done incorrectly (e.g., typo, wrong patient, etc.), because that specific test kit required manual resulting. The system may not be coded to flag if a manually entered test result appears outside the reasonable range for that test.
Scenario 1-6: (C)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had incorrect diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test result was influenced by the procedure used to conduct the test on the patient side. The patient may not have followed the appropriate procedures in preparation for the diagnostic test (fasting, etc.). This may have occurred due to a miscommunication of the test procedures to the patient, as a result of a language or literacy barrier.
Scenario 1-7: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had incorrect diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test result was influenced by the procedure used to conduct the test on the patient side. The patient may not have followed the appropriate procedures in preparation for the

Category/ Scenario #	Scenario Description
	diagnostic test (fasting, etc.). This may have occurred due to a miscommunication of the test procedures to the patient, as a result of an inability to access necessary instructions in written form through paper communications or a patient portal.
Scenario 1-8: (C)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had incorrect diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test result was inaccurate due to a design flaw in the test itself, or a sensitivity too low to detect the condition present. This may occur as a result of insufficient post-market surveillance or performance studies conducted on the test. See scenario 25-1 for a deeper discussion of post-market surveillance of devices.
Scenario 1-9: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had insufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the medical practitioner was unaware of additional clinical history of the patient or prior test results that were stored in a legacy system. If the care facility transitioned or is transitioning between HIT systems they may have applied one of the following conversion strategies: A) Converted all data, however the data could be in a different format or location in the new HIT system. B) The healthcare system may decide to do a partial conversion (e.g., 5 years of "X" type of results, 10 years of "Y" type of results, etc.). C) No conversion was done, and the legacy system remains the source of truth for historical results Currently, regulatory or statutory incentives are inadequate for HIT vendors of legacy systems to facilitate data transfers to new systems. Data conversions can be complicated because formats from one system to another can vary greatly.
Scenario 1-10: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had insufficient diagnostic information to inform their process model of the patient's condition. That may occur if the medical practitioner was unaware of additional clinical history of the patient or prior test results that were stored in a different representation (such as a local code) in their EHR. That may occur if a test or condition is new and cannot be represented in current reference terminology, so the care facility or laboratory must create a local code for it. It may also occur if the facility or laboratory has not yet mapped its local code to an appropriate standard that is recognized by the EHR. Once the reference terminology is released, results already stored with the local code may not be retroactively mapped to the terminology. The reference terminology for the test or condition may also have changed, and the care facility may be storing clinical history using deprecated terminology that will not trigger a response from a practitioner's query.
Scenario 1-11: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had insufficient diagnostic information to inform their process model of the patient's condition and treatment. That may occur if the clinical decision support provided by the EHR did not trigger to warn the practitioner of additional information that would be needed to inform treatment or of additional interventions needed based on existing information (such as laboratory results). That may occur if the reference terminology for a test or condition may has changed, and the care facility may be storing that data using deprecated terminology that will not trigger clinical decision support.
Scenario 1-12: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received inappropriate clinical decision

Category/ Scenario #	Scenario Description
	support from the EHR system. The clinical decision support may be inappropriate due to inappropriate coding of the condition or test result on which the decision support is acting. It may also be inappropriate if the system has not been updated to adequately address a change in the protocol for ordering a test result or diagnosing a condition.
Scenario 1-13: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the EHR automatically aggregated or trended test results that were obtained from different facilities with critical differences in interpretation such as reference ranges, units, or specific test methodology (e.g., specifying that a COVID-19 test was a PCR test vs. just indicating it as a generic, methodless COVID-19 test). Furthermore, results from different laboratories utilizing the same device may be reported as direct numeric instrument values or as a categorical interpretation of the numeric values (e.g., none, few, many). Each laboratory may use different bins or cutoffs to categorize numerical results, so qualitative categories may not be suitable to be charted/trended together. While CLIA regulations require that labs send appropriate reference ranges and units of measure, they do not specify a standard format for sharing this data. Furthermore, upon arrival at the care facility EHR, test result data are no longer under the purview of the interface regulations imposed by CLIA. Data in the care facility EHR are not subject to regulations that control how they may be automatically trended or aggregated. Additionally, there may be other uses of laboratory test results and their values (e.g., algorithms, displays used by health professionals other than the ordering practitioner) and regulatory requirements ensuring data elements are preserved across different internal HIT interfaces are inadequate.
Scenario 1-14: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the EHR aggregated (e.g., placed in the same field) noncomparable test results that were derived using different methodologies that have not been harmonized to give comparable results. That may occur if two different tests that use the same or similar approaches for different conditions are mapped to the same reference terminology (i.e., LOINC code, etc.). It may also occur if two tests that use different methodologies for the same condition are mapped to the same reference terminology. This could happen because mapping different formats is a manual process, subject to the interpretation of the individual mapper, who may be an IT professional rather than a medical professional. It may also be the other way around, where a medical professional without reference terminology experience is tasked with mapping codes following an update. Tests using different methodologies and producing noncomparable results may also be *appropriately* mapped to the same reference terminology, as the terminology structure may not support sufficient granularity to distinguish results performed on different noncomparable instrumentation. On the other hand, there can be multiple appropriate codes for a given test, so different users may not always select the same code. Implementation/mapping guidelines cannot anticipate every system and source data upon which the terminology or messaging standards would be implemented. Therefore, guidelines cannot provide specific mapping of proprietary data to standards. Inconsistent mapping is more likely to occur if implementers are unable to access support resources to clarify ambiguities in implementation/mapping guidelines or standards themselves.
Scenario 1-15: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the EHR presented the results of a confirmatory test in a different view than the original test ordered to

Category/ Scenario #	Scenario Description
	diagnose a condition. When the confirmatory test is reflexed (i.e., ordered by the testing laboratory based on the outcome of the first test) and is sent in a result message as a parent-child link, the EHR may not be able to retain that linkage and both results may not appear in the same view.
Scenario 1-16: (A)	The medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if the diagnostic information was provided through an HIE, using a different value set than what is defined in the exchange. That value set may have been translated into the required codes through translational fields, but the practitioner may not know how to check those fields for the appropriate codes, or the EHR may map the results automatically using the inappropriate codes.
Scenario 1-17: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received insufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are corrupted or information is lost during the transfer from the LIS to the EHR. This may occur due to a number of errors in the laboratory result message (e.g., wrong patient ID, test ID and result ID don't match, etc.) or if the result message is structured in a format the EHR cannot process (e.g., the result is for a new test with a nonstandard format). The message may be allowed to go through in this format because the care facility and laboratory chose to override the functionality that blocks an interface if a message cannot go through, so that results from new/uncommon tests are able to be shared. CLIA inspections that occur every two years may only consider some of the interfaces the LIS possesses and may not consider integrity of data shared to all systems (e.g., different HIT vendor, physician's office laboratory, etc.).
Scenario 1-18: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received insufficient diagnostic information available to inform their process model of the patient's condition. That may occur if different laboratory results for a single patient specimen are disconnected from each other. Result turnaround times may be delayed if a patient test order is split into multiple tests with varying turnaround times. Results of the tests are often delivered to the EHR in the order received and a physician may mistakenly think the order is complete even though one or more of the tests has not yet been resulted. This could happen between LIS systems of different laboratories in the case of referral testing or from the LIS to the care facility EHR.
Scenario 1-19: (A)	The medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that their mental model of the patient's condition was informed by diagnostic information presented in a misleading way. That may occur if laboratory results are corrupted, or information is lost in an interface engine software while being transmitted from an LIS to an EHR. CLIA and CAP accreditation do cover that messages arrive at the first downstream interfaced system appropriately. The interfaced system may be a care facility EHR, a public health system, data warehouse, ambulatory provider EHRs, etc. Internal interfaces between instruments, middleware, interface engines and other laboratory systems with the LIS are also checked. However, laboratories may miss problems with interface engines if verification tests are insufficient, especially after updates to laboratory tests and/or system software. A CLIA inspection may not catch the problem if that particular test is not selected for review during the inspection.

Category/ Scenario #	Scenario Description
Scenario 1-20: (C)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received insufficient diagnostic information to inform their process model of the patient's condition. That may occur if a test was conducted and results were interpreted with inaccurate clinical context (e.g., date of last drug administration, last menstrual period, etc.) about the patient. This may occur because the clinical context had to be self-reported, and the patient misreported that information. That might happen due to a patient not possessing their medication list, overall health literacy, etc.
Scenario 1-21: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received insufficient diagnostic information to inform their process model of the patient's condition. That may occur if a test was conducted and results were interpreted with inaccurate or insufficient clinical context (e.g., date of last drug administration, last menstrual period, etc.) about the patient. This may occur because the patient's prior medical history has been in another facility or state, and those non-affiliated institutions are unable to share that data due to issues of interoperability or data ownership/sharing rights.
Scenario 1-22: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they incorrectly interpreted the diagnostic information available to inform their process model of the patient's condition. That may occur if the medical practitioner received a test result relative to a new reference range or test methodology, without being aware of that change, and interpreted the result as they previously would have. Care facilities should have a process for notification to practitioners of a new or updated reference range, but due to the immense volume of alerts practitioners receive and the wide variety of laboratory tests that are available, the practitioner may not have necessarily updated their mental model after the notification.
Scenario 1-23: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they incorrectly interpreted the diagnostic information available to inform their process model of the patient's condition. That may occur if the medical practitioner received a test result from a different facility, without being informed that that result was not comparable to results produced in their care facility. This may occur if those results still appear in the patient's medical chart in the practitioner's EHR system, even if they were performed on different instrumentation with different reference ranges, units of measure, or sensitivity and specificity.
Scenario 1-24: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they were unaware of the best treatment options. This may be because the lack of good consistent healthcare data encoding of rare conditions makes it difficult for researchers and practitioners to understand how the existing data may compare in order to better inform care decisions. This could also be for conditions that are more common but better data availability could also inform better care opportunities. There is no regulatory authority on the part of the CDC to require that specific data elements be shared, so that they may provide better guidance to medical practitioners (e.g., knowing whether the patient was pregnant or not along with a Zika result).
Scenario 1-25: (A)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they received incorrect or insufficient diagnostic information available to inform their process model of the patient's condition. The diagnostic data may have been entered with missing fields that created a parentless node. Therefore, while the data was technically "in" the EHR, the physician does not know that the data exists and would have to use highly technical data querying tools to find it.

Category/ Scenario #	Scenario Description
	However, there is nothing to signal the physician that there is hidden data so the physician would not know to look for it even if they had the skills to do so.
Scenario 1-26: (B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they had insufficient diagnostic information available to inform their process model of the patient's condition. This might occur if additional diagnostic information was available but could not be shared with the medical practitioner or used for treatment decisions, because it was obtained through a test method that has not been certified for treatment (such as sequencing).
Scenario 1-27:(B)	A medical practitioner may provide treatment that does not match the patient's condition (UCA). One contributing factor may be that they were unable to ascertain the true condition of the patient. This may be because the physician was unable to look at multiple pieces of diagnostic data at the same time in an EHR display. It may have been difficult for the physician to remember critical pieces of information from one screen to another. This may allow physicians to miss trends and make it harder for them to connect information from different laboratories. Features may exist to help physicians make these decisions but physicians may not have the time or technology literacy to learn them. [87]

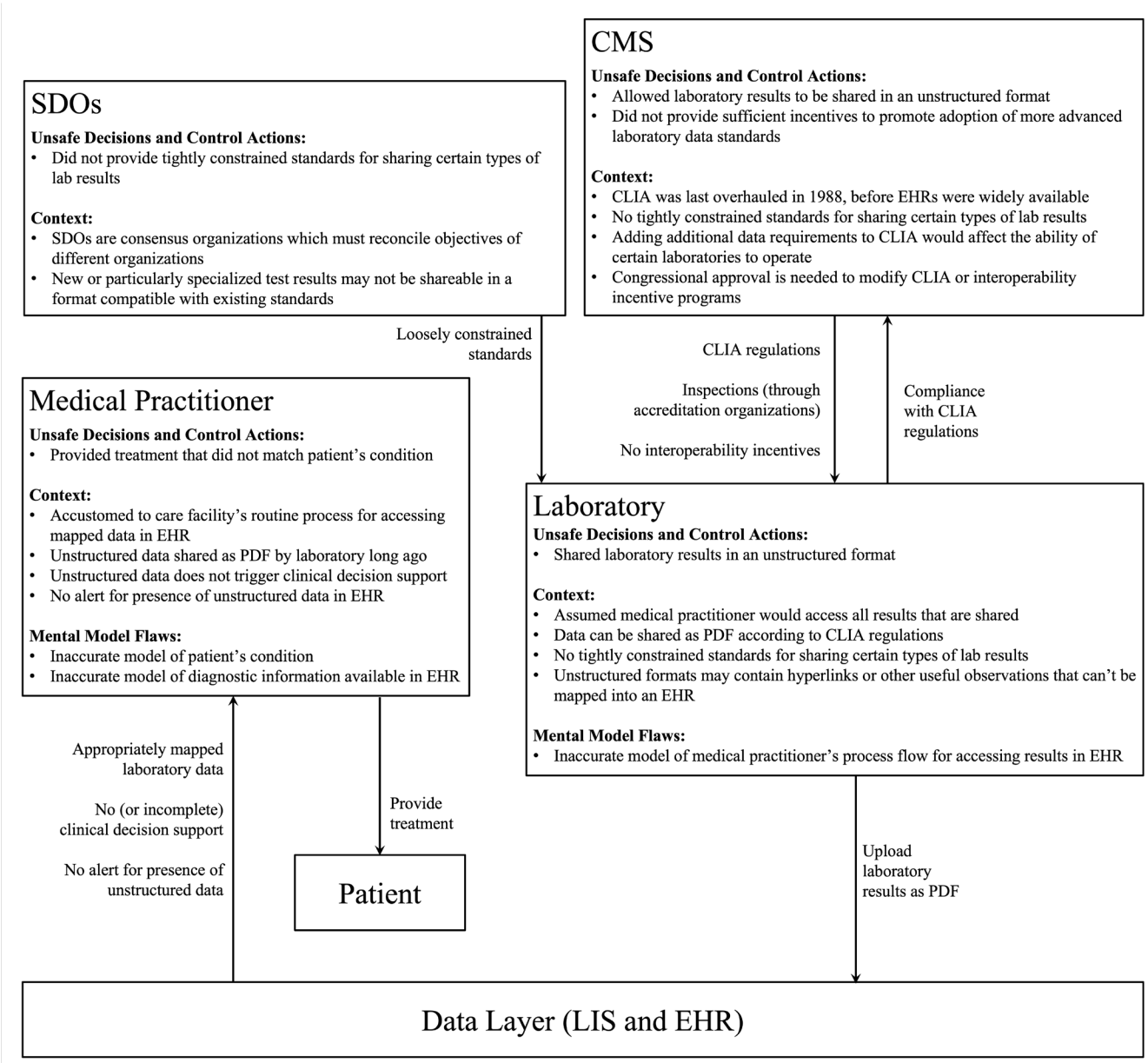

Figure 10. Visualization of scenario 1-1

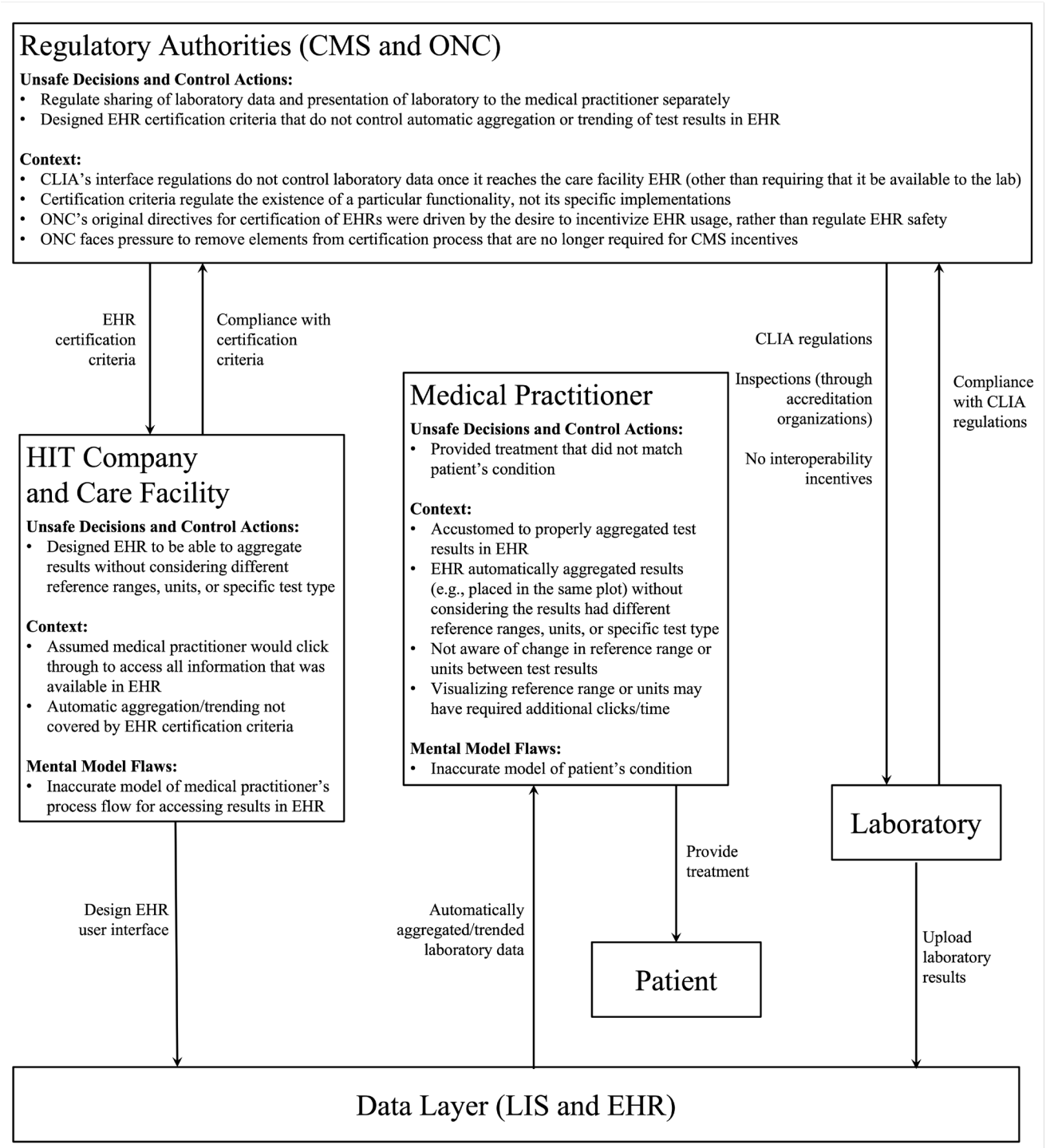

Figure 11. Visualization of scenario 1-13

Category/ Scenario #	Scenario Description
Control Action:	**Provide treatment to patient**
UCA Type:	**Too early / too late / out of order**
UCA:	**Medical practitioner provides treatment too late to avoid patient harm**
Scenario 2-1: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are never transferred into the patient's medical record. This may occur even if the test result is transmitted successfully from the LIS to the EHR but is erroneously placed in a file or data field that is inaccessible to the practitioner without database-specific tools. Because a practitioner sees many patients and may not be able to remember the status of every test they order, the practitioner may not realize that they are missing the requested test results for a particular patient.
Scenario 2-2: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the laboratory results for a patient are at another care facility and the transfer of these results into the patient's medical record in the new facility is delayed. The sending facility may not select all relevant clinical information to be exchanged when using a health information exchange (HIE). That may happen because of configuration choices in the sending facility's EHR or in the HIE system, which are compliant with standards but insufficient to provide all contextual information. Content certification for HIEs is limited, and often involves demonstrating compliance with a few test cases that do not generalize the situations encountered. Development of additional standards for what data elements are needed in test results may require facilities to update a large number of interfaces, for which they may see little return on investment without a financial/regulatory incentive.
Scenario 2-3: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are never transferred into the patient's medical record (or transferred too late). This may occur if the result message never makes it from the LIS to the EHR because the interface crashes due to a messaging error in the laboratory result message (e.g., wrong patient ID, test ID and result ID don't match, etc.). This may occur if the order message indicates the test type using a care facility local code, but the laboratory internally uses LOINC codes to differentiate tests, and the result message includes only a LOINC code, which has not been (or been inappropriately) mapped to the local code on the care facility side.
Scenario 2-4: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are never transferred into the patient's medical record (or transferred too late). This may occur if the result message never makes it from the LIS to the EHR because the interface crashes due to a messaging error in a previous laboratory result message (e.g., wrong patient ID, test ID and result ID don't match, etc.). The messaging error may occur for the same reasons as scenario 2-3, and that one incorrect message may repeatedly cause the interface to crash as it attempts to be sent, thus preventing other messages in the queue from being sent as well.

Category/ Scenario #	Scenario Description
Scenario 2-5: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are never transferred into the patient's medical record (or transferred too late). This may occur if the laboratory result message makes it from the LIS to the EHR, but not into the patient's record, because the message gets placed in a queue for manual review by care facility staff. This may occur if the message cannot be directly mapped to the EHR (e.g., new/uncommon test with results in a different format than the system was built to receive, results come in as PDF, etc.). The message may be allowed to go through in this format because the care facility and laboratory chose to override the functionality that crashes an interface if a message cannot go through so that results from new/uncommon tests are able to be shared. The care facility staff may not know how to review the queue or may have procedures for reviewing the queue that do not consider the time-sensitivity of test results waiting in the queue.
Scenario 2-6: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if laboratory results for a patient are transferred into the wrong patient's medical record. This may occur if the laboratory result message contains incorrect patient identifiers as compared to the order message. The patient identifiers may be incorrect if there are multiple patients with the same name, or if a patient's name is changed in the EHR after a test has been ordered and before the result arrives. The message may be allowed to go through in this format because the care facility and laboratory chose to override the functionality that crashes an interface if a message cannot go through, so that other (correct) results waiting in the queue are able to be shared.
Scenario 2-7: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test was never carried out (or carried out too late), because the order message never makes it from the EHR to the LIS. That may occur because the interface crashes due to a messaging error in the order message.
Scenario 2-8: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test was never carried out (or carried out too late), because the order message makes it from the EHR to the LIS, but not directly to the staff that will perform the test, as its gets placed in a queue for manual review before approval. This may occur if the message cannot be directly mapped to the LIS (e.g., test ordered with local code that the laboratory cannot process, ordered in a different format than the system was built to receive, etc.). The message may be allowed to go through in this format because the care facility and laboratory chose to override the functionality that crashes an interface if a message cannot go through, so that orders for new/uncommon tests are able to be shared. The laboratory staff may not know how to review the queue or may have procedures for reviewing the queue that do not consider the time-sensitivity of test orders.
Scenario 2-9: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test was never carried out, for reasons including diagnostic testing facilities or equipment are not

Category/ Scenario #	Scenario Description
	available due to geographic isolation, patient cannot access test due to limited mobility, patient cannot afford test which is not covered by payor, among others.
Scenario 2-10: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition. That may occur if the diagnostic test was never carried out, because the laboratory does not offer the test ordered by the practitioner. That may occur if the care facility's EHR was designed with a default set of tests that may be ordered, without consideration for what tests are actually available at the laboratory to which the patient specimen is sent. That may occur in an attempt by the EHR vendor to standardize the tests that may be ordered in a "model system", without consideration of the different laboratory test menus for the laboratories to which the provider/health entity is contracted to perform laboratory testing.
Scenario 2-11: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not have sufficient diagnostic information available to inform their process model of the patient's condition in a timely manner. That may occur if the diagnostic test results are found to not be acceptable or representative of the patient's true condition. This may occur if there exists a limited time window during which test results are valid, and they are not accessible or interpretable by the medical practitioner during that window.
Scenario 2-12: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that the patient is in critical condition and diagnostic information is available to determine appropriate treatment, but that information cannot be easily/rapidly shared between facilities due to issues of data ownership or patient data privacy. That may occur if a diagnostic test was performed at a different facility (or state) and permission could not be obtained to request that information of that facility.
Scenario 2-13: (A)	A medical practitioner may provide treatment too late to avoid patient harm because they have to duplicate testing prior to providing treatment. That may occur if a test was performed at a laboratory associated with a different care facility. The test result data shared from the different facility may not contain enough information for accurate determination of whether the test is comparable to one that would be performed at the receiving facility. That may occur if the test result was mapped by the sending facility to a reference terminology that does not match the terminology used at the receiving facility. Two different tests that use the same or similar approaches for different conditions may have been mapped to the same reference terminology (i.e., LOINC code, etc.), or two tests that use different methodologies for the same condition may have been mapped to the same reference terminology. This could happen because mapping different formats is a manual process, subject to the interpretation of the individual mapper, who may be an IT professional rather than a medical professional. It may also be the other way around, where a medical professional without reference terminology experience is tasked with mapping codes following an update. Even when correct reference terminology codes are selected, there can be multiple appropriate codes for a given test, so users may not select the same code. Implementation/mapping guidelines cannot anticipate every system and source data upon which the terminology or messaging standards would be implemented. Therefore, guidelines cannot provide specific mapping of proprietary data to standards. Inconsistent mapping is more likely to occur if implementers are unable to access support resources to clarify ambiguities in implementation/mapping guidelines or standards themselves.

Category/ Scenario #	Scenario Description
Scenario 2-14: (A)	A medical practitioner may provide treatment too late to avoid patient harm because they have to duplicate testing prior to providing treatment. That may occur if a test was performed at a laboratory associated with a different care facility. The test result data shared from the different facility may not contain enough information for accurate determination of whether the test is comparable to one that would be performed at the receiving facility. This may occur if the test performed at the other facility does not contain sufficient contextual information for interpretation and comparability determination, such as specimen source, reference range and type of testing (e.g., device identifiers, antigen testing versus a molecular assay, etc.). The results may not include sufficient information because the ability to transfer that information may be dependent on additional EHR settings each party needs to have selected or differences in data standards used. Development of additional standards for what data elements are needed when exchanging test results may require facilities to update a large number of interfaces, for which they may see little return on investment without a financial/regulatory incentive.
Scenario 2-15: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that they did not trust or were unaware of data that was self-reported from an over-the-counter test. The patient may have had no way of submitting data from an at home test. The test may have provided early and accurate results, but the practitioner may not trust or may not be allowed to trust them based on organizational policies.
Scenario 2-16: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that a laboratory called to attempt to notify the practitioner of an abnormal laboratory result, but the person who answered the phone did not pass the message directly to the physician and simply updated the patient's chart. The practitioner may not realize that an abnormal result was recorded until the next time the patient comes in and they look at the chart.
Scenario 2-17: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that the diagnostic information available did not emphasize the time-criticality of the result. That may occur if unmapped test results were shared by the laboratory as a PDF, which does not trigger time-critical alerts in the EHR system. The results may have been shared as a PDF because they pertained to a new test whose format could not be represented in the messaging standard (e.g., HL7 v2) available to that laboratory-care facility pair. Standards for new and complex tests (e.g., genomics) are not yet tightly constrained. See scenario 31-1 for a deeper discussion of this. The results are able to be shared as PDFs because CLIA only requires that data sent is received and does not specify the method of transmission. CLIA was drafted and approved in 1988, before EHRs were widely adopted and modifications to CLIA require Congressional approval.
Scenario 2-18: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that the test order sent did not have sufficient information about how quickly the test ordered needed to be done. The medical practitioner may have assumed the test would be done in a certain time window, but may not have had a way to communicate that to the recipient of the order [88].
Scenario 2-19: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that the alert notifying the provider of a significant result was one of many dozen or more alerts in the providers EHR account. This could happen because there is limited prioritization of alerts, out of date alerts (for example, a patient who died or is

Category/ Scenario #	Scenario Description
	otherwise not needing immediate response) don't clear the queue [89], or an overabundance of unnecessary alerts [90].
Scenario 2-20: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor could be that the alert notifying the provider of a significant result was only sent to the practitioner who initially ordered the test. The initial practitioner may have been a transient employee like a resident, or else someone who was not responsible for follow up care of the patient. This person may either not know how to forward the result, not be able to forward the result, or be out of the system all together when the result arrives. This may happen if the patient does not have a primary physician who is designated to receive all order results regardless of the ordering physician or other safeguard to ensure that the recipient of test results is correct [89], [91].
Scenario 2-21: (A)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor to this could be that they did not have the diagnostic information available to inform their mental model of the patient's condition in time. That may occur if the laboratory did not immediately notify the physician of an abnormal or time-sensitive lab result. The lab may not have notified the physician of a notable lab result because they did not believe the result to be notable. They may not have believed the result to be notable because it fell within the test's reference range, but different reference ranges could exist for a single test based on demographic factors. The laboratory may be using a reference range that is not compatible with the test being performed or the patient being examined, such as using a reference range for a demographic that does not represent the patient. This may occur due to inadequate contextual information transmitted alongside the specimen. Critical demographic context may include treatment status, disease progress[33], age, gender, height, weight, ethnicity, etc. [92]. Detailed clinical context may not have been included in the test order if the EHR interface makes it too time consuming or onerous for the practitioner to include. Additionally, the test order may have been filled out by a member of the health staff who did not know the patient's clinical context. CLIA requires that laboratory orders contain "Any additional information relevant and necessary for a specific test to ensure accurate and timely testing and reporting of results, including interpretation, if applicable" (§493.1241 (c)(8)). However, there are no standards or requirements that control what context should be shared for each specific test. If the order does not have the required information, the laboratory will usually try to contact the ordering physician but may or may not be successful. Even if the laboratorian reaches the ordering physician, the contextual information may not be obtainable if the patient is no longer at the care facility and cannot be reached directly.
Scenario 2-22: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor to this could be that they did not have the diagnostic information available to inform their mental model of the patient's condition in time. That may occur if the laboratory did not immediately notify the physician of an abnormal or time-sensitive lab result. The lab may not have notified the physician of a notable lab result because they did not believe the result to be accurate. They may not have believed the result to be accurate because it was so far outside the expected range that it is deemed more likely that the test was flawed than that the result is accurate. This may occur due to a lack of standardized procedures for determining the "valid range" of a diagnostic test as opposed to just the reference range.
Scenario 2-23: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor to this could be that they did not have the diagnostic information available

Category/ Scenario #	Scenario Description
	to inform their mental model of the patient's condition in time. That may occur if the laboratory did not immediately notify the physician of an abnormal or time-sensitive lab result. The lab may not have notified the physician of a notable lab result because they believed the physician would already have access to that information. They may believe that because a standard procedure exists for communicating lab results to physicians and that is considered sufficient by the lab. They may also believe it is not their responsibility to notify the physician directly if other standardized means of communication exist.
Scenario 2-24: (C)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor to this could be that they did not have the diagnostic information available to inform their mental model of the patient's condition in time. That may occur if the laboratory did not immediately notify the physician of an abnormal or time-sensitive lab result. The lab may have attempted to notify the physician of the notable lab result but may have been unable to reach the physician. They may have been unable to reach the physician because they only attempted one method of communication (telephone, email, etc.) and the physician did not respond to that method of communication in time.
Scenario 2-25: (B)	A medical practitioner may provide treatment too late to avoid patient harm (UCA). One contributing factor to this could be that they did not have the diagnostic information available to inform their mental model of the patient's condition in time. That may occur if the laboratory did not immediately notify the physician of an abnormal or time-sensitive lab result. The lab may have attempted to notify the physician of the notable lab result, but the information may have been lost or corrupted while going through a "middleman". They may have been able to reach someone affiliated with the physician, but not the physician directly, and the information is logged incorrectly or incompletely by that liaison.

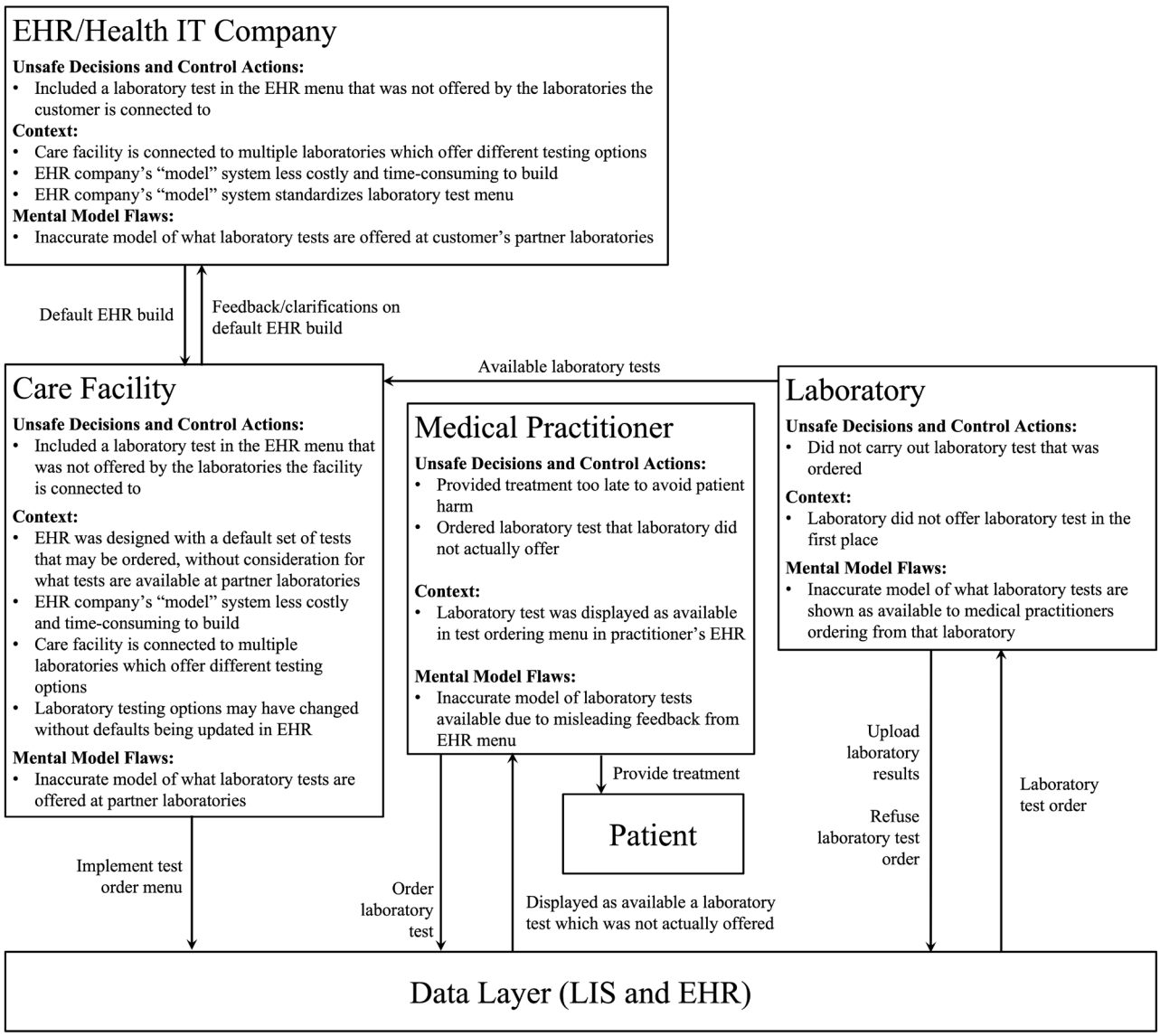

Figure 12. Visualization of scenario 2-10

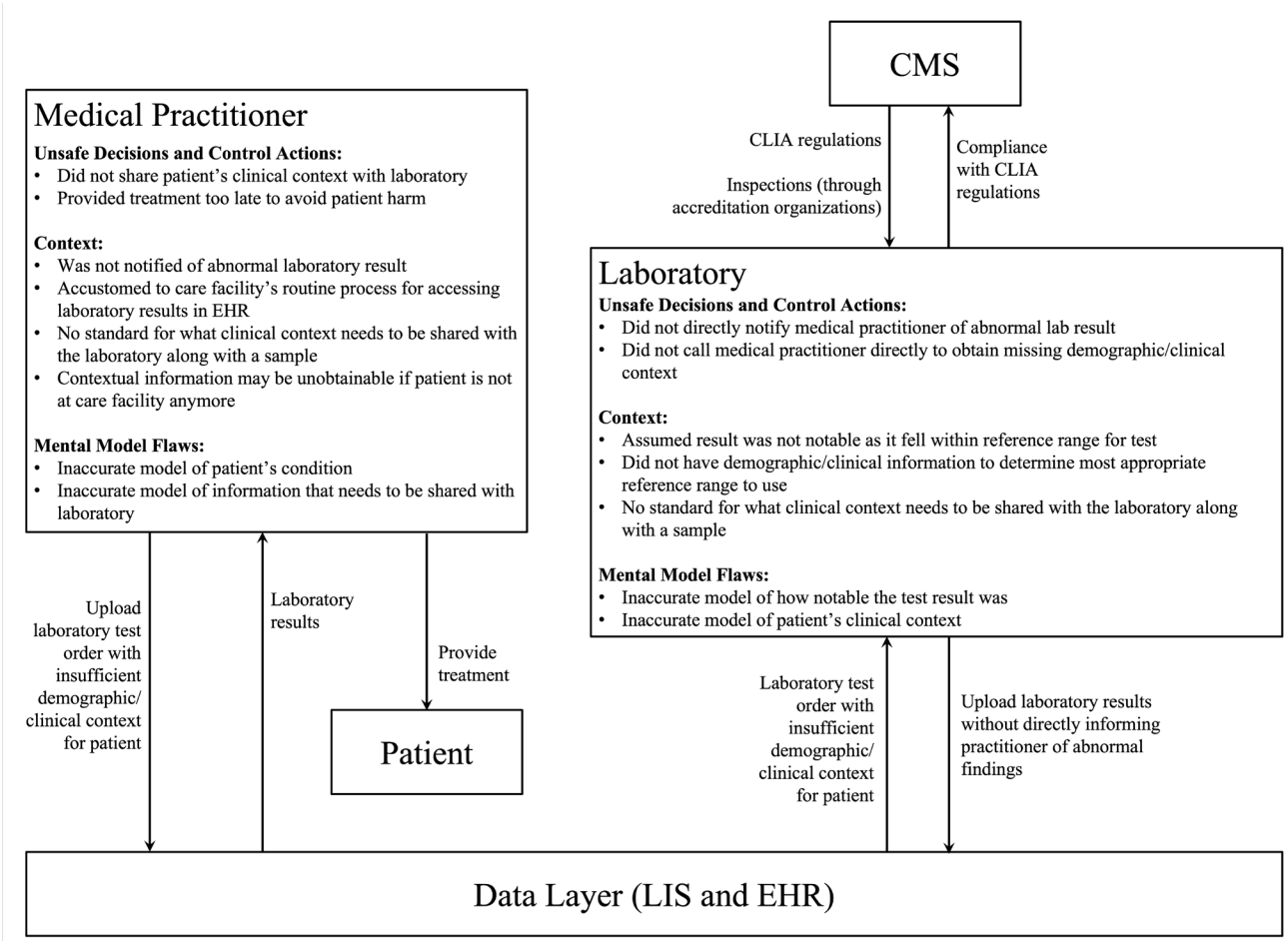

Figure 13. Visualization of Scenario 2-21

Category/ Scenario #	Scenario Description
Control Action:	**Order laboratory test**
UCA Type:	**Providing causes hazard**
UCA:	**Medical practitioner orders laboratory test that is not the best/most appropriate test to diagnose a disorder/disease**
Scenario 3-1: (B)	A medical practitioner may not order the best/most appropriate lab test to diagnose a disorder/disease (UCA). One contributing factor may be that the EHR autosuggested the test, or dropdown menu options look similar but are not the test the practitioner actually intended to order [90]. The name of the incorrect test may be too similar for the physician to notice. This is because there is often a limited amount of space on a screen and not all text is displayed in every section. Additionally, if the practitioner believes they selected the right order, they may not go back and look at that field a second time. The physician may not notice that an incorrect order was placed until the results come back for a test that does not make sense. Even if this error is reported the EHR vendor may not prioritize fixing it as they may attribute it to physician error. See scenario 13-1 for a deeper discussion of this.
Scenario 3-2: (C)	A medical practitioner may not order the best/most appropriate lab test to diagnose a disorder/disease (UCA). One contributing factor may be that they are unfamiliar with the best available tests. This may occur because the practitioner is not familiar with the interpretation of various lab tests used to diagnose and/or follow specific disorders/diseases. Certain laboratory tests have additional requirements (e.g., may only be ordered in conjunction with other lab test results or in specific clinical contexts), and that information may not always be conveyed to the ordering practitioner. While practitioners could consult a laboratorian/ pathologist to determine the most appropriate lab test, they may not be aware they are selecting a potentially inappropriate test, or do not have the time to consult them for every test order.
Scenario 3-3: (C)	A medical practitioner may not order the best/most appropriate lab test to diagnose a disorder/disease (UCA). One contributing factor may be that the test is accurate in adults but has not been suitably tested on children or a different unique demographic. The EHR may not warn the practitioner because this distinction has not been noticed by their health system or by the device manufacturer. The FDA does not require data from pediatric patients before approving IVDs [93]. This may be due to a general belief that controlled trials are already difficult to perform for IVDs and that requiring test populations of specific demographic groups would be too onerous of a burden on the IVD manufacturers.
Scenario 3-4: (B)	A medical practitioner may not order the best/most appropriate lab test to diagnose a disorder/disease (UCA). One contributing factor may be inappropriate clinical decision support provided by the EHR system. The clinical decision support may be inappropriate due to inappropriate coding of the condition or test result on which the decision support is acting. It may also be inappropriate if the system has not been updated to adequately address a change in the protocol for ordering a test result or diagnosing a condition.
Scenario 3-5: (B)	A medical practitioner may not order the best/most appropriate lab test to diagnose a disorder/disease (UCA). One contributing factor may be inconsistent test naming in EHR user interfaces (e.g., “hypertension” vs “essential hypertension”). This may occur because it is up to the care facility administration or IT team to adequately program the EHR to practitioners’ needs, which may often be conflicting (e.g., two practitioners want the same test named differently).

Category/ Scenario #	Scenario Description
Control Action:	**Order laboratory test**
UCA Type:	**Providing causes hazard**
UCA:	**Practitioner orders laboratory test for patient that is not covered by patient's health insurance**
Scenario 4-1: (C)	A medical practitioner may order a test that is not covered by the patient's health insurance if that information was not relayed to the practitioner in the ordering menu.

Category/ Scenario #	Scenario Description
Control Action:	**Order lab test**
UCA Type:	**Providing causes hazard**
UCA:	**Medical practitioner orders laboratory test for patient that has already been done**
Scenario 5-1: (B)	A medical practitioner may order a laboratory test for a patient that they already had done in a different hospital network. Because there is no way for all of a patient's data to be stored together, the physician is unaware of the previous test. The patient may be unaware that the test the physician ordered is the same one they had done previously.
Scenario 5-2: (B)	A medical practitioner may order a duplicate test intentionally because their hospital system does not trust results from outside facilities. That may occur if the care facility was unable to demonstrate compliance of that test with the facility's quality standards. This may occur if the test performed at the other facility did not achieve the sensitivity required at this facility.
Scenario 5-3: (A)	A medical practitioner may order a duplicate test intentionally because their hospital system does not trust results from outside facilities. That may occur if the original test was performed at a laboratory associated with a different care facility. The test result data shared from the different facility may not contain enough information for accurate determination of whether the test is comparable to one that would be performed at the receiving facility. This may occur if the test performed at the other facility does not contain sufficient information for interpretation and comparability determination such as specimen source, reference range and type of testing (e.g., device identifiers, antigen testing versus a molecular assay, etc.). The results may not include sufficient information because the ability to transfer that information may be dependent on additional EHR settings each party needs to have selected or differences in data standards used. Development of additional standards for what data elements are needed when exchanging test results may require facilities to update a large number of interfaces, for which they may see little return on investment without a financial/regulatory incentive.
Scenario 5-4: (B)	A medical practitioner may order a duplicate lab test if a specific test needs to be ordered within a certain amount of time from when the patient arrives at the care facility, so a "stat"

Category/ Scenario #	Scenario Description
	order is placed immediately, and that test ends up being ordered again as part of an order set that gets placed later in the patient visit.
Scenario 5-5: (B)	A medical practitioner may order a duplicate lab test if they believe the test order may not have gone through the system if it has been a long time since the order was filed and the results have not been delivered. For the ordering practitioner, there is no easy way to track at what stage of the process the laboratory test is, and when they can expect to receive results.

Controller: Laboratory/Care Facility

Category/ Scenario #	Scenario Description
Control Action:	**Update HIT system**
UCA Type:	**Not providing causes hazard**
UCA:	**Laboratory/care facility does not update HIT system when safety-critical HIT system update is released**
Scenario 6-1: (B)	A laboratory/care facility may not have updated their HIT system because they did not believe the update was safety critical. The update may not have necessarily come with labels or descriptions of the implications of not implementing the update. The decision to proceed or not with the update may have been made in the context of available resources and competing priorities. Facilities may update systems based on perceived relevance. For example, care facilities may update code sets that impact a broader range of users (like SNOMED CT or billing codes) more frequently than they update code sets regarding specific use cases (like LOINC codes for laboratory data). Additionally, the team that makes the decision to upgrade the system may not be the end users of that system. Regulatory or statutory incentives are inadequate when it comes to ensuring that laboratories and care facilities remain up to date with their HIT systems. Regulatory or statutory incentives are also inadequate when it comes to informing laboratories of implications for not proceeding with HIT system updates.
Scenario 6-2: (A)	A laboratory/care facility may not have updated their HIT system because they believed the update would interfere with other IT systems the laboratory/care facility uses. The laboratory/care facility may have this belief if prior system updates resulted in other IT systems encountering problems. They may also have received information from other facilities with the same software system that may have already taken the update and experienced problems. Some HIT system updates may have an impact on 3rd party HIT systems as well as downstream instruments. Software code changes may not be implemented successfully without thorough validation testing and coordination between HIT system vendors and users. Currently, regulatory or statutory incentives ensuring safety-critical updates do not affect other safety-critical functionality are inadequate. Maintaining up to date LIS systems depends on vendors working in partnership with users when new code releases are coming, which may not occur without dedicated maintenance contracts.

Category/ Scenario #	Scenario Description
Scenario 6-3: (A)	A laboratory/care facility may not have updated their HIT system because they did not have adequate resources (budget, manpower, or technical expertise) to install the update in a timely manner. Many HIT software updates also require hardware replacement, configuration, or re-calibration of instrumentation. The combination of additional software and hardware cost to upgrade HIT systems may create a budgetary strain for healthcare organizations. In addition, resources needed to implement and maintain HIT upgrades may be scarce as a result of economic factors. Financial incentives to defray cost for laboratories/care facilities to remain up to date with their HIT systems are non-existent.
Scenario 6-4: (B)	A laboratory/care facility may not have updated their HIT system because they believed that the HIT system was "turnkey" and did not require active maintenance. This may occur if the HIT system was marketed to the laboratory/care facility by the vendor as not needing active maintenance. The facility may be too small to have an IT team, or the team may be too small or lack the resources to fully tackle the task of maintaining the HIT system.

Category/ Scenario #	Scenario Description
Control Action:	**Update HIT system**
UCA Type:	**Providing causes hazard**
UCA:	**Laboratory/care facility updates HIT system to version that is incompatible with other systems**
Scenario 7-1: (B)	A laboratory/care facility may have updated their HIT system to a version that is incompatible with other equipment because previous updates did not break any existing connections, and they trusted that this one would behave similarly. They may have believed so because they received testing routines from the vendor which they believed to be sufficient in capturing all interactions of the system. The testing routine may not have taken into consideration every possible software or hardware the HIT system is expected to interact with, due to the high amount and variability of connections the system has. The laboratory/care facility may not have enough experts who understand the software connections on the team responsible for updates. This can happen if the IT team is completely disconnected from the lab in a system where the lab is within a larger healthcare facility. Currently, regulatory or statutory incentives ensuring safety-critical updates do not affect other safety-critical functionality are inadequate. Maintaining up to date LIS systems depends on vendors working in partnership with users when new code releases are coming, which may not occur without dedicated maintenance contracts.
Scenario 7-2: (C)	A laboratory/care facility may have updated HIT system to version that is incompatible with other equipment because they were under pressure to update within a certain window of time and did not have time, resources, or expertise to run necessary testing.
Scenario 7-3: (B)	A laboratory/care facility may have updated HIT system to version that is incompatible with other equipment because the middleware facilitating information transfer was unable to update their infrastructure in time. The middleware company may only find out about the HIT system update once that update has broken a connection the middleware software uses. Though there may be contractual clauses requiring middleware companies to be informed of

	updates in the systems with which they interact, regulatory or statutory requirements are inadequate.

Category/ Scenario #	Scenario Description
Control Action:	**Update reference terminology in HIT system**
UCA Type:	**Not providing causes hazard**
UCA:	**Laboratory/care facility does not update reference terminology in HIT system when safety-critical reference terminology update is released.**
Scenario 8-1: (B)	A laboratory/care facility may not have updated the reference terminology in their HIT system because they did not believe the update was safety critical. The decision to proceed or not with the terminology update may have been made in the context of available resources and competing priorities. Facilities may update systems based on perceived relevance. For example, care facilities may update code sets that impact a broader range of users (like SNOMED CT or billing codes) more frequently than they update code sets regarding specific use cases (like LOINC codes for laboratory data). Regulatory or statutory incentives are inadequate when it comes to ensuring that laboratories and care facilities remain up to date with their reference terminologies. Neither standards development organizations nor government agencies like NLM track whether users are going through with terminology updates. SDOs do not track their users in general or share user logs due to logistical and privacy concerns.

Category/ Scenario #	Scenario Description
Control Action:	**Map local codes to reference terminology**
UCA Type:	**Not providing causes hazard**
UCA:	**Laboratory/care facility does not map local codes to reference terminology when safety-critical reference terminology update is released**
Scenario 9-1: (A)	A laboratory/care facility might not map local codes to reference terminology because the regulation that required them to do the mapping elapsed or ended (See UCAs for CMS, ONC, Federal Government). The laboratory/care facility may not see keeping mapped codes updated as a priority, especially if there is no tangible benefit for doing so and there are no regulatory incentives or repercussions for failing to do so. Current standard ontology mapping strategies may not contain sufficient granularity to support interoperability, and care facilities or laboratories may choose to not utilize reference terminologies for particular tasks (e.g., comparability determination for exchange of results) because they are aware of these shortcomings. Additionally, it may not be necessary to have reference terminology mapped to local codes if the facilities sharing data have already built an interface that can interpret each facility's local codes.
Scenario 9-2: (A)	A laboratory/care facility may not map local codes to new reference terminology because of time or resource constraints. Facilities may make decisions on terminology mapping based on perceived relevance. For example, care facilities may update code sets that impact a broader range of users (like SNOMED CT or billing codes) more frequently than they update code sets regarding specific use cases (like LOINC codes for laboratory data). Due to the

Category/ Scenario #	Scenario Description
	immense volume of tests and possible test results, labs may not have the staffing resources to review newly released terminology mappings in a timely fashion. Neither standards development organizations nor government agencies like the NLM track whether users are mapping to new terminology releases. SDOs do not track their users in general or share user logs due to logistical and privacy concerns.
Scenario 9-3: (B)	A laboratory/care facility may not map local codes to new reference terminology because of insufficient support in the mapping process. The facility may have had initial support setting up a mapping routine, but no longer receives sufficient support to continue to make those adjustments in the long term. Implementation/mapping guidelines cannot anticipate every system and source data upon which the terminology or messaging standards would be implemented. Therefore, guidelines cannot provide specific mapping of proprietary data to standards. Inconsistent mapping is more likely to occur if implementers are unable to access support resources to clarify ambiguities in implementation/mapping guidelines or standards themselves.
Scenario 9-4: (A)	A laboratory/care facility may not map local codes to new reference terminology because of unclear or conflicting guidelines for mapping reference terminology. It may be the case that multiple SDOs developing different reference terminologies disagree on the best approach to mapping new terminologies, and each SDO releases mapping guidelines for their own terminology that conflict with the guidelines of the other SDO. There may be no formalized line of communication between different SDOs to ensure consistency in mapping guidelines.

Category/ Scenario #	Scenario Description
Control Action:	**Map local codes to reference terminology**
UCA Type:	**Providing causes hazard**
UCA:	**Laboratory/care facility maps local codes to reference terminology incorrectly/ inconsistently**
Scenario 10-1: (A)	A laboratory/care facility may map local codes to reference terminology incorrectly or inconsistently because mapping different reference terminologies is a manual process, subject to the interpretation of the individual mapper, who may be an IT professional rather than a medical professional. It may also be the other way around, where a medical professional without reference terminology experience is tasked with mapping codes following an update. Tests using different methodologies and producing noncomparable results may also be *appropriately* mapped to the same reference terminology, as the terminology structure may not support sufficient granularity to distinguish results performed on different noncomparable instrumentation. On the other hand, there can be multiple appropriate codes for a given test, so different users may not always select the same code.
Scenario 10-2: (A)	A laboratory/care facility may map local codes to reference terminology incorrectly or inconsistently if the facility does not update their reference terminology base frequently enough as new codes are released and maps their local codes to outdated (deprecated) terminology. Facilities may make decisions on terminology mapping based on perceived relevance. For example, care facilities may update code sets that impact a broader range of

Category/ Scenario #	Scenario Description
	users (e.g., SNOMED CT or billing codes) more frequently than they update code sets regarding specific use cases (e.g., LOINC codes for laboratory data). Neither standards development organizations nor government agencies like the NLM track whether users are mapping to new terminology releases. SDOs do not track their users in general or share user logs due to logistical and privacy concerns.
Scenario 10-3: (A)	A laboratory/care facility may map local codes to reference terminology incorrectly or inconsistently because they do not have systems in place for verifying mapping after mapping occurs. Current guidance from the ONC for safe EHR use does not require checking this (SAFER). Even if added to guidance like SAFER, a significant number of regulations from the ONC and CMS require simple attestations of adherence to optional or required components. Because of the lack of required proof and minimal oversight the care facility may believe that it is more cost effective to risk a potential fine than to perform the verification procedures.

Category/ Scenario #	Scenario Description
Control Action:	**Enable software feature in HIT system**
UCA Type:	**Not providing causes hazard**
UCA:	**Laboratory/care facility does not enable safety-critical software feature on HIT system**
Scenario 11-1: (B)	A laboratory/care facility may not enable safety-critical software feature on a HIT system because they do not realize the feature has safety-related significance. The HIT company may indicate whether a feature is safety-critical in the release notes, but the perception of safety-criticality may be different between a developer and a user of the system. Facilities with robust IT teams may work to review any impacts of not activating a feature, but smaller facilities may not have the resources to do so. Additionally, the team that makes the purchasing decision to acquire a system or activate a feature may not be the end users of that system and may not be aware of the safety-criticality of the feature. Medical director sign-off may be required depending on the type of decision that is being made, but the individual practitioner signing off may not have the time or resources to conduct an in-depth analysis of the feature. The safety-critical feature in the HIT software may have been required by HIT certification criteria, but the certification organizations may have certified only a "model" software rather than a specific implementation at a site. Though HIT certification organizations (ONC-ACBs) *can* randomly audit HIT implementations "in the field", ONC may not enforce that such audits actually occur. Historically, ONC-ACBs have conducted random audits on 2% of accredited programs, but currently audits only occur reactively when they receive complaints about particular programs [94].
Scenario 11-2: (B)	A laboratory/care facility may not enable safety-critical software feature on a HIT system because they did not realize they needed to enable the feature. This might be because of the intense setup timeline pressure placed on care facilities during initial installation. The team that makes the purchasing decision may not be the end users of that system and may opt for a setting which may not always reflect the best configuration for the users. The configuration may not include a feature that the users deem safety-critical feature without a regulatory or financial incentive, or if standards are written in the language of "should" rather than "shall".

Category/ Scenario #	Scenario Description
Scenario 11-3: (B)	A laboratory/care facility may not enable safety-critical software feature on a HIT system because they did not realize that the feature depends upon another feature that the facility does not possess. Relationships between HIT modules are typically complex and the decision makers at the facility, who may not be the end users of that system, may choose to opt for default settings, which may not always be compatible with the small subset of non-default settings selected.
Scenario 11-4: (B)	A laboratory/care facility may not enable safety-critical software feature on a HIT system because they do not realize that the feature is safety critical. While the CMS or ONC may provide tools that would help facilities verify safety-critical features are working, the tools may not be used by all facilities if they are optional and not tied to incentive/ disincentive structures [95], [96].

Controller: Care Facility

Category/ Scenario #	Scenario Description
Control Action:	**Acquire an Electronic Health Record System**
UCA Type:	**Not providing causes hazard**
UCA:	**Care facility does not acquire an EHR system when patient data needs to be shared electronically from other facilities or laboratories**
Scenario 12-1: (B)	A care facility may not acquire an EHR system because they were not eligible for EHR adoption incentives according to Meaningful Use or 21st Century Cures reimbursement requirements. They may not be able to make the switch because of the high initial costs and lack of incentives to make the switch. This care facility may then not be able to send useful health information to a patient's other care facilities[97].

Controller: HIT Company

Category/ Scenario #	Scenario Description
Control Action:	**Release HIT system update**
UCA Type:	**Not providing causes hazard**
UCA:	**HIT company does not release HIT system update following safety-critical reports from customers**
Scenario 13-1: (A)	A HIT company may not release a system update because they believe the reported problem to be related to the practitioner's use of the HIT system, rather than the system design. HIT companies will work with care facilities to determine safety concerns and if immediate system updates are required. However, the HIT company may rely on a "hold

Category/ Scenario #	Scenario Description
	harmless" clause in their contract with the customer, such that their system cannot be held responsible for errors the system introduces, because medical practitioners should be able to identify and correct for these errors. Additionally, the HIT company may not have received sufficient reports of safety concerns, as reports submitted by medical practitioners may be filtered through different liaisons such as IT specialists or administrators before being sent to HIT companies. These liaisons may also deem the problem to be related to the practitioner's use of the HIT system, rather than the system design. Uncovering and reporting problems with HIT systems may not be prioritized if laboratory or care facility management spend large sums of money and time acquiring and maintaining these systems. Users of HIT products may face additional barriers to reporting. For example, medical practitioners and laboratorians may be reluctant to submit reports out of concern they will be blamed for not being knowledgeable. Users may also not understand enough about the HIT system to be able to articulate a report on the issue they encounter. Additionally, if users have previously submitted reports which have not been followed up on, they may not submit additional reports. Regulatory or statutory incentives to ensure safety-critical reports are addressed on the vendor side are inadequate, partly as a result of the belief that the information presented in a HIT system is mediated by an expert user and is thus not a closed-loop system by itself. HIT certification is primarily geared towards EHR functionality and data exchange capabilities. Safety is considered as a factor in HIT certification through user centered design criteria, but direct safety-related performance criteria for programmatic activities (e.g., CMS's promoting interoperability programs) are inadequate. Introducing additional safety-specific certification criteria without additional financial incentives may lead to backlash from developers and users of HIT systems.
Scenario 13-2: (A)	A HIT company may not release a system update because they do not believe the reported issue to be safety-critical enough to warrant a system update. The company may have only received that report from a small subset of facilities, as the build at those facilities may not have been the company's "model system." Without other facilities reporting that same issue, financial incentives may lead the HIT company to require the customer to address the issue themselves. Regulatory or statutory incentives to ensure safety-critical reports are addressed by vendors or submitted to a regulatory agency are inadequate. HIT certification is primarily geared towards EHR functionality and data exchange capabilities. Safety is considered as a factor in HIT certification through user centered design criteria, but direct safety-related performance criteria for programmatic activities (e.g., CMS's promoting interoperability programs) are inadequate. Introducing additional safety-specific certification criteria without additional financial incentives may lead to backlash from developers and users of HIT systems.
Scenario 13-3: (B)	The HIT company may not release a system update because they do not believe the reported issue to be safety-critical enough to warrant a system update. The HIT company may not have received sufficient reports of safety concerns, as submitting reports may require medical practitioners to stop what they are doing and retrace a problem in HIT system to take screenshots, which may not be feasible due to time constraints.

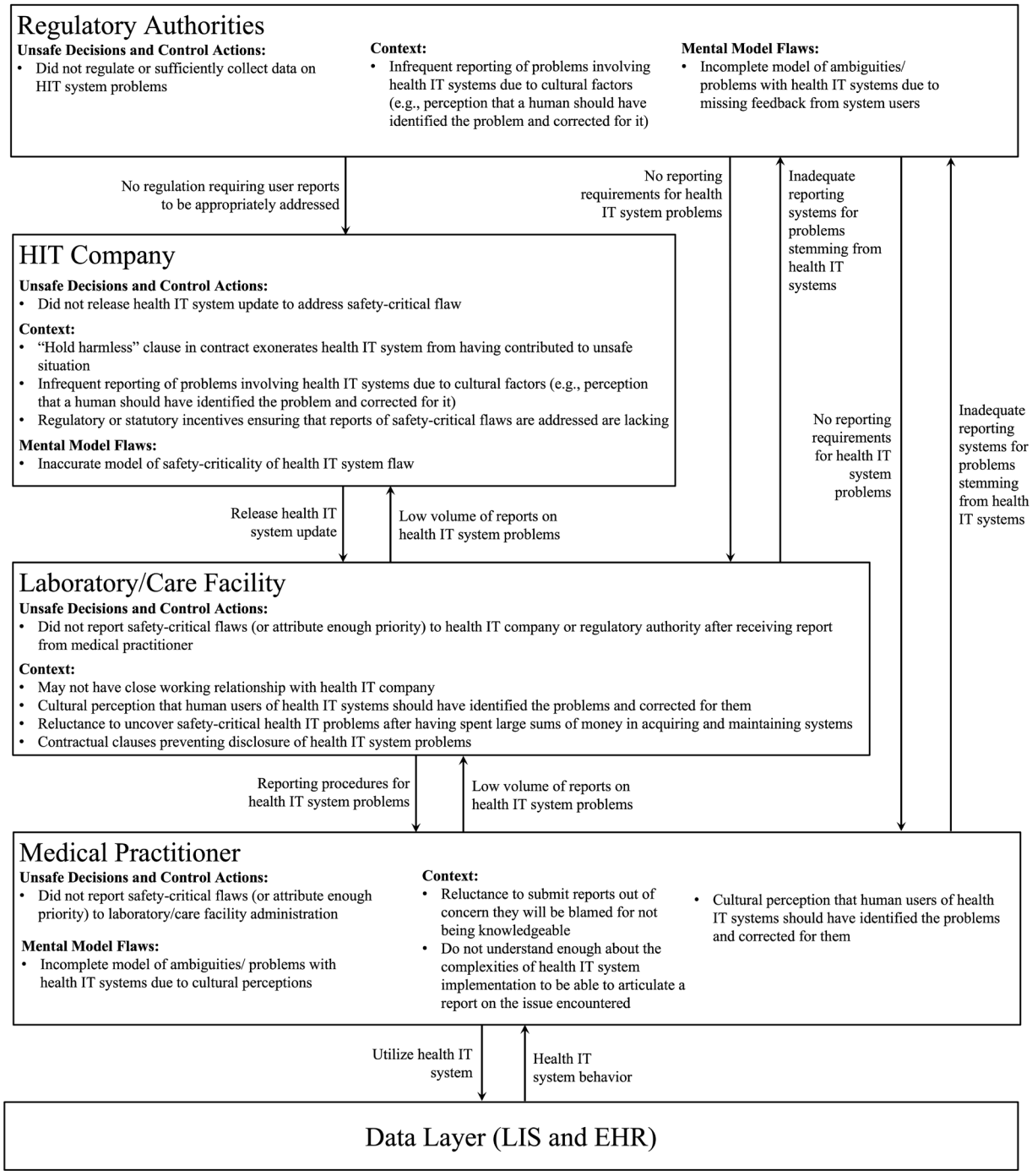

Figure 14. Visualization of scenario 13-1

Category/ Scenario #	Scenario Description
Control Action:	**Release HIT system update**
UCA Type:	**Providing causes hazard**
UCA:	**HIT company releases HIT system update that has been insufficiently tested**
Scenario 14-1: (A)	The HIT company may release a system update that has been insufficiently tested (UCA). One component of insufficient testing may be that the HIT company develops an insufficient set of test cases for customers to use to verify the compatibility of an update with their existing systems. This may occur because the HIT company may not have the information with which to develop test cases for each individual user of that system. HIT systems are built for individual customers and, if maintenance is not included in the contract, these systems are no longer under the purview of the HIT company. The company thus may not sufficiently consider the features or connections of each individual build when developing the test cases for an update. Regulatory or statutory requirements for testing of HIT systems, other than those embedded within medical devices, are inadequate.
Scenario 14-2: (A)	The HIT company may release a system update that has been insufficiently tested (UCA). One component of insufficient testing may be that the in-house regression testing performed by the HIT company does not sufficiently consider how the new update will interfere with existing functionality of the system, or its connections. This may occur because regulatory or statutory requirements for testing of HIT systems are inadequate, other than for systems embedded within medical devices. Even if a customer has a maintenance contract and uses a standard (non-custom) version of the software, they may encounter problems if updated systems have not been sufficiently tested by the HIT vendor.
Scenario 14-3: (B)	The HIT company may release a system update that has been insufficiently tested (UCA). One contributing factor may be that the extent of the testing performed following a build or update was left to the judgment of the client. The client may want to expedite the deployment of their HIT system and may not verify that the testing routine developed by the HIT company successfully addresses all cases likely to be encountered in that specific environment. This may occur because regulatory or statutory requirements for testing of HIT systems are inadequate, other than for systems embedded within medical devices.

Category/ Scenario #	Scenario Description
Control Action:	**Provide build support and maintenance for HIT system customers**
UCA Type:	**Not providing causes hazard**
UCA:	**HIT company does not provide sufficient build support or maintenance when customer does not have the resources to build or maintain HIT System**
Scenario 15-1: (C)	The HIT company may not provide sufficient build support or maintenance to its customers if any of these provisions are not included in the customer contract. They may not be included in the customer contract due to financial pressures on the customer's side. The

Category/ Scenario #	Scenario Description
	HIT company may not have incentives to spend its employees' time on support and maintenance of individual HIT systems that were implemented by care facility or laboratory IT teams.

Category/ Scenario #	Scenario Description
Control Action:	**Roll back HIT system update**
UCA Type:	**Too early / too late / out of order**
UCA:	**HIT company rolls back HIT system update with safety-critical flaws too late after update is released**
Scenario 16-1: (B)	The HIT company may roll back the HIT system update too late if the system operates though a cloud-based implementation, and the safety-critical issue was only reported in a small subset of facilities utilizing the system. HIT companies would need to coordinate rolling back the HIT system updates, which may take time and would require suspending services available to other facilities that may not be encountering the safety-critical issue.

Category/ Scenario #	Scenario Description
Control Action:	**Select data standards to implement in HIT system**
UCA Type:	**Providing causes hazard**
UCA:	**HIT company selects data standard that is not compatible with data standards used in HIT systems from competitors**
Scenario 17-1: (A)	The HIT company may choose a data standard that is not compatible with data standards used in HIT systems from competitors because it wants to make it a challenge for customers to switch HIT vendor. They are able to select which standards they use or don't use as long as they can meet certain ONC requirements, however there is regulation that specifies which data standards must be used is inadequate. The regulatory/financial incentives that do exist require systems to be able to implement some specific standards, but do not mandate a specific implementation.

Controller: CMS

Category/ Scenario #	Scenario Description
Control Action:	**Change requirements for "Promoting Interoperability" participants to avoid a negative payment adjustment.**
UCA Type:	**Providing causes hazard**
UCA:	**CMS changes requirements for "Promoting Interoperability" participants in a way that negatively impacts safety outcomes for program participants**
Scenario 18-1: (B)	CMS changes "Promoting Interoperability" program requirements that change safety outcomes for program participants by reducing quantity of points allocated to safety-critical items. Through the "Promoting Interoperability" program, CMS releases a scoring system where program participants must hit a minimum score in order to obtain full reimbursements. Care facilities may prioritize components of the program that are allocated more points. Therefore, they may deprioritize measures that are allocated fewer points, even if they are more safety critical. Components that do not add to the score at all may be particularly de-prioritized.
Scenario 18-2: (B)	CMS releases new "Promoting Interoperability" program requirements that do not align with the most safety-critical issues. This may be because CMS is not aware of the biggest issues affecting safety because the data, they receive is not high-resolution and does not allow for significant analysis of actual quality/performance versus score for the hospitals. The main feedback CMS receives is through questions and comments from care facilities. Care facilities have no incentive to provide CMS with information that would increase regulatory oversight.
Scenario 18-3: (B)	CMS changes "Promoting Interoperability" program requirements to include too many optional components which results in fewer hospitals following safety-critical but optional requirements. This may be because CMS receives feedback from care facilities that previous requirements were too rigid and caused them to lose funding. CMS may get the feedback either through direct messaging or through lower program participation [98].
Scenario 18-4: (B)	CMS adds "Promoting Interoperability" program requirements that are too difficult for participants to adhere to in time. This could cause hospitals to lose critical funding and could increase political pressure on CMS to loosen restrictions overall. They may create requirements that are difficult to meet because CMS receives feedback from other HHS agencies that certain criteria are critical for achieving an interdepartmental goal [99]. CMS may receive feedback from hospitals through notice and comment rulemaking procedures. If insufficient comments are left, CMS may not realize the rule is too severe.
Scenario 18-5: (B)	CMS releases "Promoting Interoperability" program requirements with no premarket audit plans or other way of tracking honest attestations. The attestation data may then give a false sense of security in overall performance on that metric. CMS may not be able to easily conduct audit because the data it receives is not detailed enough to critically evaluate performance independently.

Category/ Scenario #	Scenario Description
Control Action:	**Provide hardship exception for "Promoting Interoperability" program participant**
UCA Type:	**Providing causes hazard**
UCA:	**CMS provides a hardship exception for a requirement that allows hospitals to operate EHRs with known safety risks** [86]**.**
Scenario 19-1: (B)	CMS provides too many hardship exceptions for complying with promoting interoperability rules such that care facilities wait for multiple years to fix safety-critical problems that are out of compliance with the regulations. This may be because too many hospitals would fail if they allowed fewer exceptions. High rates of failure could potentially disrupt healthcare for many people [99].
Scenario 19-2: (B)	CMS provides too few hardship exceptions such that care facilities lose critical funding when a HIT company is found to be out of compliance with the regulations. This could cause additional pressures to distort data or otherwise conceal lack of compliance.

Category/ Scenario #	Scenario Description
Control Action:	**Provide negative payment adjustment to care facility**
UCA Type:	**Not providing causes hazard**
UCA:	**CMS does not provide negative payment adjustment to care facility that did not meet funding requirements and is using systems that do not meet minimum safety requirements.**
Scenario 20-1: (B)	CMS may not provide negative payments to care facilities that did not meet regulatory requirements because CMS was unaware that the care facility's attestation was falsely attested. CMS has historically relied on "post payment audits" as opposed to pre-payment verification [100]. They may rely on post payment audits because CMS does not have the funding or statutory ability to properly conduct audits earlier. Additionally, the sheer volume of program participants may make proactive action difficult. Furthermore, CMS does not have access to data that would allow them to verify attestation data. Adding additional data requirements would require funding to analyze it, and additional time and resources on the care facility side.

Controller: ONC

Category/ Scenario #	Scenario Description
Control Action:	**Adopt technical standards in HIT certification criteria**
UCA Type:	**Providing causes hazard**

Category/ Scenario #	Scenario Description
UCA:	**ONC adopts technical standards in HIT certification criteria that are insufficient to create interoperable HIT systems**
Scenario 21-1: (A)	ONC may adopt technical standards in HIT certification criteria that are insufficient to create interoperable HIT systems because they may receive insufficient feedback from HIT system users on problems involving healthcare data exchanges. For users of certified systems, ONC does not mandate case reports of instances where certified HIT systems don't interoperate. Individual medical practitioners or patient safety organizations may notice patterns in poor interoperability of HIT systems but may be unable to understand the full scope of the problems and report them in an actionable format. Furthermore, not all care facilities and laboratories use certified HIT systems and may not use the specific standard(s) adopted by the ONC. There may be nowhere for users of non-certified HIT to report safety-related concerns. Feedback to the ONC may primarily involve their standards and programs and the ONC may not have the capacity to analyze other reports.
Scenario 21-2: (B)	ONC may adopt technical standards in HIT certification criteria that are insufficient to create interoperable HIT systems because not all HIT systems are certified by the ONC. This may occur because only certain care facilities and physician practices fell under categories that allowed them to get incentives for acquiring certified EHRs [97]. Current programs for Promoting Interoperability only apply to clinicians, eligible hospitals and critical access hospitals utilizing certified HIT systems. Laboratories, among others, were not included in programs that offered financial incentives for adopting certified EHRs and are currently not included in programs that tie funding to ONC certified system usage.

Category/ Scenario #	Scenario Description
Control Action:	**Adopt technical standards in HIT certification criteria**
UCA Type:	**Too late/ too early/ out of order**
UCA:	**ONC adopts technical standards in HIT certification criteria too late after HIT systems are already deployed**
Scenario 22-1: (B)	ONC may adopt technical standards in HIT certification criteria too late because the ONC takes 3-5 years to get legislation from mandate from Congress to use in EHRs. The conditions that inspired the mandate may have been worsening throughout the time delay. The HIT companies may also use the comment periods during that time to weaken any regulatory oversight that they view as too onerous.
Scenario 22-2: (B)	ONC may delay adopting regulatory standards to wait for a sector of industry to develop before adopting regulation. The ONC may have sought to give flexibility to industry to gain necessary implementation experience given how frequently some standards are updated as new technology is developed.

Category/ Scenario #	Scenario Description
Control Action:	**Certify EHR as meeting current certification requirements**
UCA Type:	**Providing causes hazard**
UCA:	**ONC certifies EHR that does not meet current certification requirements**
Scenario 23-1: (A)	ONC may approve an EHR system that may not meet certification requirements if the EHR vendor fraudulently represented their EHR to the ONC / ONC-ACB at the time. For example, the EHR may have been hard coded to pass certain certification tests that it could not pass in the field. The ONC/ONC-ACB may not be aware of deceptive practices unless a user or employee alerts them to the fraudulent activity. Users may not be aware of the certification criteria and may not know how to report a violation if encountered. Additionally, certification organizations may have certified only a "model" software rather than a specific implementation at a site. Though health IT certification organizations (ONC-ACBs) *can* randomly audit health IT implementations "in the field", ONC may not enforce that such audits actually occur. Historically, ONC-ACBs have conducted random audits on 2% of accredited programs, but currently audits only occur reactively when they receive complaints about particular programs [94].

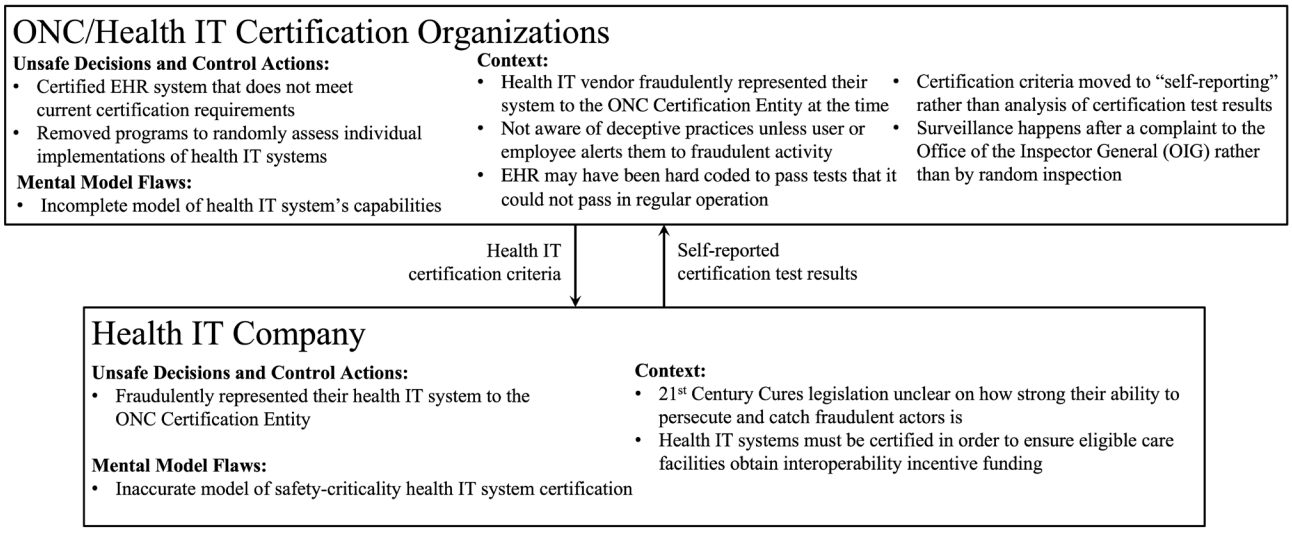

Figure 15. Visualization of scenario 23-1

Controller: FDA

Category/ Scenario #	Scenario Description
Control Action:	**Approve IVD device**
UCA Type:	**Providing causes hazard**
UCA:	**FDA approves an IVD device that does not perform to expected performance levels**
Scenario 24-1: (C)	The FDA might approve an IVD device that does not perform to expected performance levels because they compared it to a previously approved product, where a regulatory decision may have been made with inadequate validation data. Because approval is often based on comparisons, if another device was approved on inadequate validation data, it is now easier for more devices to be approved from that same data.
Scenario 24-2: (B)	The FDA might approve an IVD device that does not perform to expected performance levels because there are not enough resources or time to perform controlled clinical trials on all IVD devices prior to approval, especially in emergency use authorization situations. Additionally, after deployment of the device, data from different facilities utilizing that device may have been coded differently and not be aggregable in a way that reveals the device's performance issues, due to lack of standardization for reporting IVD performance data to the FDA.

Category/ Scenario #	Scenario Description
Control Action:	**Issue corrective action to IVD manufacturer**
UCA Type:	**Too Early, too late, out of order**
UCA:	**FDA issues corrective action to IVD manufacturer too late following a series of inappropriate results from IVD device**
Scenario 25-1: (A)	The FDA may issue corrective action to IVD manufacturer too late following a series of inappropriate results from IVD device (UCA). One contributing factor may be that an IVD malfunction may not lead to a safety signal that is detectable or actionable by the FDA. This may occur because the FDA are not getting all reports from care facilities about invalid or inaccurate results, since this reporting is voluntary and considered passive surveillance. The FDA may not be aware that the few reports they do get are indicative of a larger trend regarding a device. Care facilities or laboratories may not report all errors because they are not required to report unless there was clear harm caused. They may also not have realized that the tests were providing inaccurate results if the error was subtle enough to not be quickly detectable. Minor problems may only be reported to IVD manufacturers, many of whom are based internationally and cannot have their quality programs easily inspected by the FDA due to a backlog stemming from factors like high demand for diagnostic tests or international border restrictions. Even if the FDA can arrange a directed inspection of a manufacturer quickly, without appropriate reporting they may not know to prioritize an inspection. FDA may also not get all reports from care facilities or laboratories because post-market performance studies may not be conducted or completed for all devices. The FDA may not

Category/ Scenario #	Scenario Description
	have the ability to fund all post-market studies, so studies may be conducted by industry, payors, or academia and results may not reach the FDA in a standardized format. Additionally, laboratory data available to care facilities may contain little to no information about what specific device/test methodology was used (e.g., through a unique device identifier), making further investigation into device performance difficult. Post-market performance data collected by IVD manufacturers might use data aggregated from different facilities across different geographic or demographic profiles. The data from those different facilities may have been coded differently and not aggregated in a way that reveals the performance issues, due to lack of standardization for reporting IVD performance data to the FDA. IVD manufacturers may also not be incentivized to report negative research findings to the FDA.
Scenario 25-2: (B)	The FDA might attempt to issue corrective action to an IVD manufacturer in the form of an injunction/recall following a pattern of inappropriate results from IVD device, but that action may not go through because the Department of Justice assigns it a low-priority status or decides against litigation. This decision may be informed by the volume of devices affected or the level of perceived risk. This may occur because of a pattern of treating IVD devices as "not directly responsible" for an adverse event, as the incorrect or misleading test result is not what directly harms the patient, it is rather the incorrect treatment provided later.
Scenario 25-3: (B)	The FDA might not issue corrective action to an IVD manufacturer following a pattern of inappropriate results from IVD device because the invalid or inaccurate results are not deemed safety-critical enough to warrant corrective action. This may occur because of a pattern of treating IVD devices as "not directly responsible" for an adverse event, as the incorrect or misleading test result is not what directly harms the patient, it is rather the incorrect treatment provided later. This may also occur because the health hazard analysis performed by the IVD manufacturer during development attributed a low risk level to the device. The risk threshold set for the device might not match the disease risk level based on an incorrect diagnosis. This may be because the form of test is novel (e.g., genomic or personalized tests) and their risks are not fully understood by the IVD manufacturer or the FDA.

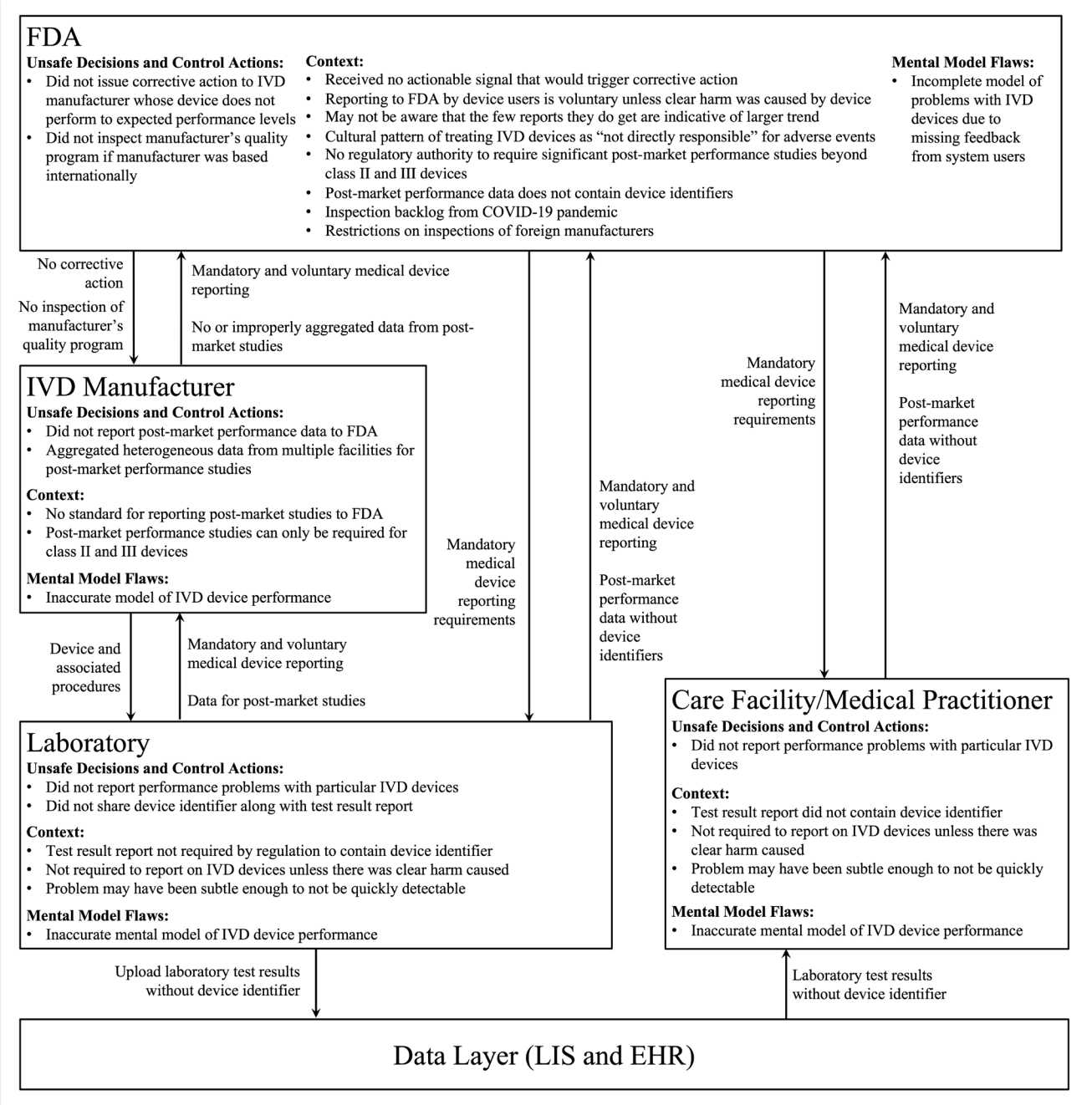

Figure 16. Visualization of Scenario 25-1

Controller: IVD Manufacturer/Importer

Category/ Scenario #	Scenario Description
Control Action:	**Associate IVD device output to reference terminology codes**
UCA Type:	**Not providing causes hazard**
UCA:	**IVD manufacturer does not associate device output to reference terminology codes when device output needs to be shared with external facilities**
Scenario 26-1: (B)	IVD manufacturer may not associate device output to reference terminology codes because different reference terminologies are more widely used in some geographic regions, and the manufacturer may export to regions using different reference terminologies. There is no regulatory or statutory incentive for IVD manufacturers to associate their device outputs to reference terminology, as well as no industry incentive as individual laboratories are capable of linking outputs to local codes.
Scenario 26-2: (B)	IVD manufacturer may not associate device output to reference terminology codes because associating reference terminology may require software modifications to equipment that has been operational for extended periods of time, potentially leading to interruptions in service. There is no regulatory or statutory incentive for IVD manufacturers to associate their device outputs to reference terminology, as well as no industry incentive as individual laboratories are capable of linking outputs to local codes.

Controller: Payor

Category/ Scenario #	Scenario Description
Control Action:	**Provide coverage/reimbursement for laboratory test**
UCA Type:	**Not providing causes hazard**
UCA:	**Payor does not provide coverage/reimbursement for a laboratory test that may provide value to an individual patient's case**
Scenario 27-1: (B)	Payor may not provide coverage for a test that may provide value to an individual patient's case if CMS does not cover the lab test, despite it having FDA clearance. The test may be the best for the patient's case, but the CMS may not view it as being enough of an improvement over other available options to merit increased costs of covering that test. This occurs because the FDA scrutinizes tests based on safety and efficacy, while CMS scrutinizes them based on reasonableness and necessity.

Category/ Scenario #	Scenario Description
Control Action:	**Provide additional preventative healthcare/well-being services to patients**
UCA Type:	**Stopped too soon / applied too long**

Category/ Scenario #	Scenario Description
UCA:	**Payor stops providing additional preventative healthcare/well-being services that patients are actively utilizing**
Scenario 28-1: (B)	Payor may stop providing preventative healthcare/well-being services that patients are actively utilizing if the payor does not receive funding from CMS due to not having achieved the necessary quality measures. This may occur if the payor does not receive the necessary clinical data (e.g., receiving only what kind of test was done and not the result, or patient's clinical context) in order to meet all quality metrics imposed by CMS. This may occur if the payor cannot negotiate a data sharing agreement with a laboratory or practitioner due to patient privacy concerns or interoperability issues. The laboratory who typically files the claim may also not possess all the clinical data that the payor needs for quality purposes. There is no regulatory requirement for what data elements need to be shared with payors for quality purposes.

Controller: Naming/Coding/Messaging (NCM) Standards Development Organizations (SDO) & Reference Libraries

Category/ Scenario #	Scenario Description
Control Action:	**Create/release new reference terminology**
UCA Type:	**Too early, too late, out of order**
UCA:	**SDO creates/releases new reference terminology too late after a new type of diagnostic test is developed or disease/condition is identified**
Scenario 29-1: (B)	The SDO may release the reference terminology too late because some terminologies only have regular updates every six months, and there may not be an appropriate system for requesting the terminology release to be expedited. The lab/care facility may have needed to create temporary local codes in the meantime. Because this happens somewhat regularly, labs/care facilities often prefer to keep local code systems in parallel with reference terminology codes.

Category/ Scenario #	Scenario Description
Control Action:	**Create/release new reference terminology**
UCA Type:	**Providing causes hazard**
UCA:	**SDO creates/releases reference terminology or messaging standard that does not sufficiently standardize communication between users.**
Scenario 30-1: (A)	The SDO may release reference terminology that does not sufficiently standardize communication between users because their terminology does not capture enough information to adequately identify a test/disease. That may occur because the individual codes do not capture contextual information regarding a specific instance of a test/disease, such as the specific test kit used to perform one instance of a test, or the body site at which a condition has manifested.

Category/ Scenario #	Scenario Description
	This may occur because reference terminology SDOs are not tasked with capturing all contextual information regarding a specific instance of a test/disease, as they operate under the assumption that HIT systems and their associated messaging standards will include additional fields for contextual information about a specific instance of a test/disease. SDOs are typically consensus organizations and ideally, clinical information is modeled in a manner that is most efficient for use by implementers for many different use cases with a wide range of requirements. Therefore, there is not a single model that is used, and clinical information may need to be available in multiple forms. Each member of the consensus organization may thus have goals that conflict with those of other members, and standards may be written loosely to compromise to each member's goals.
Scenario 30-2: (A)	The SDO may release reference terminology that does not capture enough information to adequately identify a test/disease because the reference terminology is made up of multiple terminology standards that are poorly integrated. This results in difficulty with determining how codes/terms in HIT systems represent equivalent concepts and results in incorrect usage of standards due to multiple representations and overlapping concepts, resulting in confusion of which standard to use leading to errors of omission and commission which could lead to incorrect diagnosis or treatment.

Category/ Scenario #	Scenario Description
Control Action:	**Provide reference terminology mapping guidelines**
UCA Type:	**Providing causes hazard**
UCA:	**SDO provides conflicting or ambiguous reference terminology mapping guidelines following safety-critical terminology release**
Scenario 31-1: (B)	The SDO may provide conflicting or ambiguous reference terminology mapping guidelines because they may not be aware that the guidelines are conflicting or ambiguous. It may be the case that SDOs developing two or more different reference terminologies disagree on the best approach to mapping new terminologies, and each SDO releases mapping guidelines for their own terminology that conflict with the guidelines of the other SDO. There may be no formalized line of communication between different SDOs to ensure consistency in mapping guidelines.
Scenario 31-2: (A)	The SDO may provide conflicting or ambiguous reference terminology mapping guidelines because they may not be aware that the guidelines are conflicting or ambiguous. This may occur because mapping reference terminology may be subject to different interpretations by the individuals performing the mapping. Additionally, there may not exist a process for receiving and processing user reports of conflicting or ambiguous reference terminology. Regulatory or statutory incentive for SDOs to receive and process user reports are inadequate.

Category/ Scenario #	Scenario Description
Control Action:	**Provide messaging standard implementation guides**
UCA Type:	**Providing causes hazard**
UCA:	**SDO provides conflicting or ambiguous implementation guides following safety-critical messaging standards update**
Scenario 32-1: (B)	The SDO may provide conflicting or ambiguous implementation guides because they use inconsistent models for the format and content of recording clinical statements. This may occur because, ideally, clinical information is modeled in a manner that is most efficient for use by implementers for many different use cases with a wide range of requirements. Therefore, there is not a single model that is used, and clinical information may be available in multiple model forms. This poses a challenge for analysis of aggregate information because meaningful use of the data requires a common format and semantics, but currently, the data is highly variable. Additionally, there may not exist a process for receiving and processing user reports of conflicting or ambiguous implementation guides, as the guides may have been released without direct communication/support from the SDO to the care facility in interpreting the guide.

Controller: Patient

Category/ Scenario #	Scenario Description
Control Action:	**Follow laboratory pre-test instructions or test procedures**
UCA Type:	**Not providing causes hazard**
UCA:	**Patient does not follow laboratory pre-test instructions or test procedures when procedures are necessary for validity of test results (e.g., does not fast, etc.)**
Scenario 33-1: (C)	A patient may not follow laboratory pre-test instructions or test procedures because they are not aware of the laboratory pre-test instructions or test procedures. This may have occurred because the patient was never provided the laboratory pre-test instructions or test procedures. This may occur if both the laboratory and the physician believed the other party provided the patient the lab pre-test instructions or test procedures.
Scenario 33-2: (B)	A patient may not follow laboratory pre-test instructions or test procedures because they are not aware of the lab pre-test instructions or test procedures. This may have occurred because the patient was never provided with the lab pre-test instructions or test procedures. This may happen if the lab pre-test instructions or test procedures were provided only through an electronic interface that the patient is unable to access.
Scenario 33-3: (C)	A patient may not follow laboratory pre-test instructions or test procedures because they were unable to interpret the instructions. This may have occurred because the patient was provided the lab pre-test instructions or test procedures in a language (e.g., English vs. Spanish) or in terminology (e.g., using excessive jargon) they are unable to understand.
Scenario 33-4: (C)	A patient may not follow laboratory pre-test instructions or test procedures because they are unaware of the criticality of following instructions. This may have occurred if the instructions were only communicated indirectly (e.g., email, portal, etc.), and the criticality

Category/ Scenario #	Scenario Description
	of following such procedures was not emphasized by the ordering physician.
Scenario 33-5: (C)	A patient may not follow laboratory pre-test instructions or test procedures because they are unable to consult test procedures after the individual appointment. This may have occurred if the test procedures were only communicated verbally to the patient and not accessible either in writing or through an electronic interface.

Category/ Scenario #	Scenario Description
Control Action:	**Make/attend laboratory appointment**
UCA Type:	**Not providing causes hazard**
UCA:	**Patient does not make/attend laboratory appointment when laboratory results are necessary to inform care plan**
Scenario 34-1: (C)	A patient may not attend a laboratory appointment because they cannot access the laboratory at which the test is to be performed. This may occur for reasons including geographic isolation (e.g., takes too long to get to the lab, lab is not on public transportation routes, patient lives in rural environment), limited patient mobility, patient cannot afford test which is not covered by payor, among others.
Scenario 34-2: (C)	A patient may not attend a laboratory appointment because they are unaware of the criticality of performing the test. This may have occurred if the need for a test was only communicated indirectly (e.g., email, portal, etc.), and the criticality of that test result to the care plan was not emphasized by the ordering physician. It may also occur if the patient does not have the information needed to make the decision to seek care and additional testing.
Scenario 34-3: (B)	A patient may not attend a laboratory appointment because they do not believe the lab results are trustworthy enough to merit the time and cost of performing the test. This may occur if the patient has had prior negative experiences with diagnostic test results, or if guidance from public health authorities surrounding diagnostic test results has fluctuated in the past. That guidance may fluctuate because public health authorities do not collect data on specific diagnostic devices used, only on the type of test performed (e.g., COVID test, but not what brand/type). Though PHAs may have patient identifiers and may be able to match laboratory results to other data elements (e.g., vaccination records), it may take heavy manual effort. Additionally, data containing patient identifiers may also not have been collected in a format that is shareable while preserving patient privacy.
Scenario 34-4: (C)	A patient may not make a laboratory appointment because laboratory draw hours do not align with patient availability. This might occur if laboratory draw hours do not match the clinic hours and this information is not readily accessible to the patient. Additionally, work or other personal commitments of the patient may conflict with the laboratory's draw hours. The laboratory may also have high demand such that there are long waits to perform testing, or no appointments are available.
Scenario 34-5: (C)	A patient may not make a laboratory appointment because they are unable to contact the care facility or medical practitioner to inquire about their condition and potential treatment options. This may occur if patients are unable to contact the practitioner/clinic directly over the phone (e.g., can only obtain nurse advice), or if phone wait times are too long.

Category/ Scenario #	Scenario Description
Scenario 34-6: (C)	A patient may not make a laboratory appointment because they are unsure of how to make the appointment with the lab. This might be because the lab is in a different location than their PCP or other healthcare provider.
Scenario 34-7: (C)	A patient may not attend a laboratory appointment because they realize that CMS does not cover the lab test, despite it having FDA clearance. The test may be the best for the patient's case, but the CMS may not view it as being enough of an improvement over other available options to merit increased costs. This occurs because the FDA scrutinizes tests based on safety and efficacy, while CMS scrutinizes them based on reasonableness and necessity.

***Controller*: CDC/PHAs**

Category/ Scenario #	Scenario Description
Control Action:	**Set standards for reporting of diagnostic data from laboratories**
UCA Type:	**Providing causes hazard**
UCA:	**CDC/PHAs set standards for reporting of diagnostic data that laboratories are unable to comply with**
Scenario 35-1: (B)	CDC/PHAs may set standards for reporting of diagnostic data that would be helpful for identifying trends in diagnostic results, but laboratories are unable to comply because the standards are too onerous for labs to follow. The standards may be too onerous if the information requested is outside of the scope of normally collected data for diagnostic testing. The data might exist on the EHR side of the system but not be transmitted to the laboratory or may never have been collected. In addition, even if the requested data exists in the EHR, the laboratory may be unable to develop new data sharing protocols that would allow them to report the requested data to the CDC/PHA.
Scenario 35-2: (B)	CDC/PHAs may set standards for reporting of diagnostic data that would be helpful for identifying trends in diagnostic results, but laboratories are unable to comply because the standards are too onerous for labs to follow. The standards may be too onerous if there is high sensitivity to the data being transmitted to and from laboratories out of privacy/social concerns (e.g., occupation and place of employment might be useful for tracking disease outbreaks, but may raise privacy concerns with patients).

Category/ Scenario #	Scenario Description
Control Action:	**Provide healthcare guidance**
UCA Type:	**Providing causes hazard**
UCA:	**CDC/PHAs provide healthcare guidance that conflicts with current/previous guidance**

Scenario 36-1: (A)	CDC/PHAs may provide healthcare guidance that conflicts with current/previous guidance if they receive conflicting diagnostic data or had originally received insufficient diagnostic data with which to provide guidance. This may be because the lack of good consistent healthcare data encoding of rare conditions makes it difficult for researchers and practitioners to understand how the existing data may compare in order to better inform guidance decisions. This could also be for conditions that are more common but better data availability could also inform better care opportunities. There is no regulatory authority on the part of the CDC to require that specific data elements be shared, so that they may provide better guidance to medical practitioners (e.g., knowing whether the patient was pregnant or not along with a Zika result). Currently, requiring that specific data elements get shared with CDC would require action from ONC and CMS as well. Promoting interoperability programs only apply to clinicians, eligible hospitals and critical access hospitals and don't apply to laboratories.
Scenario 36-2: (C)	CDC/PHAs may provide healthcare guidance that conflicts with current/ previous guidance if they receive conflicting diagnostic data or had originally received insufficient diagnostic data with which to provide guidance. This may be because of a lack of diagnostic tests being performed for new or uncommon conditions. There may also be a lack of diagnostic information available if tests were done in uncommon environments (e.g., drive-thru COVID tests, etc.).
Scenario 36-3: (B)	CDC/PHAs may provide healthcare guidance that conflicts with current/ previous guidance if they receive conflicting diagnostic data or had originally received insufficient diagnostic data with which to provide guidance. This may be because of an inability to link diagnostic test data with immunization data, due to deidentification of patient data at the state health agency level for preservation of privacy. This may be a result of existing state laws, or perceived requirements at the state level.

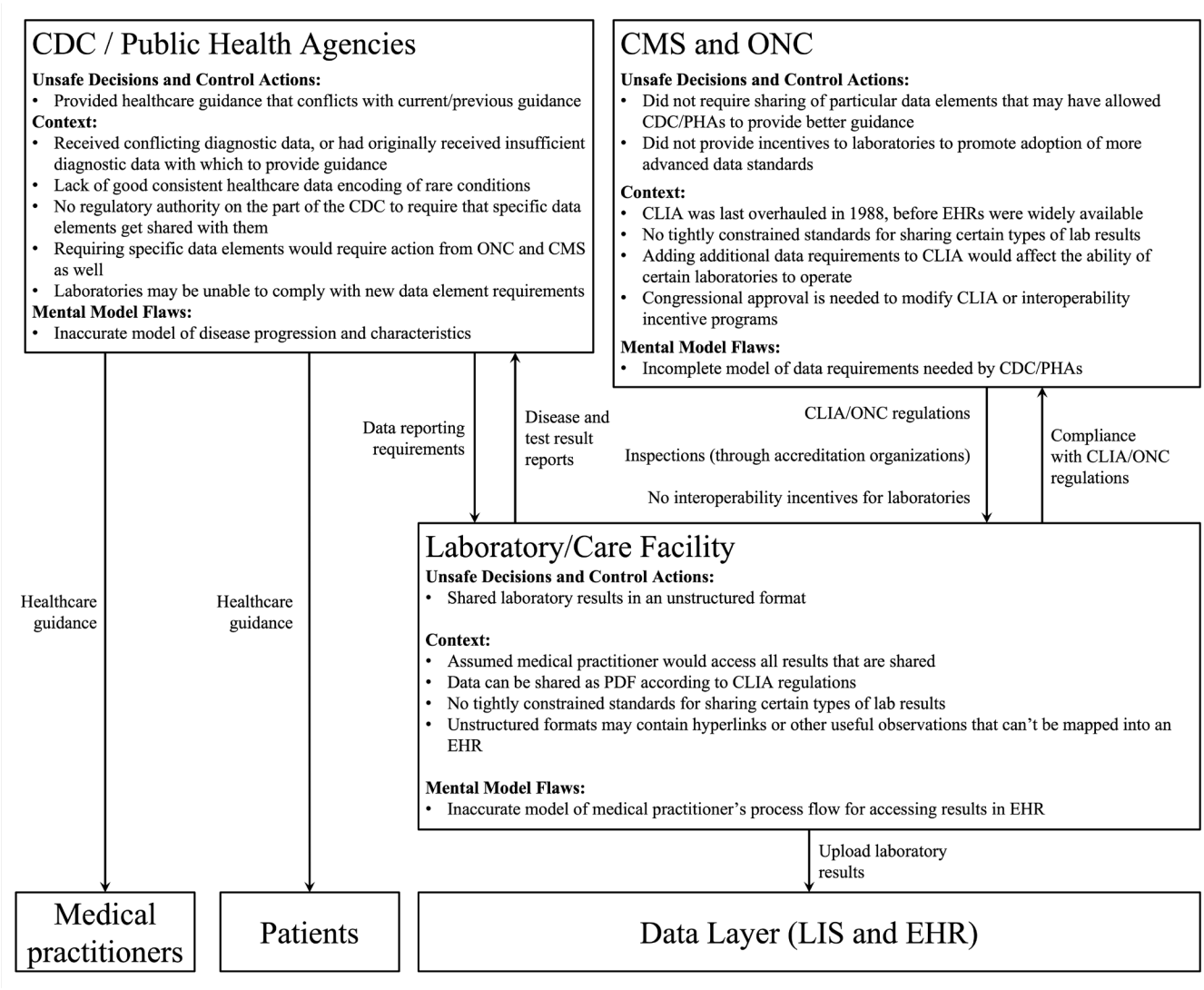

Figure 17. Visualization of scenario 36-1

Controller: Laboratory/Personnel Accreditation Organization

Category/ Scenario #	Scenario Description
Control Action:	**Provide accreditation to laboratory**
UCA Type:	**Providing causes hazard**
UCA:	**Laboratory accreditation organization provides accreditation to laboratory without being able to enforce minimum interoperability requirements**
Scenario 37-1: (B)	A laboratory accreditation organization may provide accreditation to a laboratory without being able to enforce minimum interoperability requirements because laboratories are accredited according to the requirements enshrined in CLIA, which was written at time when laboratory data interoperability was not a major consideration or priority. Therefore, data interoperability was not explicitly written into the statute, and inspections are focused only on the quality and safety of laboratory testing operations, rather than interoperability requirements.

Controller: HHS Administration

Category/ Scenario #	Scenario Description
Control Action:	**Determine responsibilities of component agencies**
UCA Type:	**Not providing causes hazard**
UCA:	**HHS does not assign any agency responsibility over safety-critical component of laboratory data ecosystem**
Scenario 38-1: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because they believe industry is self-regulating. This may be due to a lack of feedback from care facilities and medical providers of issues that have been impacting care.
Scenario 38-2: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because they believe the gap is covered by existing responsibilities. This may be because the feedback they receive is not high enough quality to identify gaps that do exist.
Scenario 38-3: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because they do not believe they have the jurisdiction to assign responsibility over that component. This may be because they were sued for prior attempts to cover the perceived gaps or because there is direct verbiage in federal laws that prohibit certain regulations.
Scenario 38-4: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because the gap is new and undetected due to a development of novel technology. This may be because HHS is a massive organization and the gap may take a while to trickle up from the first person who detects it, to HHS admin, and then to go through

Category/ Scenario #	Scenario Description
	the necessary steps to regulate it.
Scenario 38-5: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because of a lack of funding support to go alongside the new responsibility. This may be because funding support decreases across the board or is kept level year over year which limits the ability to regulate new areas effectively unless other areas are neglected.
Scenario 38-6: (B)	HHS may not assign any agency responsibility over a safety-critical component of laboratory data ecosystem because the responsibility is outside of the scope of an existing agency but is not big enough to merit creating a new agency.

Category/ Scenario #	Scenario Description
Control Action:	**Determine responsibilities of component agencies**
UCA Type:	**Providing causes hazard**
UCA:	**HHS assigns agencies overlapping regulatory responsibilities**
Scenario 39-1: (B)	Overlapping responsibilities may be assigned because of dynamic technological growth of industry. Agencies may not have the bandwidth to sufficiently add new requirements as they arise. Sometimes agencies may contract with other agencies within HHS to help build up new programs. This can help alleviate bandwidth concerns immediately but can hinder inter-agency coordination over time.
Scenario 39-2: (B)	Overlapping responsibilities may be assigned because they are not seen as overlapping due to preexisting expertise of various agencies. This could be because technically the final work is different but involves so much similar administrative or technical work that there is significant duplicative work being done across agencies. This may be because many agencies have similar concerns (like interoperability) and are all trying to use available resources to improve it but do not have the ability to know exactly what is happening at all HHS agencies at any given time.
Scenario 39-3: (B)	Overlapping responsibilities may be assigned because of insufficient coordination when distributing roles across organizations. Allocation of responsibilities may be done project by project because there are so many components to HHS that complete redesign would be slow, complicated, and expensive.

Controller: Congress/White House

Category/ Scenario #	Scenario Description
Control Action:	**Update Federal regulatory authority's statutory boundary**
UCA Type:	**Stopped too soon/ applied too long**
UCA:	**Congress/White House updates a Federal regulatory authority's statutory boundary in a way that removes components that were critical for safe control loop design**
Scenario 40-1: (B)	Congress/White House updates a Federal regulatory authority's statutory boundary in a way that removes components that were critical for safe control loop functionality. One factor that may lead to this change is industry pressure that asserts that the regulations are too taxing. The federal government may not realize how important the regulations were for constraining behavior in a certain way, and there may be unintended consequences for removing the regulations.

Category/ Scenario #	Scenario Description
Control Action:	**Expand Federal regulatory authorities' statutory boundaries**
UCA Type:	**Not providing causes hazard**
UCA:	**Congress/White House do not expand federal regulatory agencies' statutory boundary to cover technologies that have emerged or undergone significant changes since previous statutory boundaries were enacted.**
Scenario 41-1: (B)	Congress/White House may not expand statutory boundaries because they believe the technology has not changed sufficiently to require additional regulation. This may be influenced by IVD manufacturers having a strong lobbying presence in the Federal Government and IVD manufacturers believe stronger regulations would negatively impact their commercial success.
Scenario 41-2: (B)	Congress/White House may not expand statutory boundaries because they believe the current regulations are sufficient despite changes in technology. They may believe this be because there is not sufficient data tracking the problems occurring in the new space. Data may not be available because it is a new space and data tracking mechanisms are either underdeveloped, underfunded, or are suppressed by commercial interests who do not want there to be increased interest in new regulations.
Scenario 41-3: (B)	Congress/White House may not expand statutory boundaries because they believe that would create too big of a burden on industry. This could be because they fear intense regulations on a new or small industry could damage innovation potential. This fear may come from direct influence from industry, political ideologies, or past experiences.
Scenario 41-4: (B)	Congress/White House may not expand statutory boundaries because they do not want to allocate more funds towards that regulatory sector. New regulations may require additional funding that is unavailable.

Category/ Scenario #	Scenario Description
Scenario 41-5: (B)	Congress/White House may not expand statutory boundaries on emergent technology because changes to the regulated industry are so extreme that no current regulatory body is set up to regulate the technology. These extreme changes may also make it difficult to pass legislation that fully encapsulates the problem, and different groups may disagree on what aspects should and can be regulated in addition to if and how regulation should impact growth in a new industry.

Category/ Scenario #	Scenario Description
Control Action:	**Expand Federal regulatory authority's statutory boundaries**
UCA Type:	**Providing causes hazard**
UCA:	**Congress/White House expand regulatory authority's statutory boundaries in a way that diminishes the safety of the regulated industry**
Scenario 42-1: (B)	Congress/White House may expand regulatory authority's statutory boundaries without providing sufficient funding that enables the regulatory body to enforce everything they are tasked with enforcing. The agency may not have the resources to create or enforce new regulations and attempts to expand their scope may pull resources away from other critical regulations.
Scenario 42-2: (B)	Congress/White House may expand regulatory authority's statutory boundaries in a way that causes significant slowdown in the development and release of new safety-critical technologies. This may be because the regulations had unintended consequences or caused inadvertent incentives for malicious conduct.
Scenario 42-3: (B)	Congress/White House may expand regulatory one authority's statutory boundaries in a way that creates overlap with other regulatory authority's boundaries. Assigned overlap may stem from disjoint efforts

Appendix E – Glossary of Acronyms/Terms

Acronym	Definition
CAP	*College of American Pathologists* provides laboratory accreditation and proficiency testing services.
CAST	*Causal Analysis based on System Theory* (an MIT Model) is an approach to identify the questions that need to be asked during an accident investigation and determine why the accident occurred. **Additional Resource**
CDC	*U.S. Centers for Disease Control and Prevention* is the United States' leading science-based, data-driven, service organization that protects the public's health. It is a federal agency under HHS.
CDS	*Clinical Decision Support* provides clinicians staff and patients with knowledge and person specific information that is filtered and presented at appropriate times. **Additional Resource**
CLIA	*Clinical Laboratory Improvement Amendments,* passed by Congress in 1988, ensures quality laboratory testing. There are currently 320,865 labs that are CLIA certified. **Additional Resource**
CMS	*U.S. Centers for Medicare and Medicaid Services* is a federal agency under HHS that provides insurance and medical services for the United States' civilians who might not be able to afford care otherwise, including disabled peoples, low-income families, people 65 years old and older, pregnant women, and people who need long term care.
EHR	An *Electronic Health Record* is a digital version of a patient's medical chart.
FDA	*U.S. Food and Drug Administration* is a federal agency under HHS that focuses on regulating food, drugs, medical devices, radiation-emitting products, vaccines, blood, biologics, animal and veterinary products, cosmetics, and tobacco products in the United States.
FHIR	*Fast Healthcare Interoperability Resources* employs RESTful web services such as JSON and RDF data formats. Web services approach that makes it easier for systems to exchange specific data/information. **Additional Resource**
FMEA	The *Failure Mode and Effects Analysis* approach is used to identify all possible failures in a design, process, or service. **Additional Resource**
HHS	*U.S. Department of Health and Human Services* is the parent organization over twelve federal divisions, including CDC, CMS, FDA, NIH, and ONC. The mission of the U.S. Department of Health and Human Services (HHS) is to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. **Additional Resource**
HIE	*Health Information Exchange* is a process/system that allows clinicians to access and securely share patient medical records electronically.
HIT	*Health Information Technology* Includes electronic health records (EHR), laboratory information systems (LIS), etc.

Acronym	Definition
HL7	*Health Level 7* refers to international standards for transfer of administrative and clinical data between software applications used by many different healthcare providers. *LOINC codes are typically embedded in HL7 messages.* **Additional Resource**
HRO	*High Reliability Organizations* operate in high-hazard domains during extended periods of time without failures. Example organizations would be a nuclear power plant or air traffic control systems. **Additional Resource**
IVD	*In vitro diagnostics* are tests conducted in laboratories (i.e., bio samples such as spit or blood). It detects diseases and other bodily disorders. **Note:** There are differences in IVD products and calibration techniques which are not reflected in current electronic lab data. **Additional Resource**
LIS	*Laboratory Information System* is a computer system that helps manage aspects of a medical laboratory.
LIDR	*Laboratory Information Data Repository* is a concept promoted in the SHIELD Community Roadmap. Objectives include improving data quality in the LIDR, have IVD manufacturers assign codes using SHIELD's direction, and then submitting the codes to the LIDR.
LIVD	*LOINC-to-IVD* specifications define IVD industry format for use by lab personnel or application and focus on describing the same laboratory tests from the same vendor in the same manner across all labs. **Additional Resource**
LOINC	*Logical Observation Identifiers Names and Codes* is a database and universal standard for identifying medical laboratory observations. First developed in 1994, it was created and is maintained by the Regenstrief Institute, a US nonprofit medical research organization. LOINC was created in response to the demand for an electronic database for clinical care and management and is publicly available at no cost. **Additional Resource**
NIH	*National Institutes of Health* is a federal agency under HHS made up of centers and institutes that focus on medical research.
NLM	*National Library of Medicine*, a part of NIH, is the world's largest biomedical library.
ONC	*Office of the National Coordinator for Health Information Technology* is an organization under HHS that leads Health IT efforts.
PHA	*Public Health Agency*
RCA	*Root Cause Analysis* is the process of discovering the root causes of problems in order to identify appropriate solutions. **Additional Resource**
SDO	*Standards Development Organizations.* Includes LOINC, SNOMED, HL7, etc.
SNOMED	*Systematized Nomenclature of Medicine* systematically organized computer-processable collection of medical terms providing codes, terms, synonyms and definitions used in clinical documentation

Acronym	Definition
	and reporting. SNOMED CT is the most comprehensive, multilingual clinical healthcare terminology in the world. **Additional Resource**
STAMP	MIT's *System-Theoretic Accident Model and Processes* model is a systems approach to safety engineering that is founded on the concepts that accidents are part of a process and are control problems, which can be avoided by enforcing restraints and improving interactions. **Additional Resource**
STPA	*System-Theoretic Process Analysis* is a hazard and accident analysis technique built on the STAMP model. This technique helps to identify unsafe control actions and causal factors/control flaws. **Additional Resource**
UCA	An *Unsafe Control Action* is a control action that, in a particular context and worst-case environment will lead to a hazard. **Additional Resource**
USCDI	*ONC's United States Core Data for Interoperability* is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange. **Additional Resource**