Application of STPA to the U.S. Diagnostic Laboratory Data Ecosystem

Rodrigo Rose, Graduate Assistant
Polly Harrington, Graduate Assistant
Prof. Nancy Leveson, PhD
John Thomas, PhD
Massachusetts Institute of Technology

Stephen Powell, DHA, MSc
Daniel Wyman, MD, MPH
Alana Keller, BA, PMP®
Synensys

For U.S. FDA Contract # 75F40122C00112

June 7th, 2023

Disclaimer

- The opinions expressed in this presentation are those of the research team members. 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.

2

The Problem

- NIH estimates about 400,000 hospitalized patients experience preventable harm every year, with approximately 100,000 dying from medical errors
- Diagnostic testing data plays a significant role in the safety and reliability of the patient diagnostic and treatment process.

Specific Goals for this Research (FDA)

- Assess and evaluate the safety of the current laboratory data ecosystem using a system safety engineering approach
- Envision a future system redesign to address the hazards by implementing new or redesigned control structures
- Demonstrate and justify the urgency for system redesign to address critical hazards and risks to public health.

Losses and Hazards

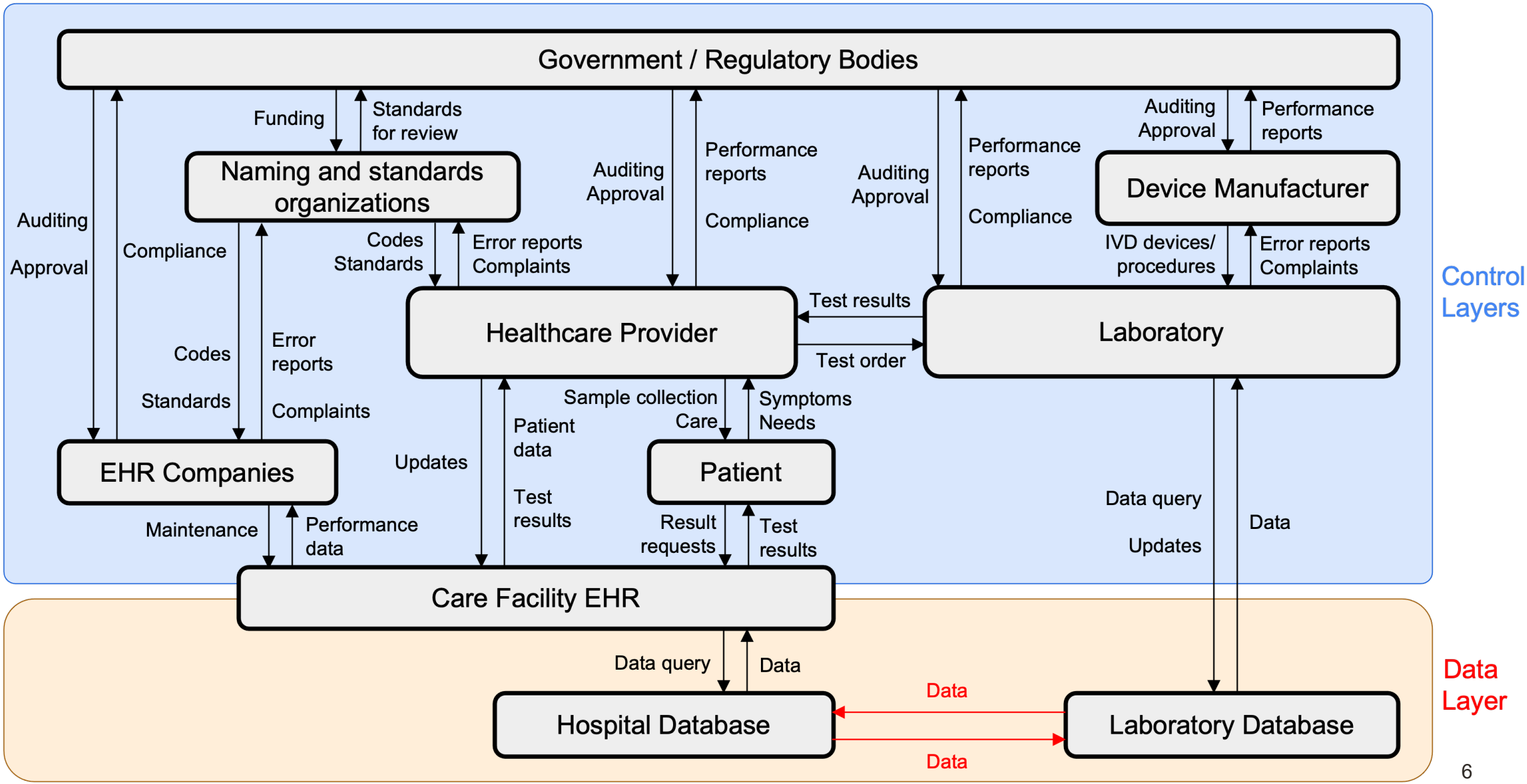
- Diagnostic Laboratory loss examples:
  - Loss of life or injury to patient or personnel
  - Loss of reputation or trust in laboratory data ecosystem

- Diagnostic Laboratory hazard examples:
  - Patients receive less than the acceptable standard of care
  - Person is exposed to harm during testing process
  - Laboratory ecosystem stakeholders including patients (the public) lose trust in data being collected, shared, analyzed, and reported

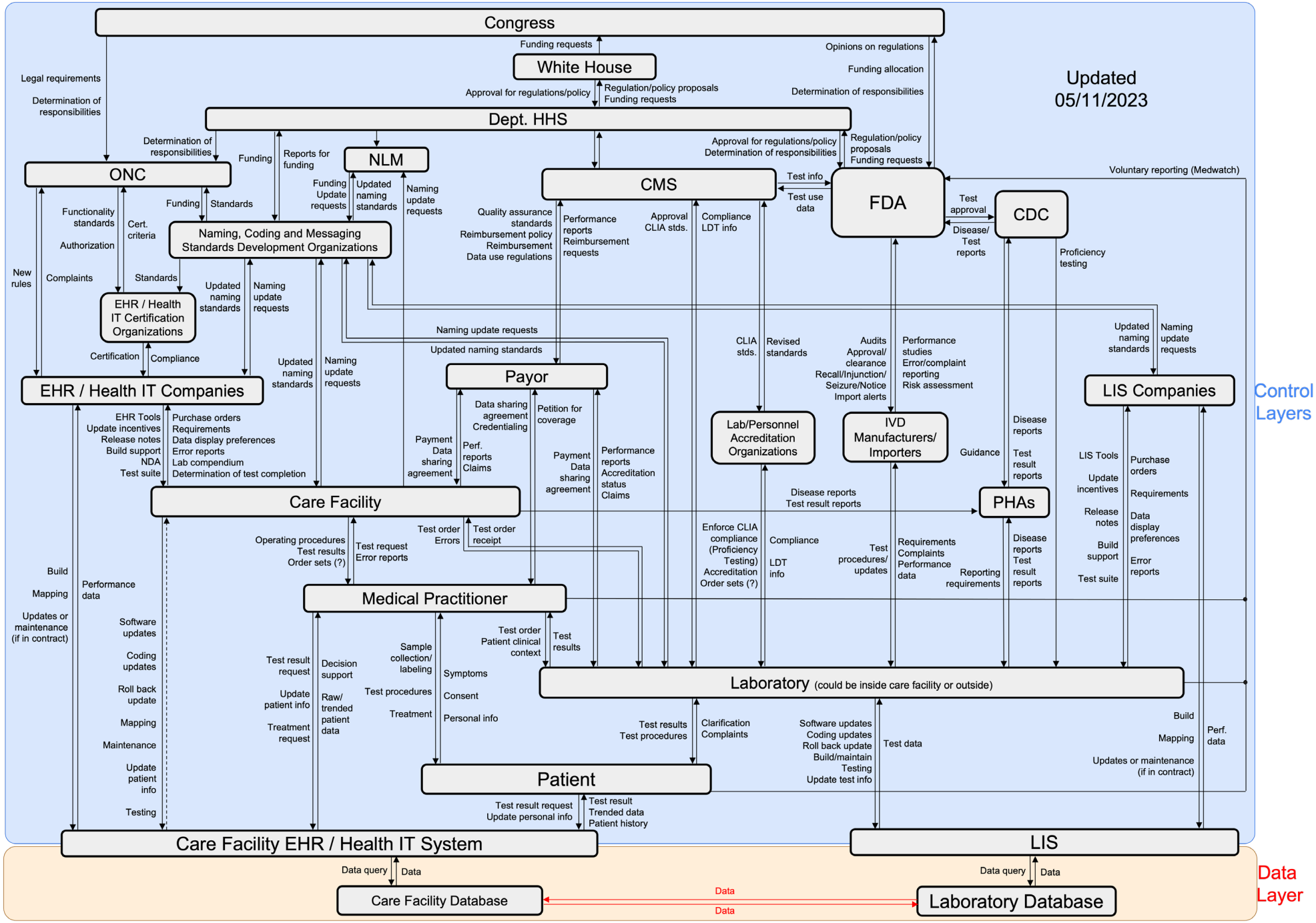
Using interviews to understand current system

42 Stakeholders interviewed

Create Formal Control Structure



Detailed Control Structure



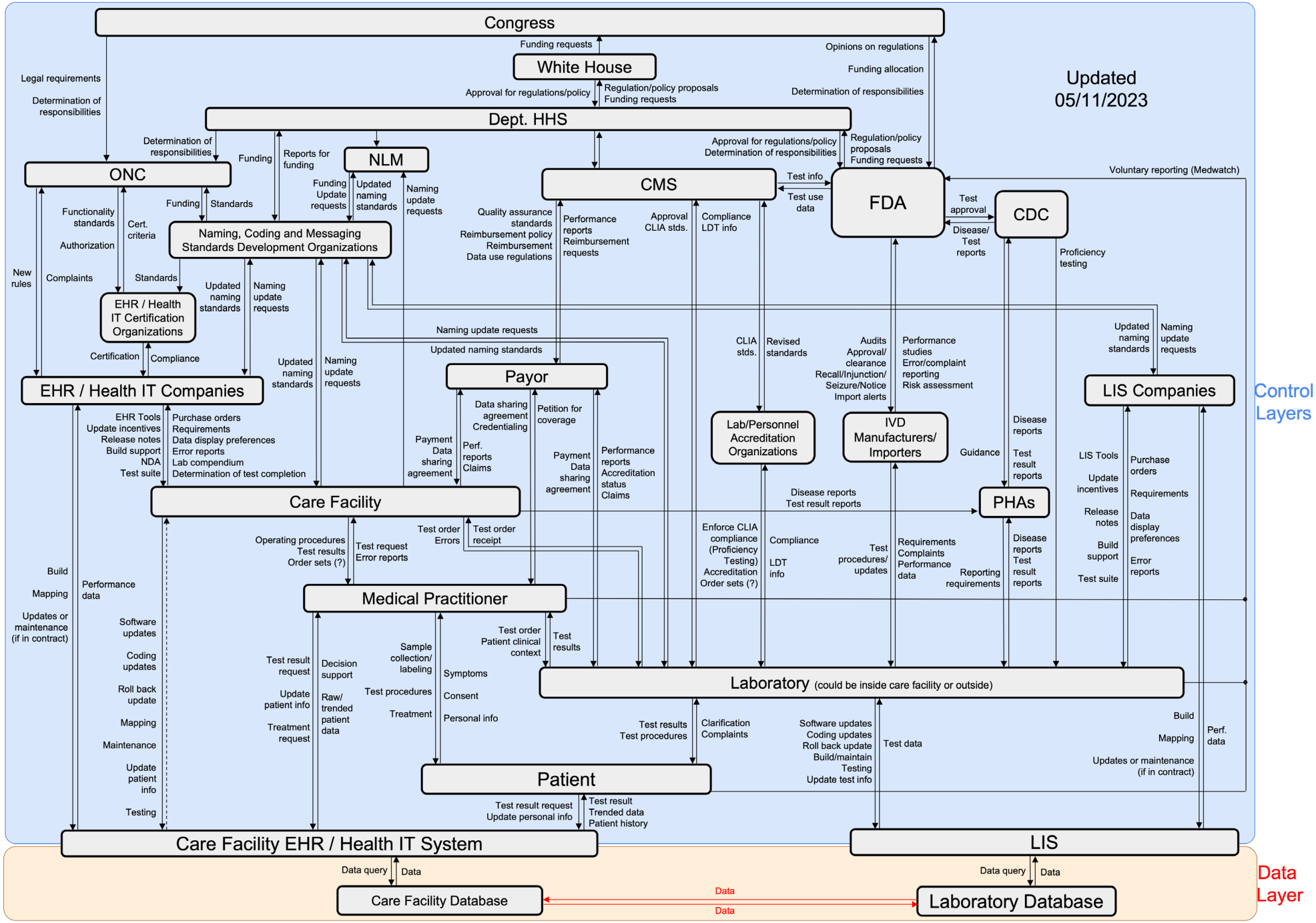
Next Steps

- Augment the model with each controller's responsibilities, process models and decision-making processes

- Identify unsafe control actions (UCAs) and scenarios leading to them (there is a structured, step-by-step process for doing this, but we are omitting it in this presentation)

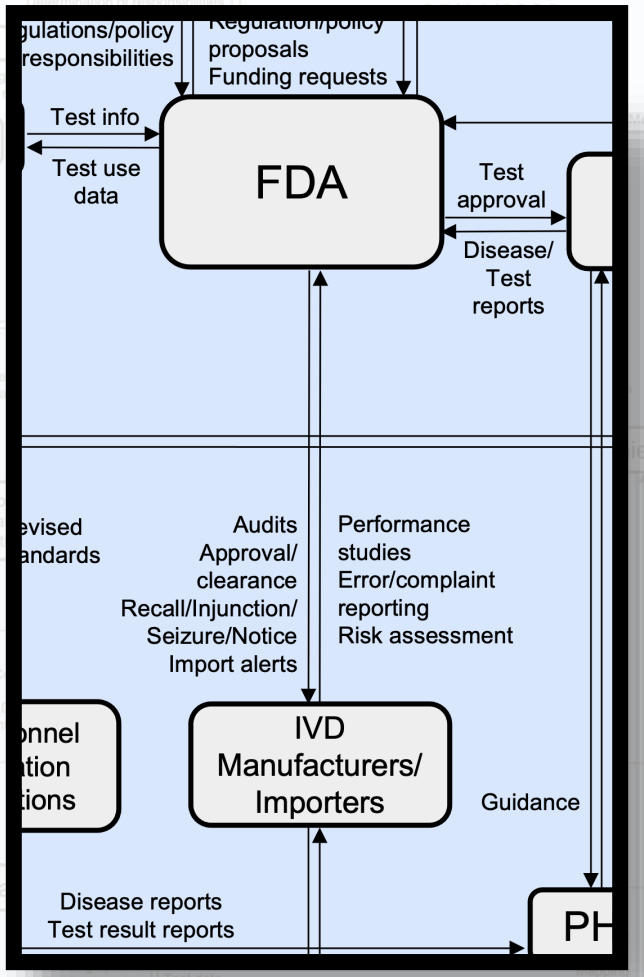
- Analyze flaws in control structure as a whole (e.g., assignment of responsibilities, implementation of responsibilities, culture, economic and political pressures, communication/coordination problems, safety information system, changes and dynamics over time, etc.)

Detailed Control Structure



Example: UCA for FDA

- **UCA:** FDA does not issue injunction/recall to company providing testing equipment with known errors.
- **Scenario 1:** *FDA does not issue injunction/recall because of a lack of meaningful real-world data (RWD) on device performance.*

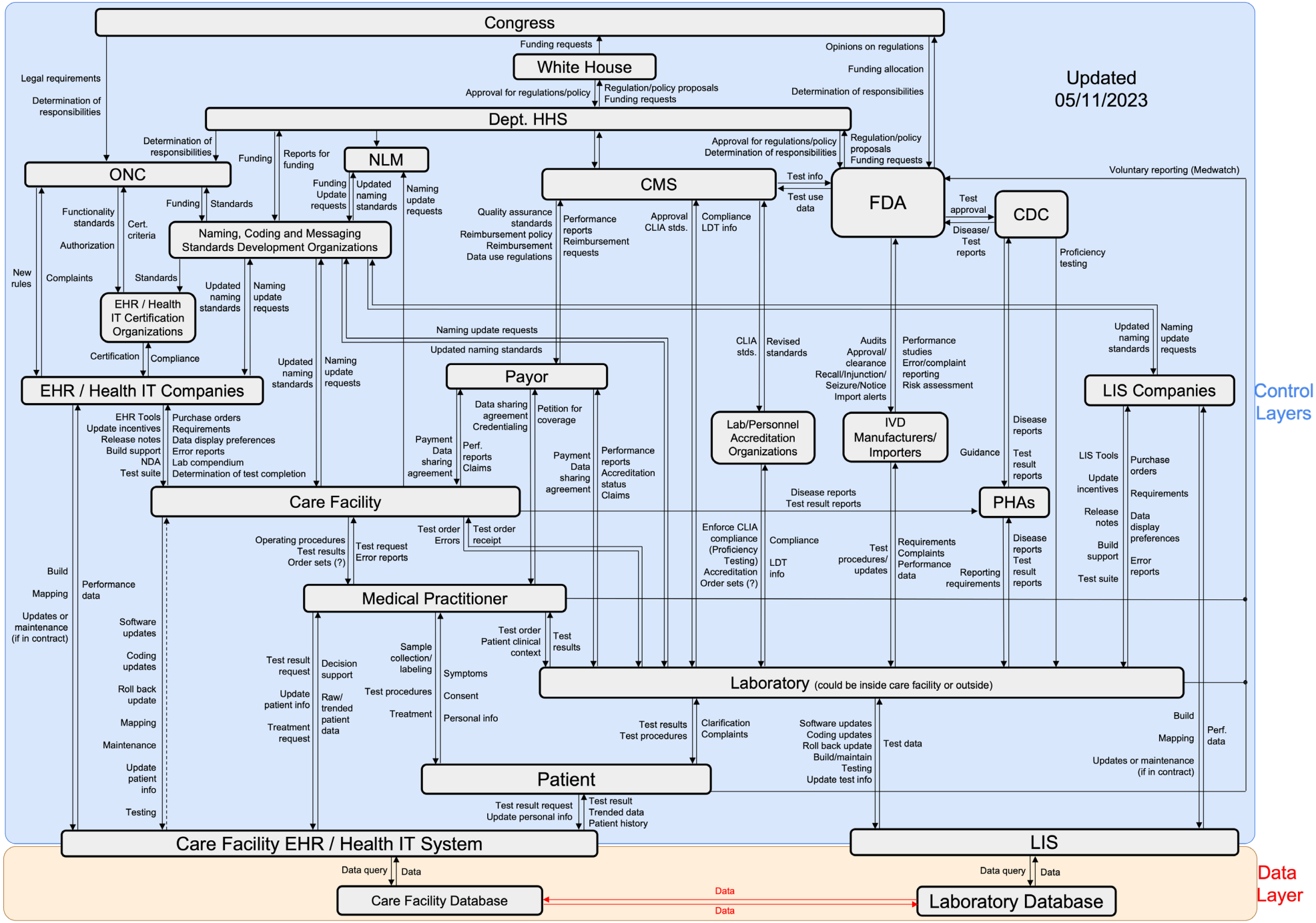


Rec. 1.1: Device performance data must be shareable by IVD manufacturers and laboratories using coding and messaging standard X, including fields A, B, C, etc.

Rec. 1.2: Investigation into adverse events involving medical practitioner action must emphasize decision-making process and identify source(s) of unsafe decisions (for example, incorrect/ incomplete diagnostic data leading to misdiagnosis)

…

Detailed Control Structure

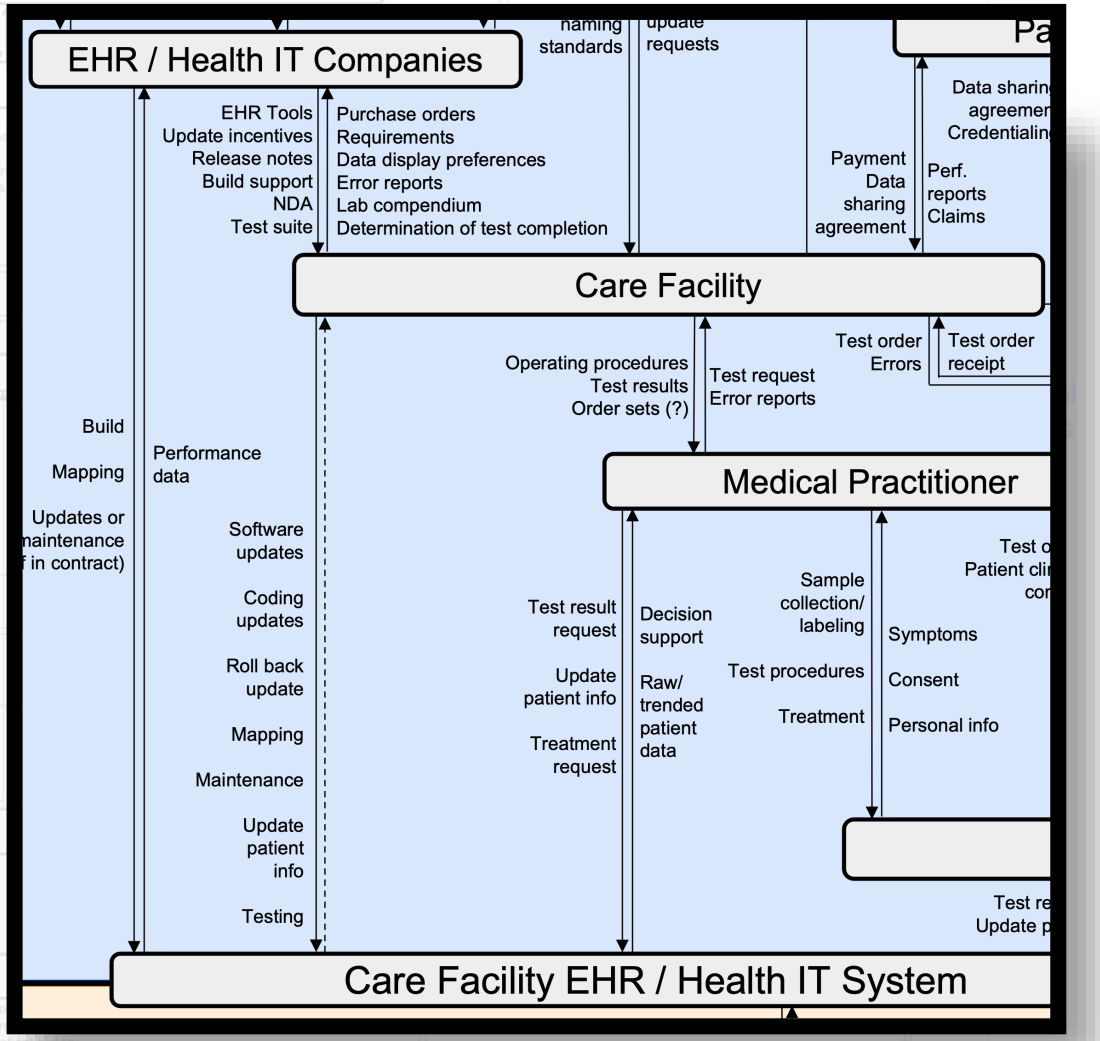


Example: UCA for Care Facility

- **UCA:** Care facility does not update electronic health record (EHR) when safety-critical EHR update is released

- **Scenario 1:** *Care facility did not have adequate resources (budget, manpower, or technical expertise) to install the update in a timely manner.*

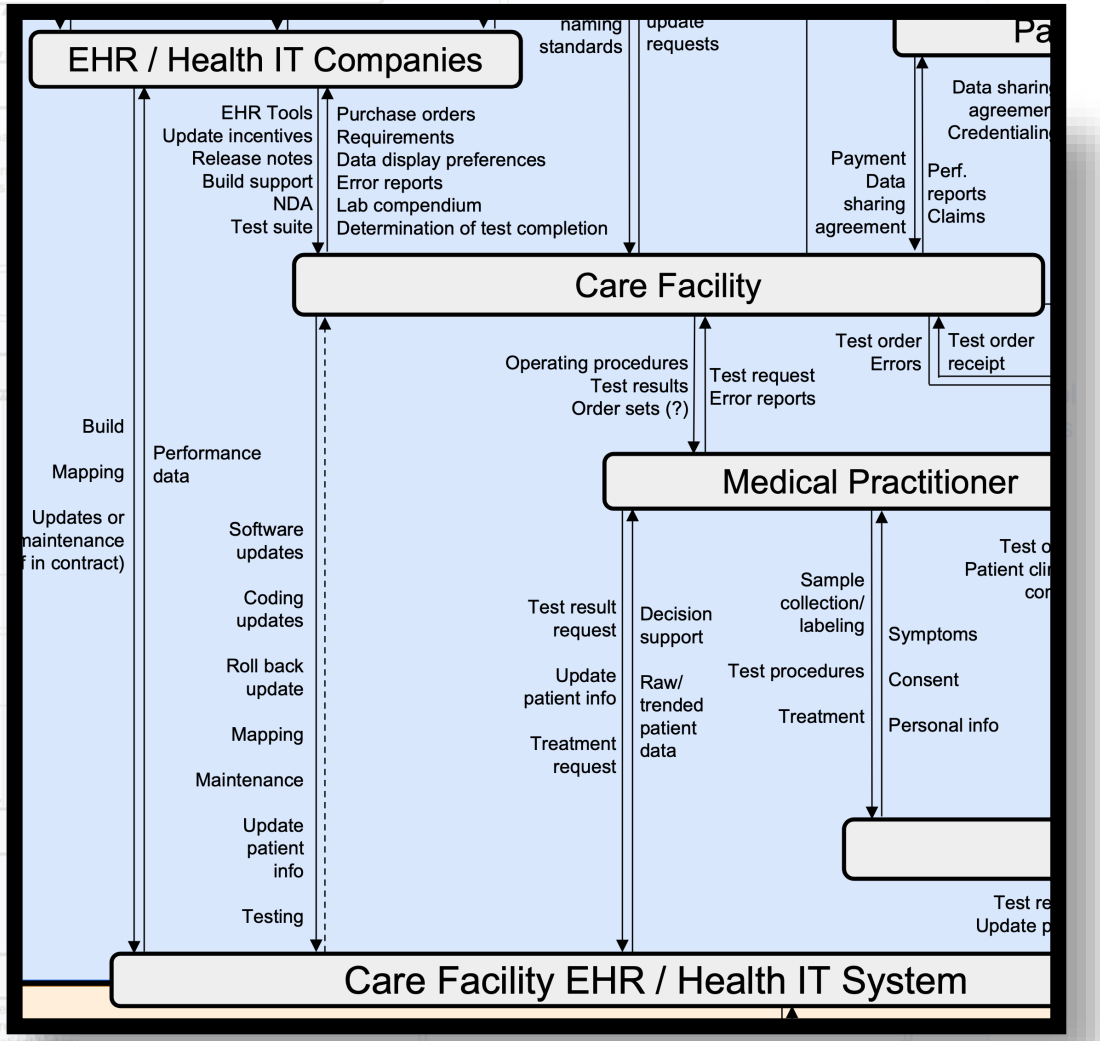
Rec. 1.1: EHR company must provide build/update support to care facilities when releasing updates with safety-critical functionality or addressing previously identified safety issues



Example: UCA for Care Facility

- **UCA:** Care facility does not update electronic health record (EHR) when safety-critical EHR update is released

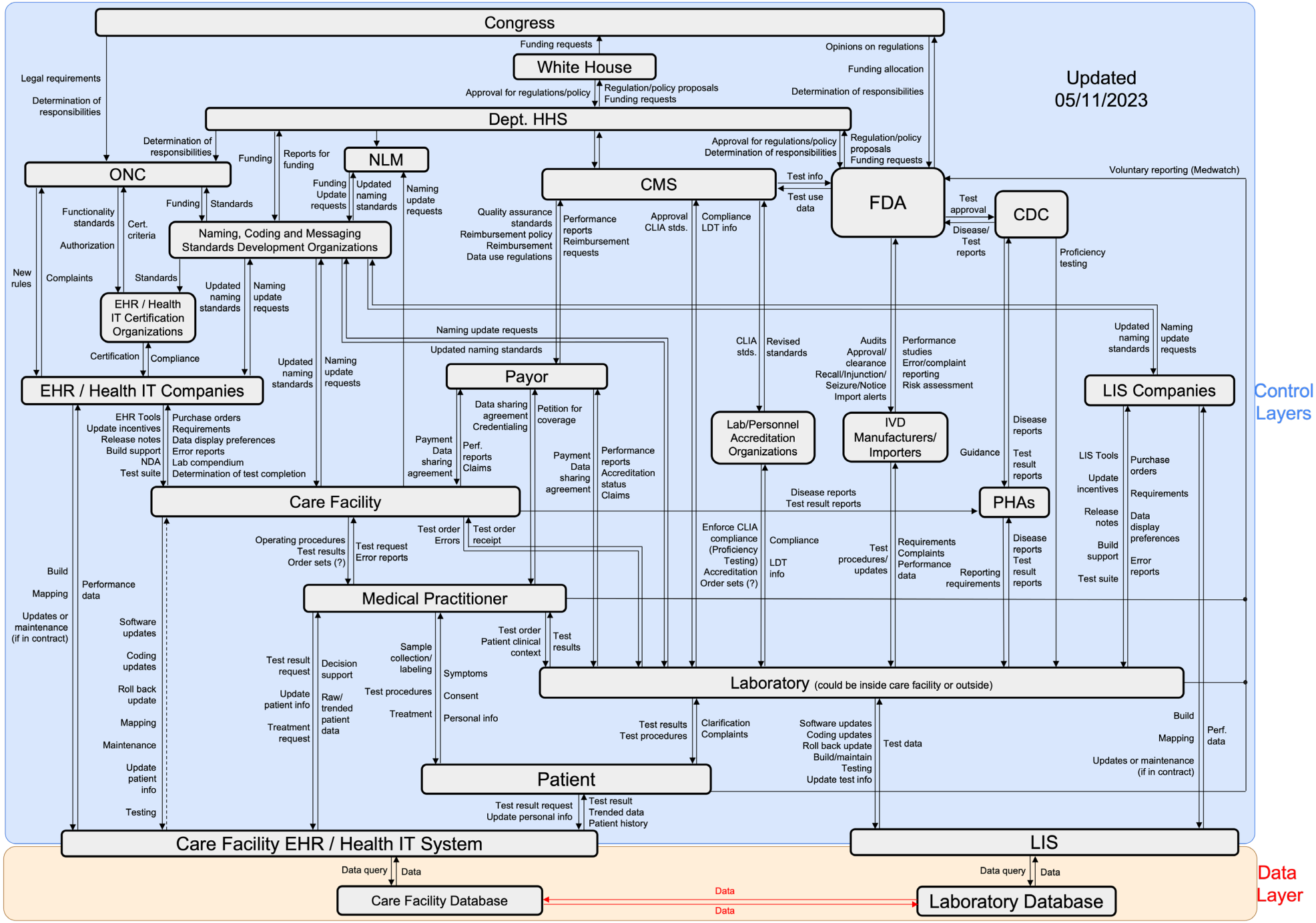
- **Scenario 2:** *Care facility team believed the update would interfere with other software they use. The update may not have taken into consideration every possible software or hardware the EHR interacts with and updating it may have caused other systems to malfunction.*



Rec. 2.1: EHR company must follow an approved standard for developing test suites for safety-critical updates

Rec. 2.2: Care facility IT team must report safety-critical issues identified after EHR update to EHR company and a regulatory body, who must submit that report to a nationwide repository of safety-critical EHR issues

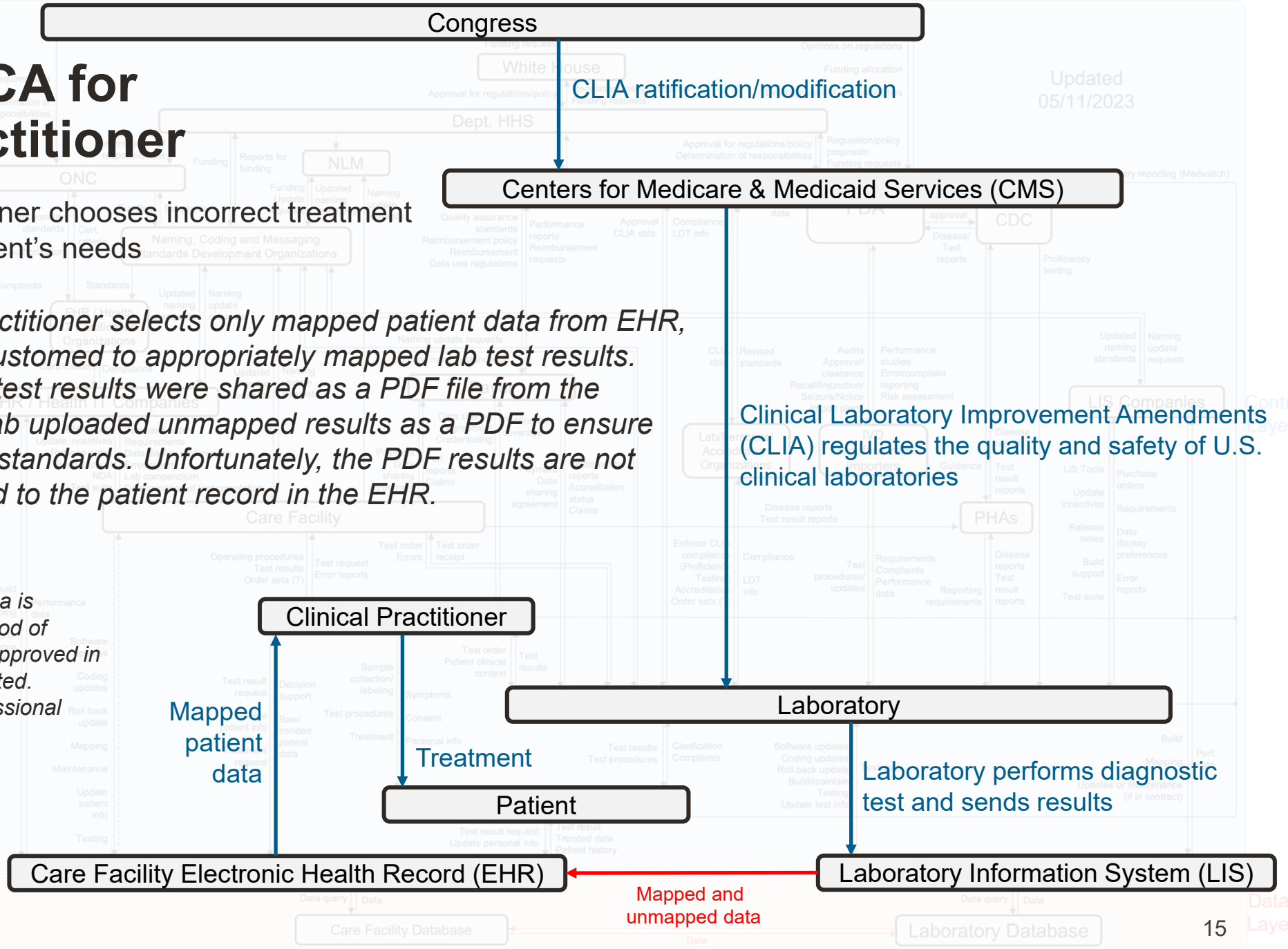
Detailed Control Structure



Example: UCA for Clinical Practitioner

- **UCA:** Clinical practitioner chooses incorrect treatment option to address patient's needs

- **Scenario:** *Clinical practitioner selects only mapped patient data from EHR, because they are accustomed to appropriately mapped lab test results. Additional unmapped test results were shared as a PDF file from the LIS to the EHR. The lab uploaded unmapped results as a PDF to ensure compliance with CLIA standards. Unfortunately, the PDF results are not computable or mapped to the patient record in the EHR.*



Note: CLIA only requires that sent data is received. It does not specify the method of transmission. CLIA was drafted and approved in 1988, before EHRs were widely adopted. Modifications to CLIA require Congressional approval.

Additional Examples of UCAs and Potential Causes

- Hazard: Patients receive less than the acceptable standard of care
- Unsafe control actions and potential causes: (not exhaustive)

- Healthcare provider orders wrong test
  - *Confusing test menus*
  - *Provider lacks familiarity*
  - *Look alike, sound alike tests*
  - *Test is new*
- Healthcare provider receives incorrect test result
  - *False positive/false negative*
  - *Incorrect test procedure used*
- Healthcare provider does not receive / receives delayed test result
  - *Supply chain issues, transportation failures, etc.*
- Healthcare provider receives test results for a different patient
  - *Patient names corrupted during exchange of locally coded data between healthcare facilities*
- Unavailability of diagnostic tests/equipment
  - *Geographic isolation (urban/rural divide)*
  - *Difficult access to care (limited health insurance)*
  - *Limited patient mobility*
  - *Supply chain issues, transportation failures*

Systemic Concerns

- Weak/nonexistent controls
- Localized solutions
- Money and profits emphasized over patient safety
- Dilution of authority arbitrarily across multiple agencies

System Redesign Recommendations

(not all are politically and economically feasible but they can start the conversation)

Conclusions

- Healthcare is a **system** and **system safety engineering** approaches can be used to analyze it

- **Large socio-technical systems** can be modeled and analyzed using STAMP and STPA. The approach is particularly powerful as:

  - It looks at the system as a whole, rather than just fixing pieces (which would lead to unintended consequences)

  - People within large systems don't themselves understand how all the pieces fit together. Control structure is a great way to help them understand their own systems.
    - **More about this in the next presentation!**

Acknowledgments

- Association of Public Health Laboratories
- The College of American Pathologists
- Deloitte Consulting, LLP
- J P Systems, Inc.
- LOINC ® from Regenstrief Institute
- Office of the National Coordinator for Health IT (ONC)
- Safe Health Systems, Inc.
- SNOMED International
- State University of New York at Buffalo
- Stratametrics, Inc.
- Sujansky and Associates, LLC
- Synensys, LLC
- University of Nebraska Medical Center
- University of Pennsylvania

Questions, Comments, Observations,
Discussions, Feedback, Follow-up

Developing Control Structures for Complex Sociotechnical Systems

Polly Harrington, Graduate Assistant
Rodrigo Rose, Graduate Assistant
Prof. Nancy Leveson, PhD
John Thomas, PhD
Massachusetts Institute of Technology

Stephen Powell, DHA, MSc
Daniel Wyman, MD, MPH
Alana Keller, BA, PMP®
Synensys

For U.S. FDA Contract # 75F40122C00112

June 7th, 2023

Disclaimer

- The opinions expressed in this presentation are those of the research team members. 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.

What is difficult about modeling complex socio-technical systems

This is not a trivial problem

- Interdisciplinary – technical, management, economic
- No one understands the whole system
- Analyst may be unfamiliar with system – Where to start? What are the bounds? What are the relevant components?

26

Starting out

- What information do you know?
- What do you know you don't know?
- How do you obtain more information? → **Interviews**
  - Interview those you already know
  - Ask interviewees who else you should talk to
  - Aim to interview a broad range of people across the system

27

Conducting Interviews

- Interviewees don't know about STPA
- Go over interview goals and rudimentary STPA intro with interviewee
  - Define and show a basic control loop (with examples)
  - Later you may also need to define
    - What is a control structure (with examples)
    - What are losses and hazards (with examples)
- Pre-reads can be helpful as the project progresses
- Intro will get more in depth as project progresses

Conducting Interviews

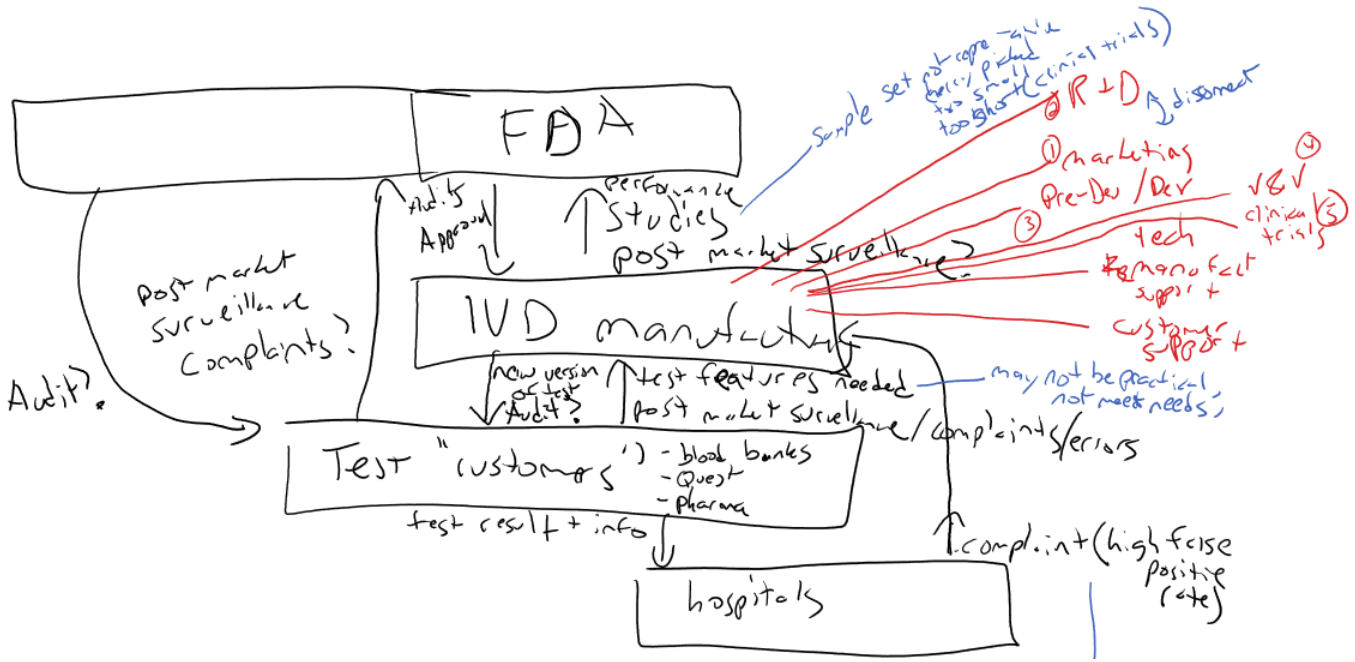
- Leave initial questions open ended
  - Most helpful information is not what you anticipate
- Ask more specific follow up questions
  - Translate what they said into “STPA terms” and confirm that you interpreted them correctly
- Showing the control structure has advantages and disadvantages
  - May inspire new connections
  - Can also bias what they say or do not say

Who did we interview?

42 Stakeholders interviewed

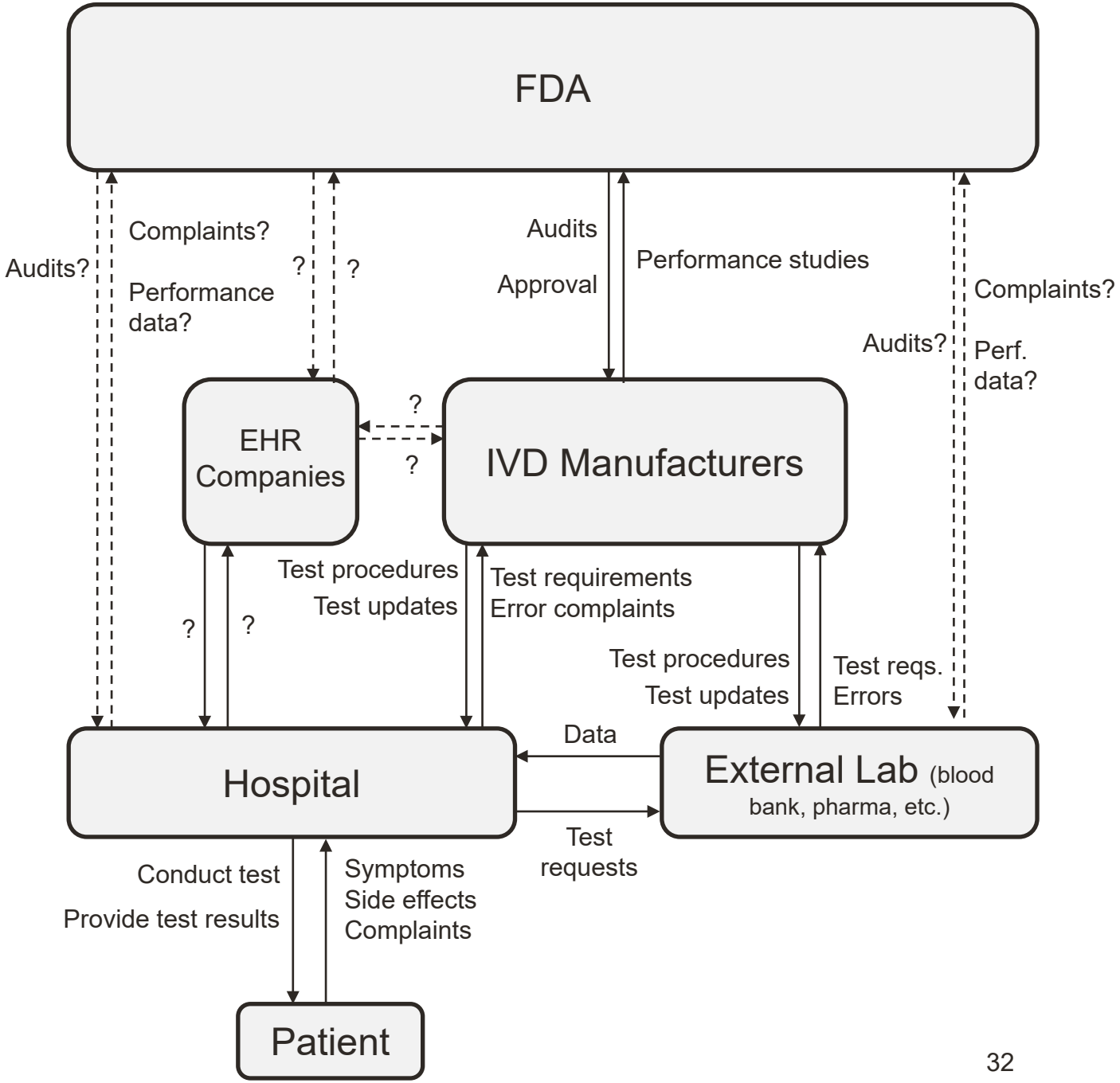
Initial Sketches

- We didn't have a control structure in our first interview
- We sketched this rough diagram live during initial interviews
- Shows the interviewee we are listening
- Gives interviewee ability to correct us



First Control Structure

- Start to formalize control structure
- Identify relationships you might be missing
- During interviews you can draw on the diagrams “live”
- Being wrong is usually okay, people love to make corrections
- Rougher drafts will make people more comfortable making corrections



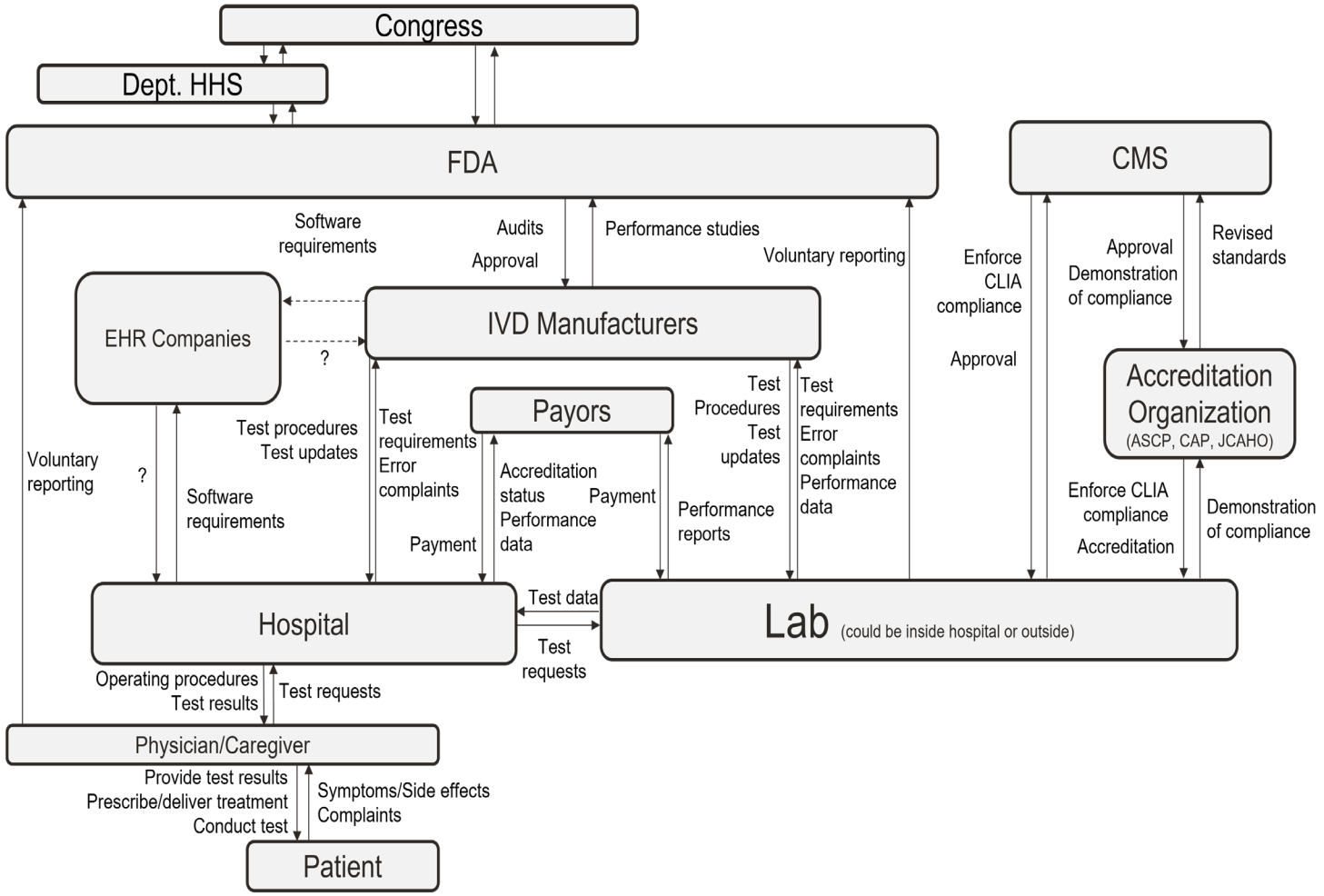
Iterating

System boundaries may change

For example

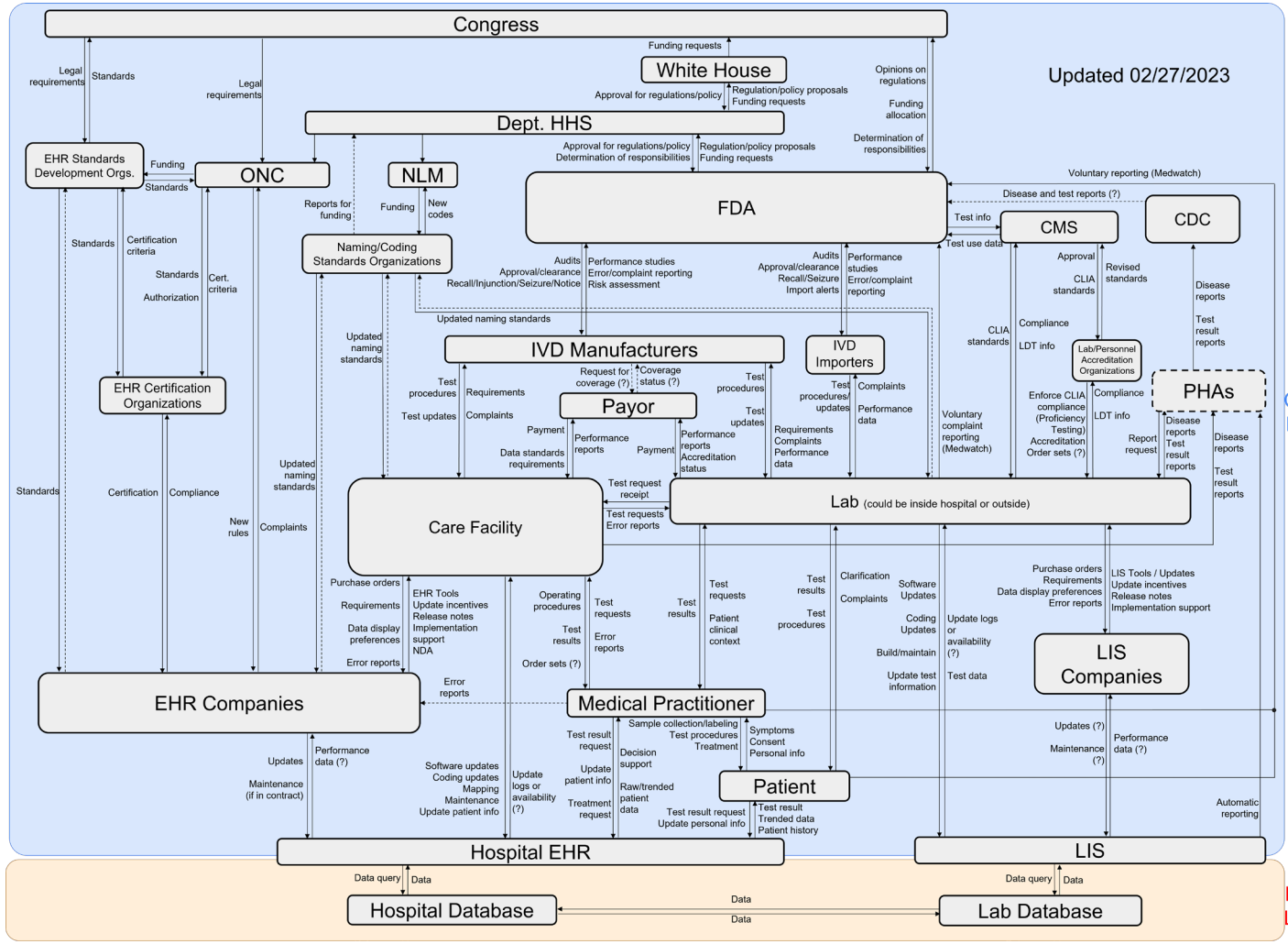
- New regulatory authorities
- Higher level agents

You can always trim back later



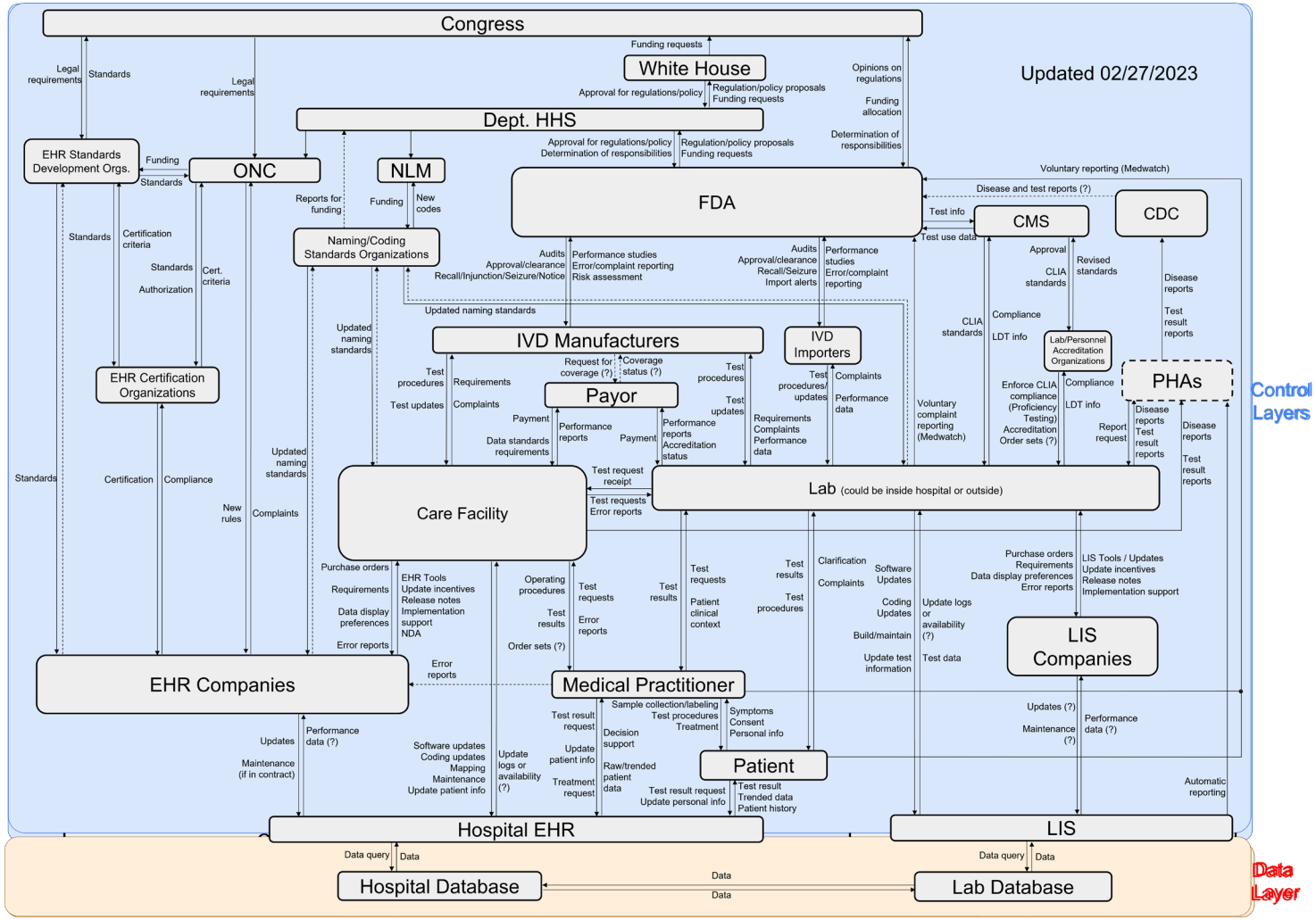
Iterating

- Things may start to get extremely complicated
- Think about where abstraction may be required
- Make compromises to help your interviewees map their understanding
  - We added a “data layer” as the controlled process



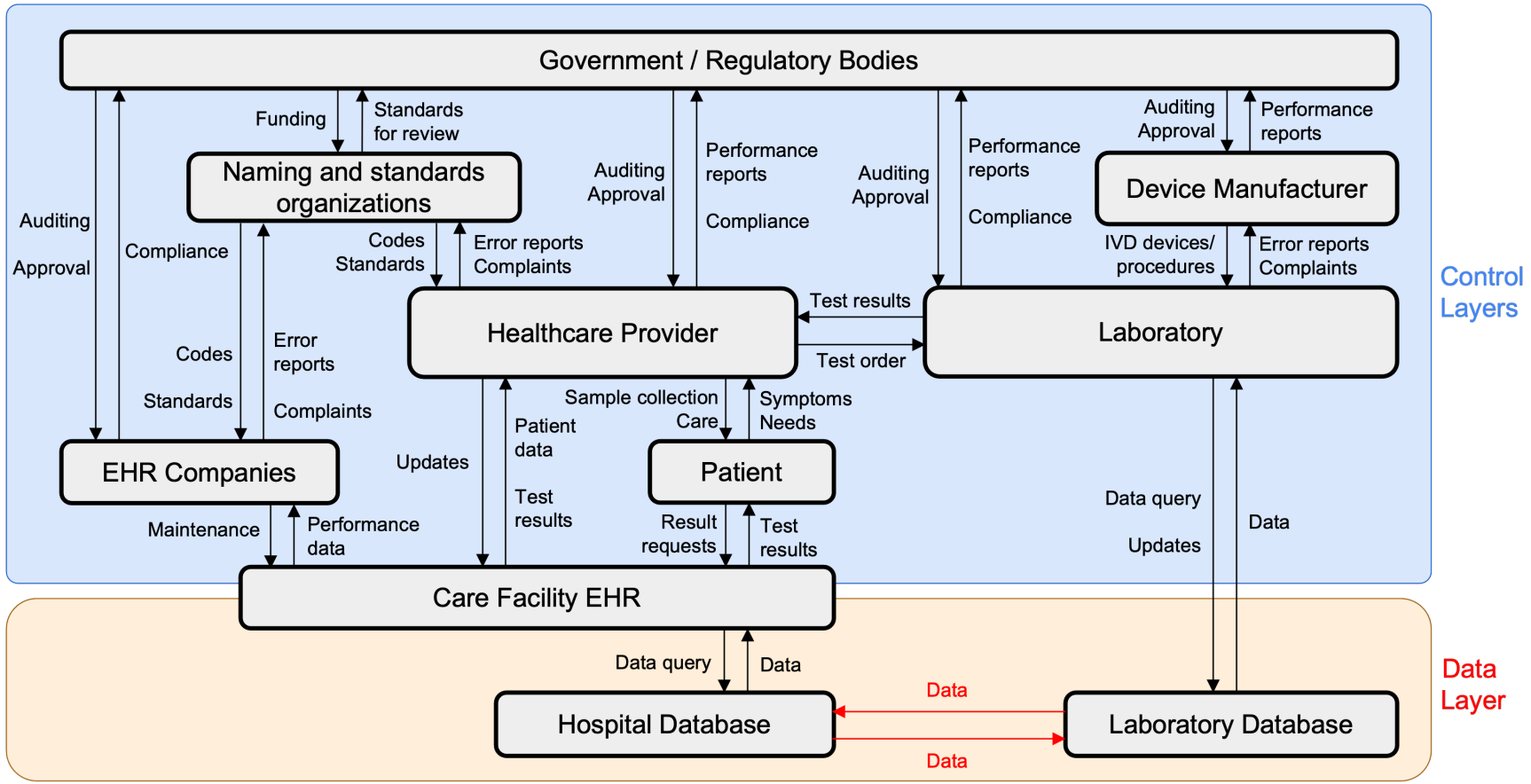
Iterating

- As you gain more information, question your assumptions about the original model
- Control hierarchy may change
  - EHR/Care Facility example
- Boxes and arrows may merge or split
  - Standards organizations example



Abstraction

- Abstract out for your own clarity and modeling
- Interviewees may want to see themselves clearly
- Look for ways to abstract in the detailed version as well



Later Stage Interviewing

- Once the control structure gets more complete, shift interviews towards UCA and Scenario generation
  - Giving examples can help the interviewee understand what you are looking for

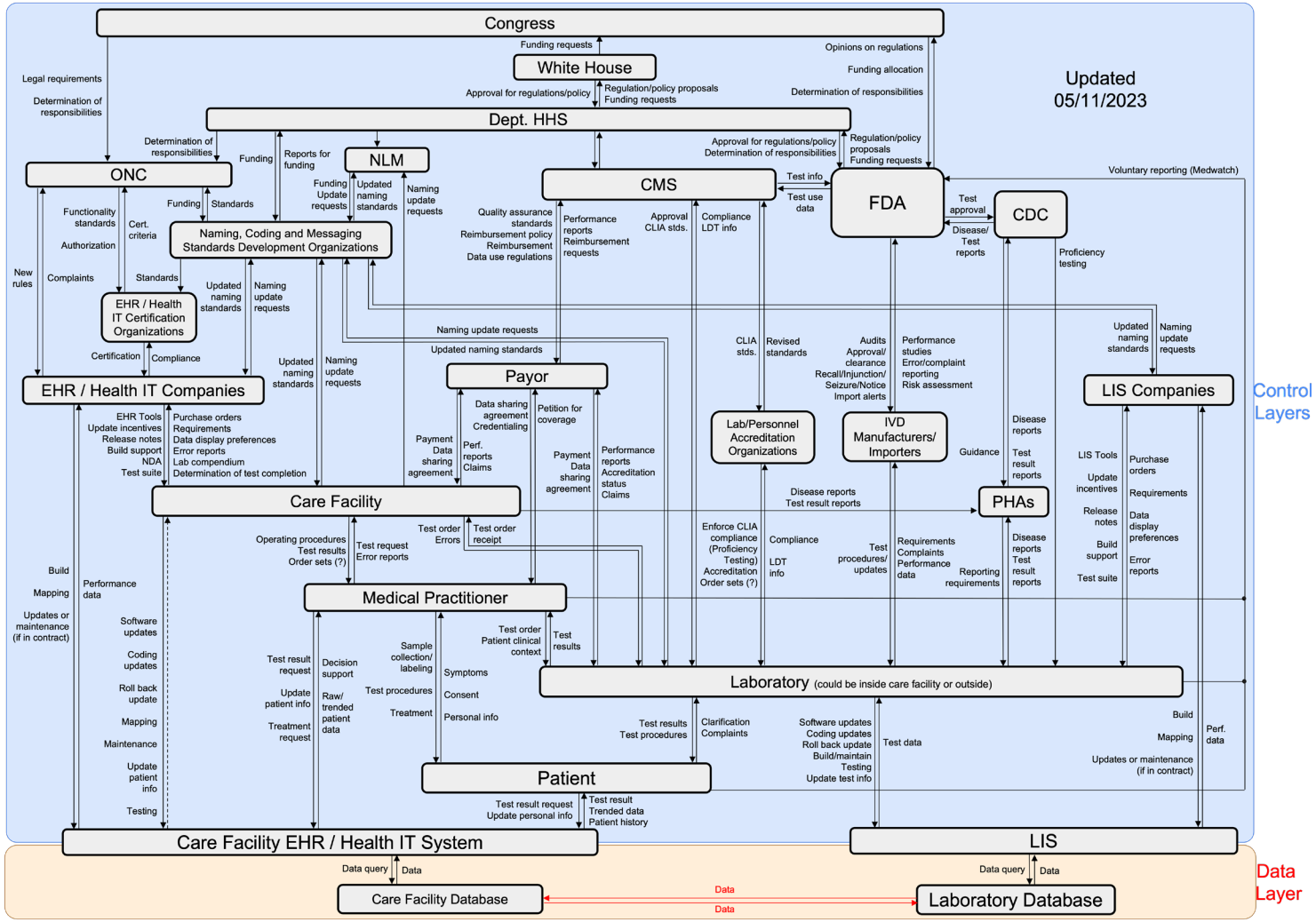
- Ask interviewees about the connections to other agents
  - “Have you seen situations like these arise?”
  - “Could you see situations like these arising?”
  - “Can you think of other situations you have seen or could see arising?”

- Show control structure at the end, for validation (or corrections)

Converging

- At the end, your goal is that with every interview, fewer and fewer changes happen in the control structure

- Converge on an acceptable (and **useful**) model of the system, even if it is not complete



Final Notes

- Control structure is a tool, not the end product
- Transcripts are useful
  - You might not fully appreciate information from initial interviews
- Difficult to speak same language as interviewees
  - Make sure you use language they are familiar with
  - Ask them to clarify their language
- Continually evaluate what is working and what is not

Acknowledgments

- Association of Public Health Laboratories
- The College of American Pathologists
- Deloitte Consulting, LLP
- J P Systems, Inc.
- LOINC ® from Regenstrief Institute
- Office of the National Coordinator for Health IT (ONC)
- Safe Health Systems, Inc.
- SNOMED International
- State University of New York at Buffalo
- Stratametrics, Inc.
- Sujansky and Associates, LLC
- Synensys, LLC
- University of Nebraska Medical Center
- University of Pennsylvania

Questions, Comments, Observations,
Discussions, Feedback, Follow-up

Contact

Rodrigo Lopes Rose
rlrose@mit.edu

Polly Harrington
ph1@mit.edu