System Safety within Laboratory Data Exchanges Report Executive Summary

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.