System-Theoretic Process Analysis (STPA) Applied to Clinical Decision Support Systems (CDSS) in Healthcare

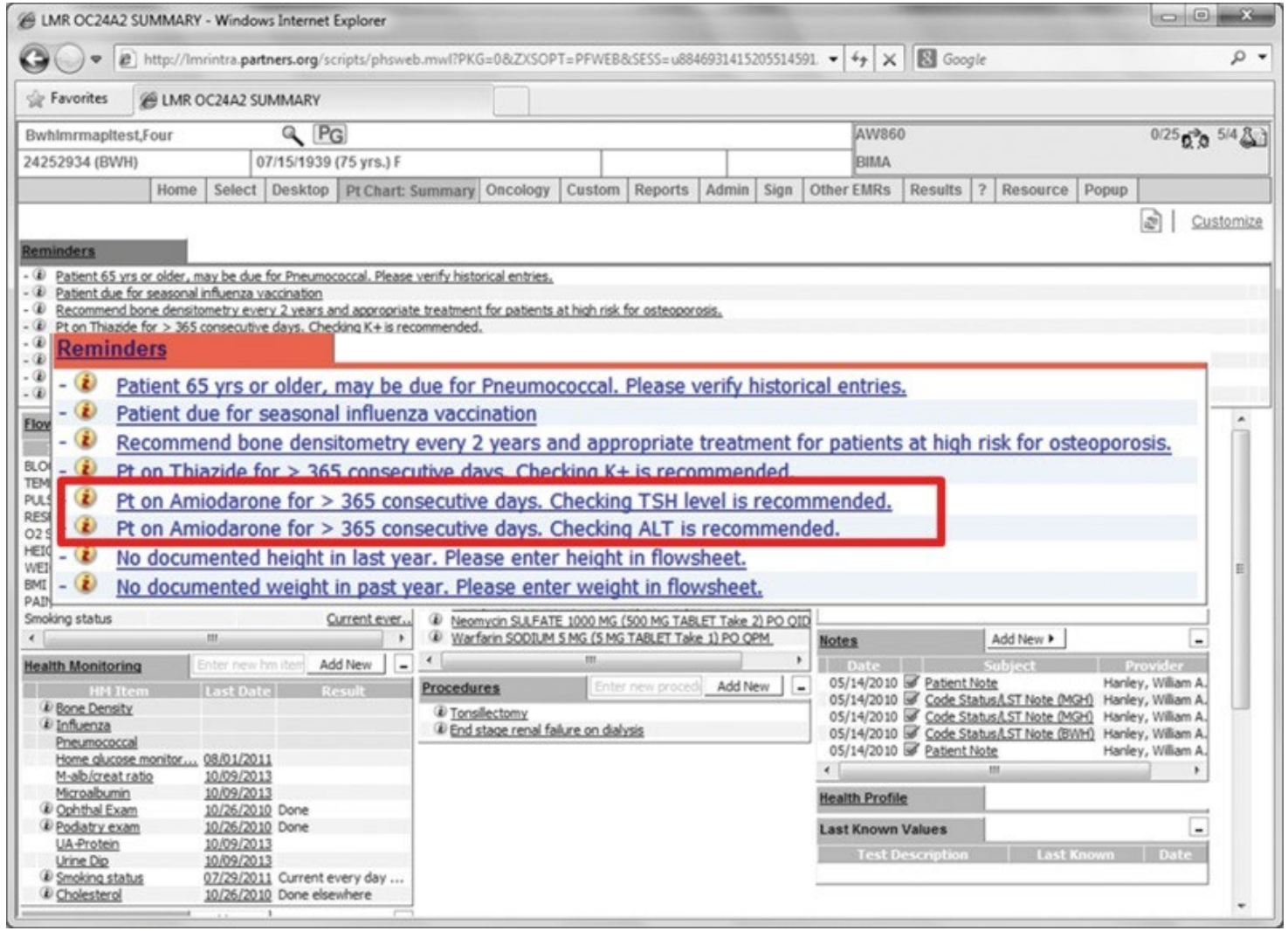
Eugenia Kim

MIT STAMP Workshop

September 2025

What are Clinical Decision Support Systems (CDSS)?

- Health IT tools that are used to support decision-making in diagnosis and treatment
- Include:
  - Automatic alerts and reminders
  - Condition-specific order sets
  - Patient-specific data reports



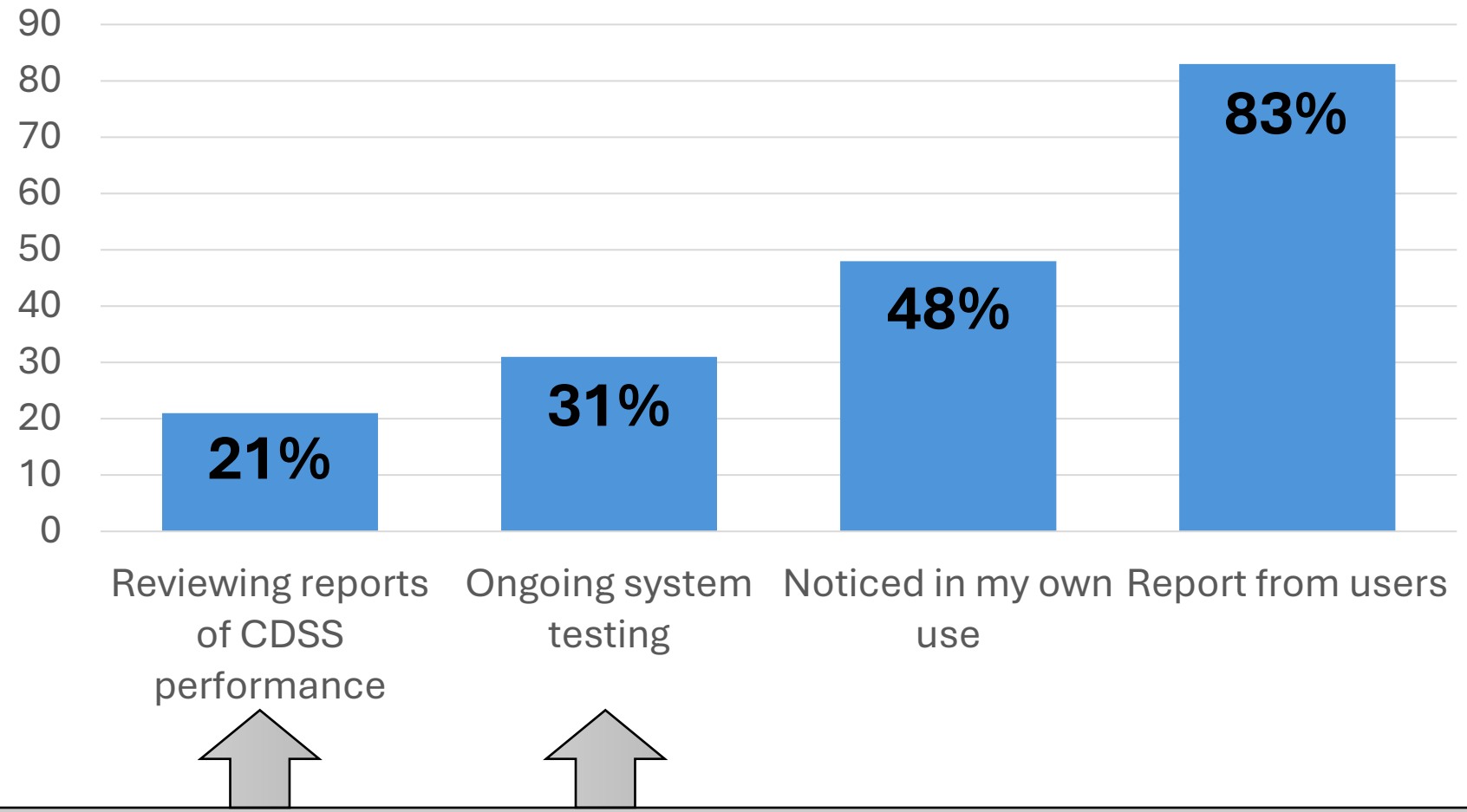
Example of CDSS laboratory monitoring reminders.

Figure from Wright A, Hickman TT, McEvoy D, Aaron S, Ai A, Andersen JM, Hussain S, Ramoni R, Fiskio J, Sittig DF, Bates DW. Analysis of clinical decision support system malfunctions: a case series and survey. J Am Med Inform Assoc. 2016 Nov;23(6):1068-1076. doi: 10.1093/jamia/ocw005. Epub 2016 Mar 28. PMID: 27026616; PMCID: PMC5070518.

Current State of CDSS Safety

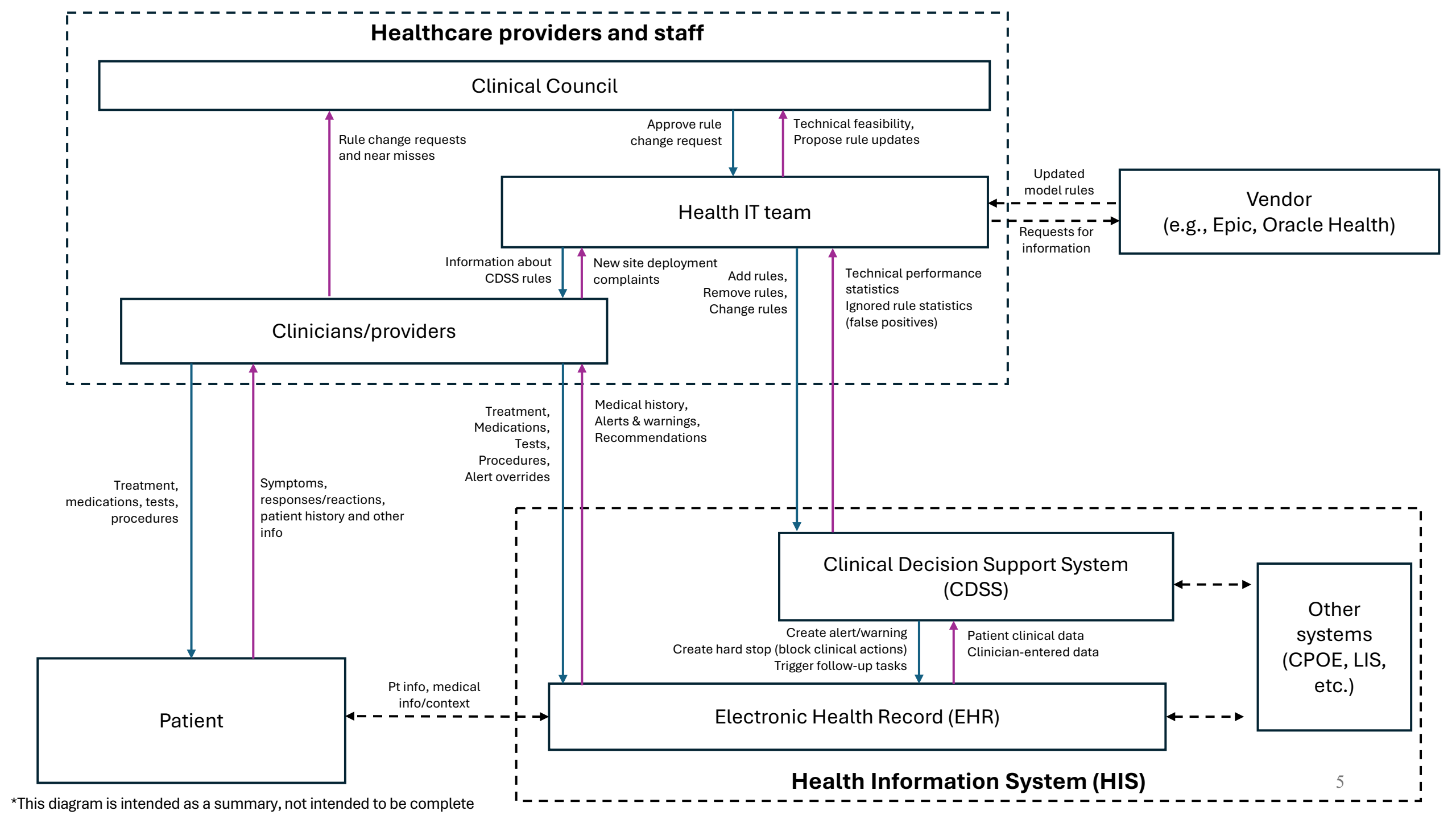
- Long story short? Not ideal
- There are recognized benefits of CDSS in healthcare, BUT there are also weaknesses, ones that can result in adverse events
- Many CDSS deficiencies are often found through voluntary reports from users
- These CDSS deficiencies are often only fixed long after they are introduced

How are CDSS malfunctions found today?



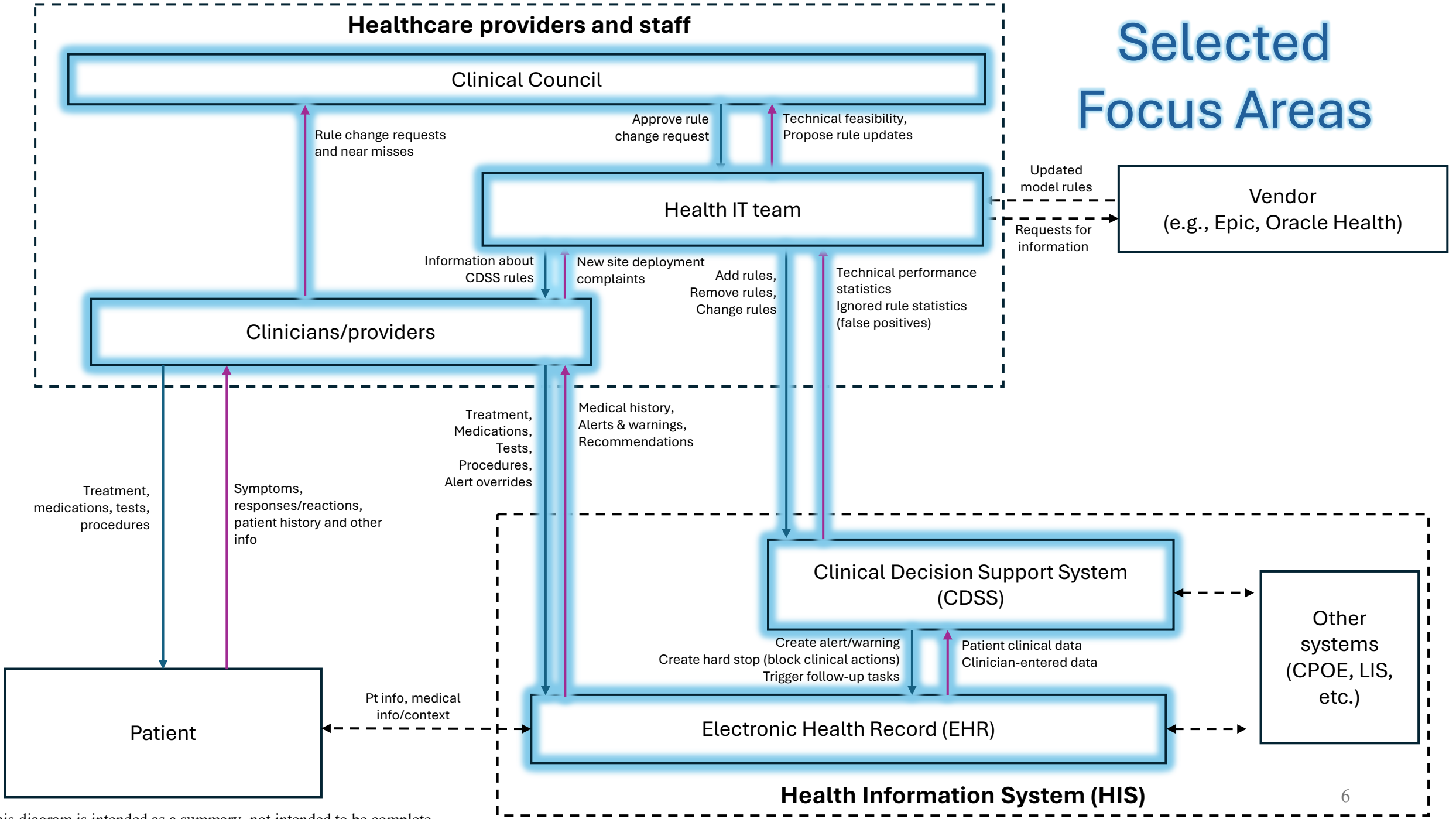
The vast majority of CDSS malfunctions are being **overlooked by testing** and existing CDSS performance metrics

Wright et al, 2016. “Analysis of clinical decision support system malfunctions: a case series and survey”

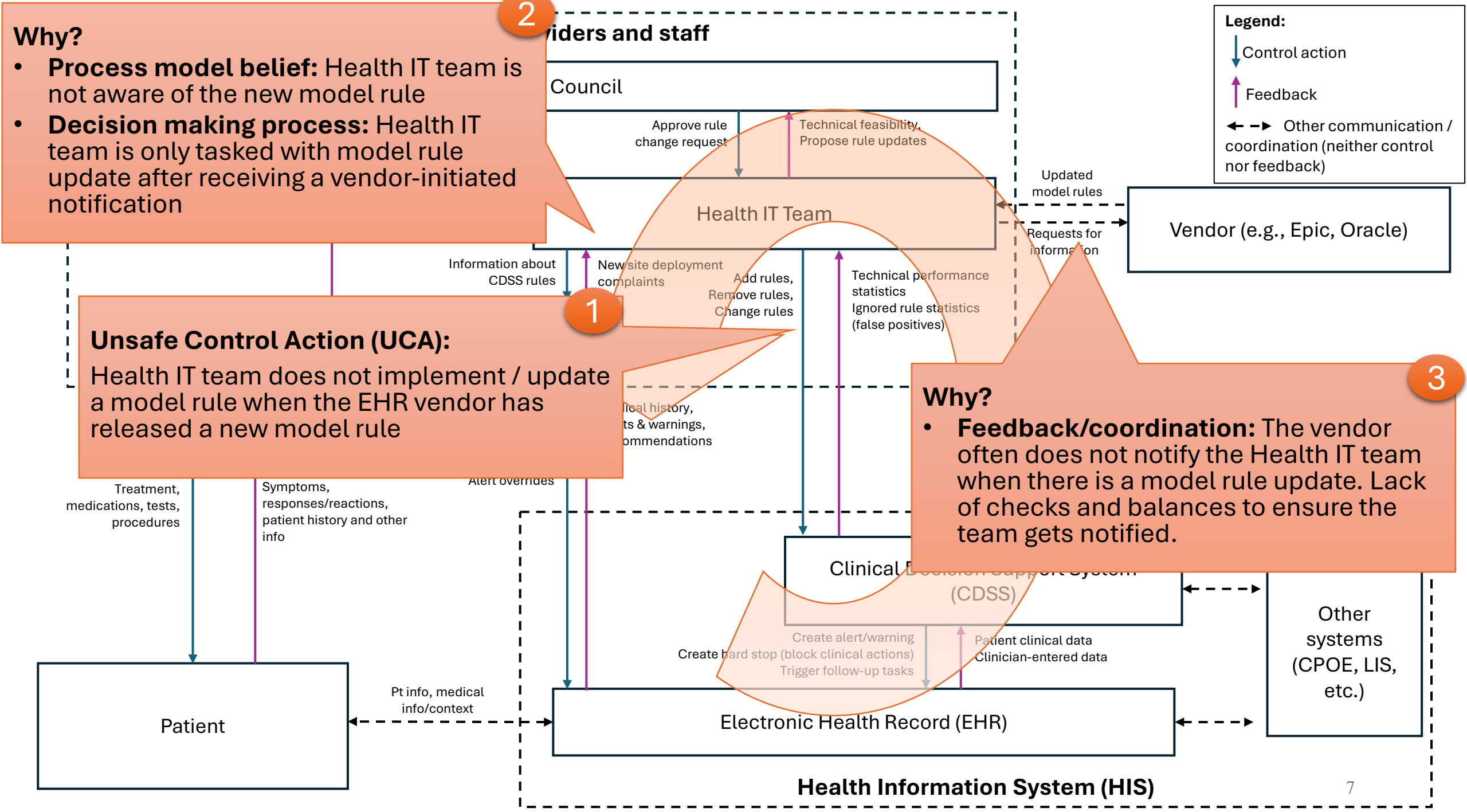


*This diagram is intended as a summary, not intended to be complete

Selected Focus Areas



*This diagram is intended as a summary, not intended to be complete

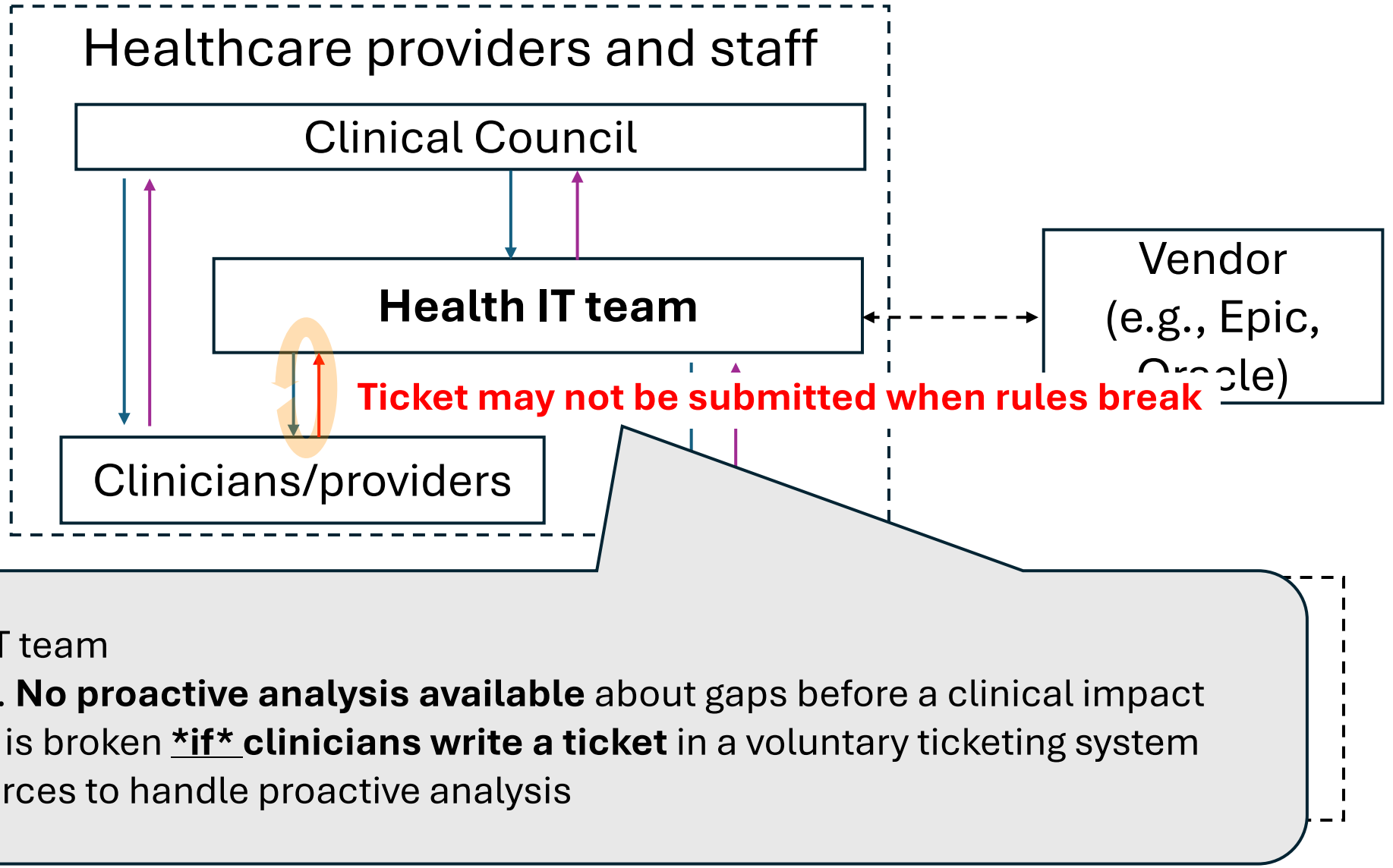

Why?
• Process model belief: Health IT team is not aware of the new model rule
• Decision making process: Health IT team is only tasked with model rule update after receiving a vendor-initiated notification
2
viders and staff
Council
Approve rule change request
Technical feasibility, Propose rule updates
Health IT Team
Updated model rules
Vendor (e.g., Epic, Oracle)
Requests for information
Information about CDSS rules
New site deployment complaints
Add rules, Remove rules, Change rules
Technical performance statistics
Ignored rule statistics (false positives)
1
Unsafe Control Action (UCA):
Health IT team does not implement / update a model rule when the EHR vendor has released a new model rule
ical history,
ts & warnings,
ommendations
Alert overrides
Treatment, medications, tests, procedures
Symptoms, responses/reactions, patient history and other info
Why?
• Feedback/coordination: The vendor often does not notify the Health IT team when there is a model rule update. Lack of checks and balances to ensure the team gets notified.
3
Clinical Decision Support System (CDSS)
Create alert/warning
Create hard stop (block clinical actions)
Trigger follow-up tasks
Patient clinical data
Clinician-entered data
Other systems (CPOE, LIS, etc.)
Patient
Pt info, medical info/context
Electronic Health Record (EHR)
Health Information System (HIS)
Legend:
Control action
Feedback
Other communication / coordination (neither control nor feedback)

Example Scenario

Unsafe Control Action (UCA)	Example Scenario
Health IT team **does not fix a rule** when the rule is broken	A rule is broken and not working as intended, but the health IT team does not know that the rule is broken because a ticket has not been submitted to report the broken rule.

Systemic Factor

Reactive vs. Proactive



Feedback to Health IT team

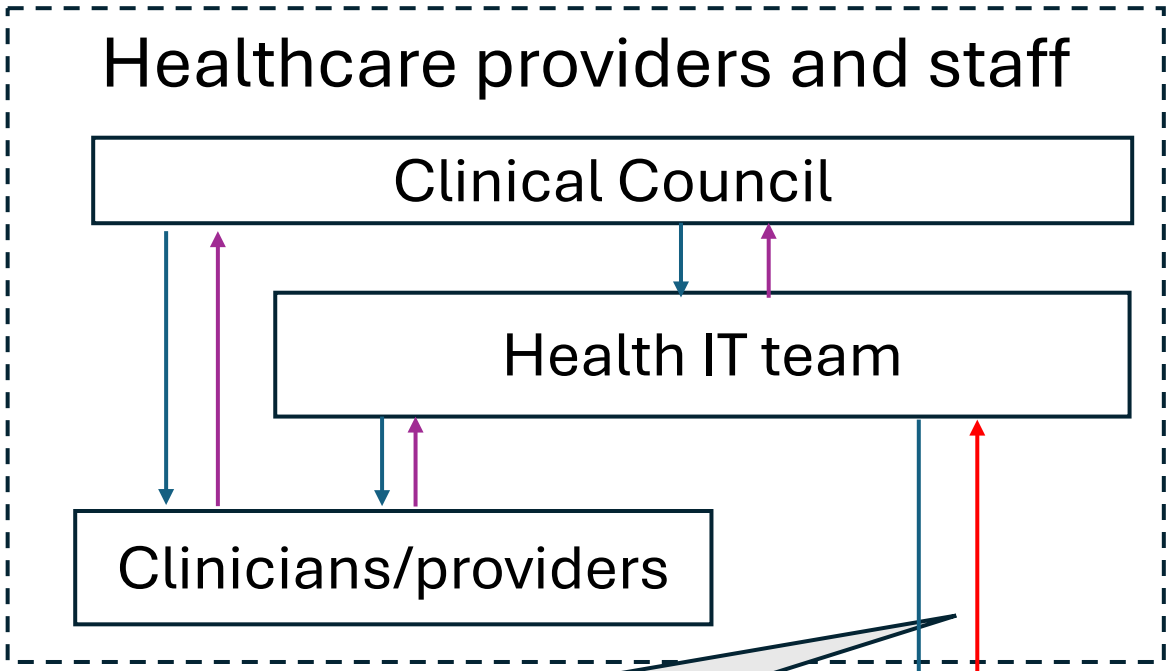
- Primarily reactive. **No proactive analysis available** about gaps before a clinical impact
- Only aware a rule is broken ***if* clinicians write a ticket** in a voluntary ticketing system
- Inadequate resources to handle proactive analysis

Example Scenario

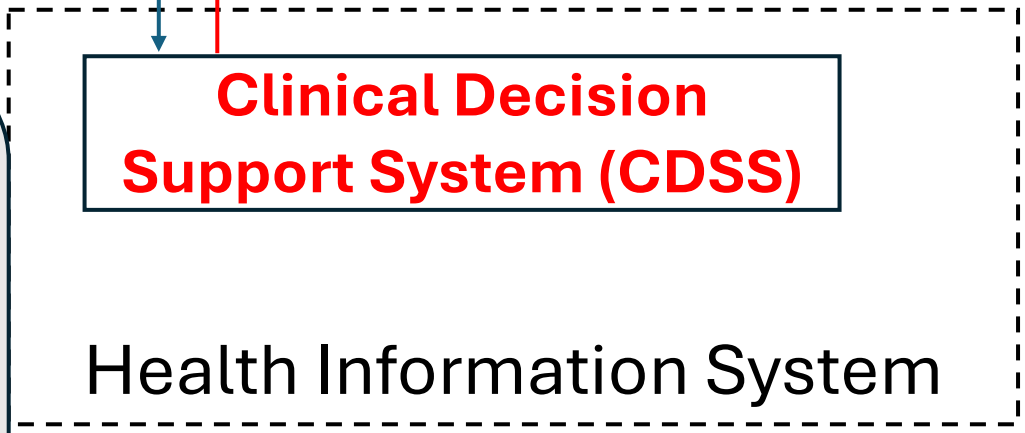
Unsafe Control Action (UCA)	Example Scenario
Health IT team **pulls a data audit report too late** after a rule is not firing as intended	The data audit report that the health IT team pulls does not indicate when a rule is not firing as intended. The log is temporary and only contains historical data going back 30 days before disappearing. If there is a problem with a rule that was deployed in the system more than one month in the past, the health IT team has difficulty in diagnosing the problem since there are no diagnostic archives. The report is not able to be used for prospective analysis of which rules are firing as intended.

Systemic Factor

Unused & Missing Feedback



Rule detail and historical data lost after one month



Diagnostic data challenges

Logs are temporary: Rule data logs (loopback view) disappear after 30 days.

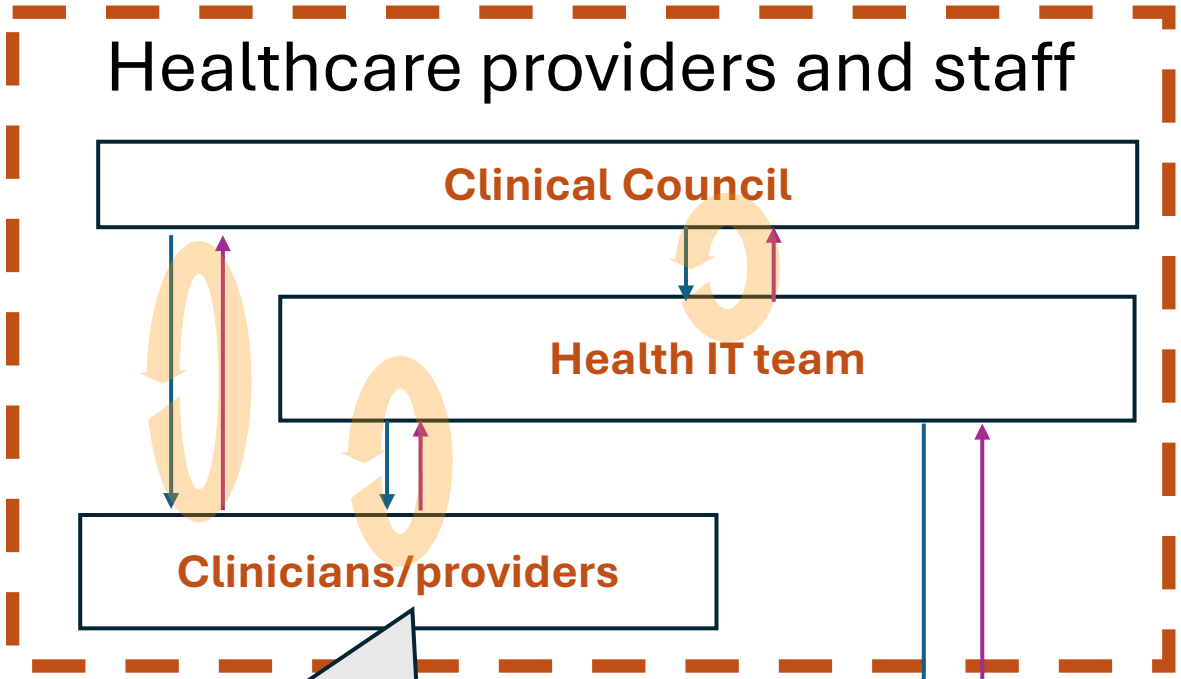
No diagnostic archives

- Difficult to diagnose a problem after 30 days
- Difficult to answer: “Has this malfunctioned before?” “How often?”

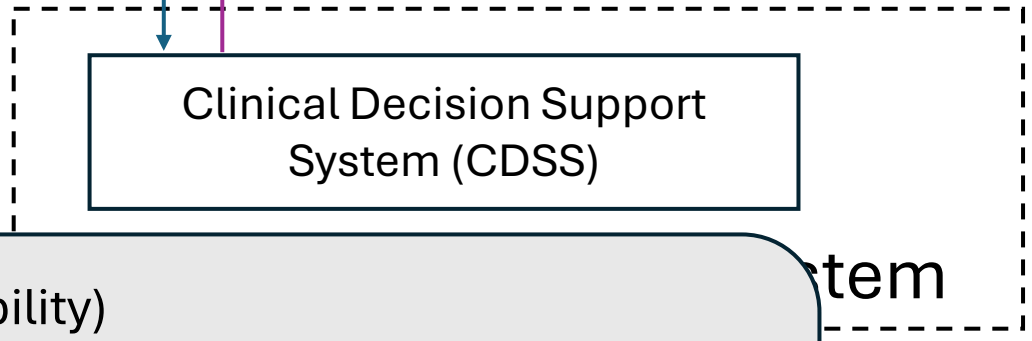
Minimal records saved: The only persistent data is a simple log of popup events that occurred (not other events, not diagnostic info)

Systemic Factor

Lack of Rule Ownership



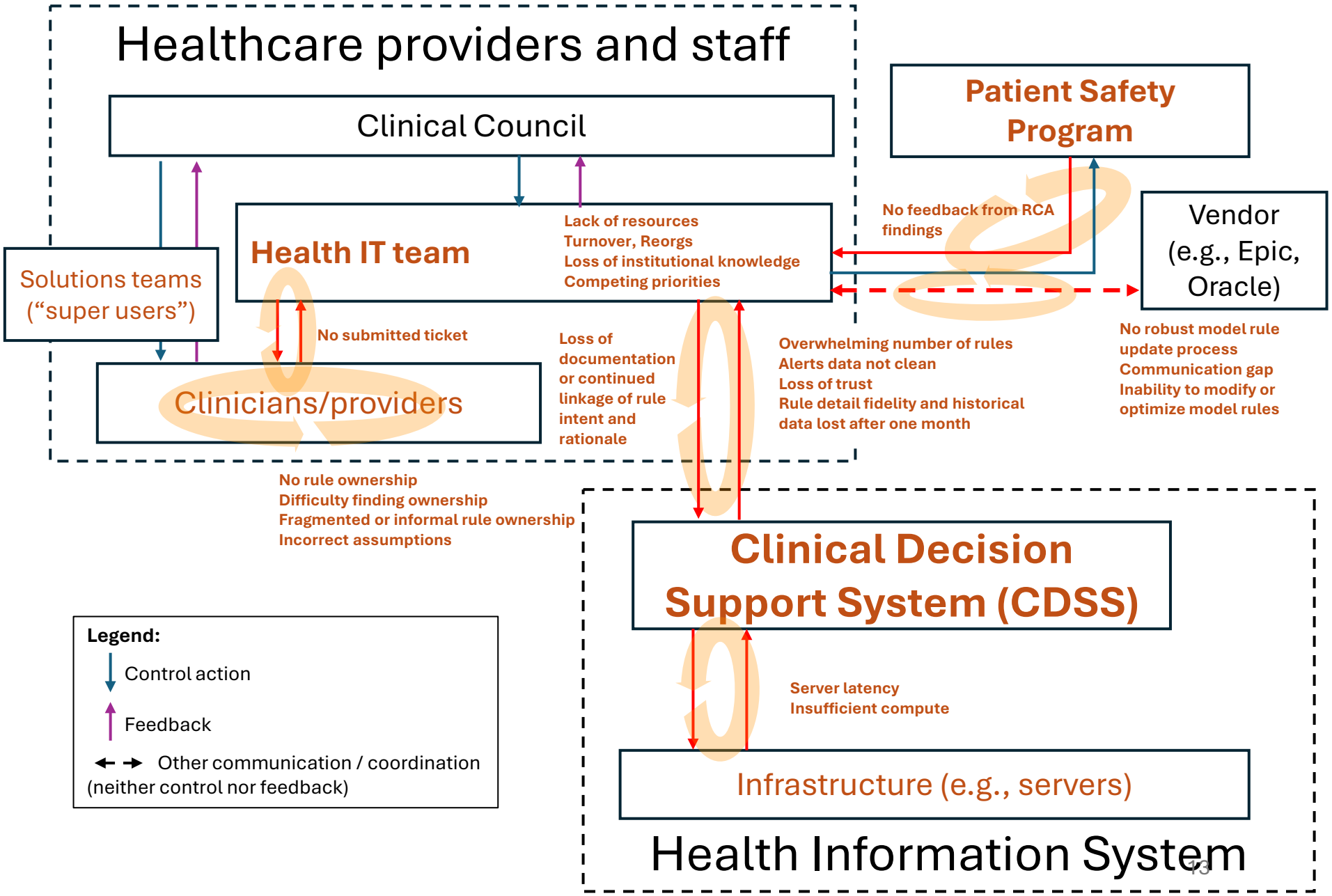
- **Fragmented ownership**
- **Informal only**
- **Only for handful of rules**
- **Incorrect assumptions by other groups**



No Clinical Rule Ownership (Missing Responsibility)

- No **tracking of changes**, such as clinical guidelines, that affect rules
- No continuous **monitoring of clinical relevance**, periodic reassessment
- No systematic checks of **rule effectiveness**; reliant on users submitting tickets
  - E.g., false-positive and false-negative rates
- No checks for **unintended consequences** after implementation

Examples of Opportunities to Strengthen Safety Management System

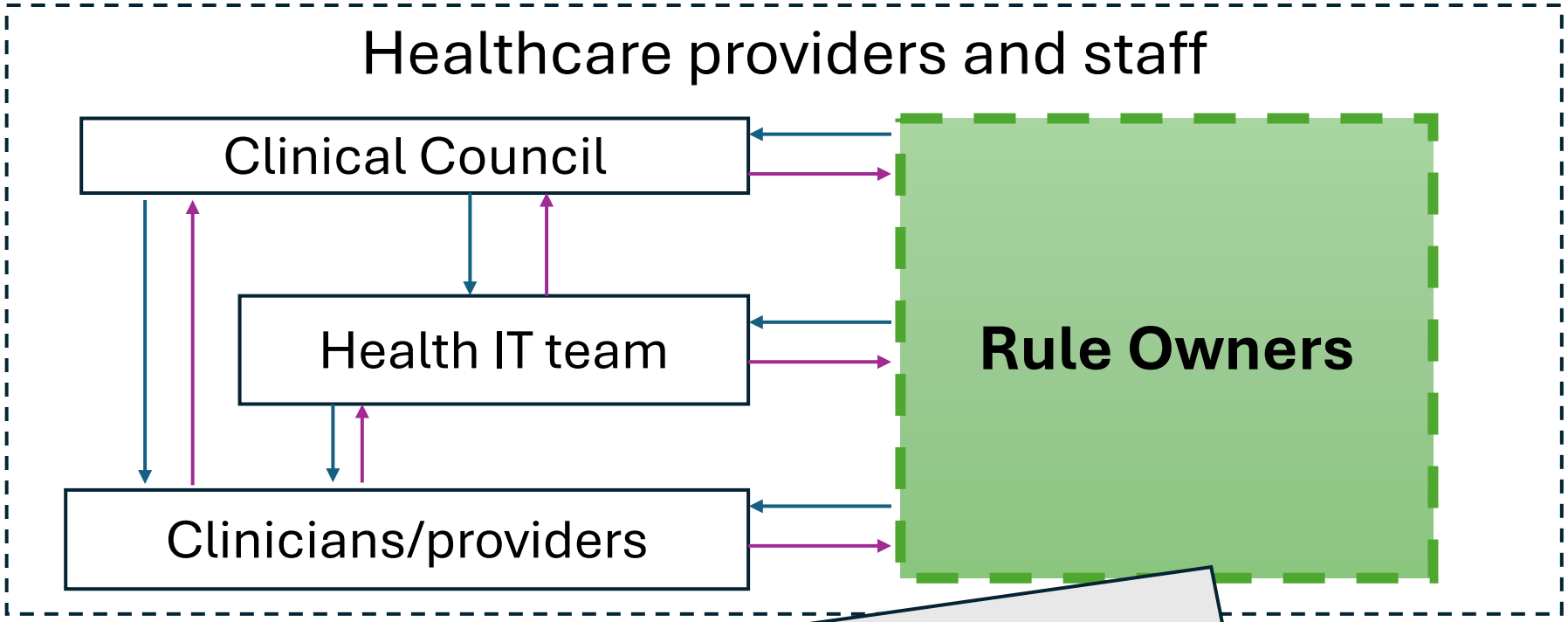


Sample of other findings

- Coordination gaps with EHR vendor
- Delayed or missing model rule updates
- Limited ability to customize model rules
- Fragile model rules that break after updates
- Reactive issue detection and response
- Short data retention window
- High alert volumes
- Excessive alert override rates
- Alert fatigue reducing trust and effectiveness
- Lack of clinical effectiveness monitoring
- Minimal use of performance and feedback data
- No diagnostic archives for troubleshooting
- Limited compute and increasing latency risks
- Resource constraints (small team, high workload)
- Lack of formal rule ownership
- Fragmented informal ownership
- Loss of institutional knowledge due to turnover and reorgs
- No systematic hazard analysis
- No human-factors analysis in design or updates
- Inadequate RCA findings / communication regarding HIT
- Governance and contracting gaps
- Lack of monitoring tools for clinical effectiveness
- Inconsistent processes between facilities
- Difficulty tracking rule rationale and history
- Limited tools implemented for proactive analysis
- Late-found flaws causes higher cost to fix
- Missed opportunities for continuous improvement

Opportunities

- Improve model rule coordination with vendor
- **Establish clear rule ownership**
- Incorporate strong proactive measures
- Add feedback currently missing



Establish clinical rule ownership role

Assign responsibilities:

- Monitor relevant **clinical guidelines** for changes that require rule updates
- Monitor **clinical effectiveness** of rules
  - Identify measures to **evaluate clinical impact**, like override rates and false-positive rates
  - If a rule is ineffective, take appropriate response
- Monitor **unintended consequences** of rules
- Clearly document and **link rule metadata**: rule owners, change history, rationale, etc.

Was it useful to apply STPA to CDSS?

YES!

- Benefits: Effective, economical, *proactive*
- For anyone in the healthcare industry, **would recommend using STPA** to find weaknesses in CDSS and their environments