Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412493

The Critical Value Chain: A Narrative Review of Systems Analysis, Human Factors, and Security-Based Interventions to Prevent Communication Failures in Life-Threatening Laboratory Result Reporting

Yahya Hamad Ahmed Mahdi [(1)] , Lamyaa Mahdi Mohammed Hazazi [(2)] , Elham Ali A Mahnashi [(3)] , Mohammed Ibrahim Mohsen Gome , Abdullah Essa Magbool Oraybi , Khalid Hamoud Najea Somaily , Ahlam Mohammed Ahmed Arishi , Essa Ali Ali Oraybi , Abdullah Zain Abdullah Abbas , Samira Ali Hussin Halawi [(4)] , Amani Mohammed Ali Arishi [(5)] , Huda Ali Hassan Alshehri [(6)] , Reem Mohammed Ahmed Shaabi , Dhuha Nasser Hassan Muharraq [(6)]

(1) Samtah PHC,Ministry of Health, Saudi Arabia,
(2) Khwalf PHC,Ministry of Health, Saudi Arabia,
(3) Jazan health cluster, Ministry of Health, Saudi Arabia,
(4) General Samtah Hospital,Ministry of Health, Saudi Arabia,
(5) Samtah General Hospital,Ministry of Health, Saudi Arabia,
(6) Ministry of Health in Aseer Region, Saudi Arabia

Abstract

Background: The timely and reliable communication of critical laboratory values (CLVs)—results indicating imminent, life-threatening patient risk—is a non-negotiable patient safety standard. Despite long-standing protocols, failures in this communication chain persist, leading to diagnostic and treatment delays, patient harm, and sentinel events. These failures represent systemic vulnerabilities rather than isolated human errors.

Aim: This narrative review aims to analyze the multi-factorial causes of CLV communication breakdowns and synthesize evidence for a systems-based, security-informed response. It specifically evaluates the integrated roles of the clinical laboratory, nursing, and healthcare security/patient safety functions in designing fail-safe processes.

Methods: An integrative narrative review methodology was employed. A systematic search of PubMed, CINAHL, Scopus, and Web of Science (2010-2024) was conducted. Keywords included "critical results," "critical values," "communication failure," "patient safety," "laboratory reporting," and "systems analysis." Included literature comprised sentinel event reports, root cause analyses, quality improvement studies, and reviews on health information technology and human factors engineering.

Results: Communication failures arise from a complex interplay of latent system conditions (e.g., poorly designed interfaces, ambiguous policies, alert fatigue) and active errors (e.g., misdialed numbers, unacknowledged alerts). Effective mitigation requires a multi-layered defense: 1) Robust, redundant, and secure technological pathways mandated and audited by Health Care Security; 2) Clear, standardized protocols defining laboratory and nursing duties with closed-loop verification; 3) A proactive security mindset that treats failures as system breaches, necessitating rigorous root cause analysis and the implementation of corrective controls (e.g., read-back protocols, automated escalation, system hardening).

Conclusion: Safeguarding the critical value chain demands reconceptualizing it as a vital security protocol within the clinical environment. Moving beyond policy reiteration to engineered reliability, informed by human factors and security principles, is essential. A collaborative model where laboratory science, nursing practice, and security engineering jointly own the integrity of this high-stakes information pathway is paramount for eliminating preventable harm.

Keywords: Critical Laboratory Values; Patient Safety; Communication Barriers; Systems Analysis; Root Cause Analysis; Health Information Systems

Introduction

The concept of the "critical value" or "panic value," first articulated by Lundberg in 1972, established a fundamental patient safety tenet: certain laboratory results are so profoundly abnormal they mandate immediate clinician notification to avert catastrophic outcomes, such as arrhythmia from critical hyperkalemia, hypoglycemic coma, or septic shock from a positive blood culture. This protocol creates a critical information lifeline between the laboratory and the bedside. However, this lifeline remains disconcertingly fragile. Despite decades of accreditation standards from bodies like The Joint Commission and the College of American Pathologists, failures in the communication chain persist as a stubborn contributor to preventable patient harm and feature prominently in sentinel event databases (Piva et al., 2011; Valenstein et al.,

*Corresponding author e-mail: ymahde@moh.gov.sa (Yahya Hamad Ahmed Mahdi).
Receive Date: 19 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

2016). These failures—where a known, life-threatening result is either not communicated, not received, or not acted upon—represent a profound breach in the core covenant of healthcare.

Traditional responses often default to retraining individuals or reiterating policies, a strategy that overlooks the complex, systemic nature of these breakdowns. A single missed critical potassium value is rarely the fault of a single negligent person; rather, it is typically the end result of a cascade of latent system failures—a poorly designed order-entry system, ambiguous call-back procedures, conflicting priorities at the nursing station, or a pager with a dead battery (AlSadah et al., 2019). This review posits that managing critical laboratory value (CLV) communication failures requires a paradigm shift: from a focus on individual compliance to a systems analysis and security response. We will investigate the communication chain not merely as an administrative procedure, but as a vital, high-reliability clinical process that must be engineered for safety. This narrative review synthesizes current evidence to analyze the multifactorial etiology of CLV communication failures and propose an integrated, tripartite model for prevention, centering on the essential and interdependent roles of the clinical laboratory, nursing, and health care security/patient safety functions (Saffar et al., 2022).

A Taxonomy of Breakdowns in the Critical Value Chain

To effectively design interventions that prevent communication failures, a nuanced understanding of the precise points where the process breaks down is essential. These breakdowns can occur at any stage, from the analytical phase within the laboratory to the final therapeutic action at the bedside (Getawa et al., 2023). A practical and widely applicable taxonomy organizes these failures into four distinct categories: failures of **transmission, reception, acknowledgment, and action** (Karcher & Lehman, 2014). This framework allows for targeted analysis and remediation by pinpointing the specific vulnerabilities within the critical value chain.

Transmission failures originate within the laboratory at the point of alert initiation. These occur when the laboratory, despite an accurate analytical result, fails to successfully launch the critical notification (Stankovic et al., 2023). Common causes are multifactorial, often stemming from systemic rather than individual shortcomings. They include reliance on incorrect or outdated provider contact information within the laboratory information system (LIS), a failure to recognize a result as critical due to interpretive error or overwhelming workload, or a complete technological failure of an automated notification system (Gosselin et al., 2020). Furthermore, an attempt to communicate can be thwarted by operational missteps, such as calling an incorrect number or leaving a voicemail on an unattended line, coupled with a failure to pursue mandatory escalation pathways as dictated by policy. Each of these scenarios represents a breach at the very genesis of the safety communication (Lippi et al., 2017).

Once a transmission is attempted, the chain remains vulnerable to reception and acknowledgment failures at the clinician node. This broad category encompasses situations where the alert is sent but never properly reaches the cognitive awareness of the intended caregiver or where its receipt is not formally validated. A primary cause is the unavailability of the intended provider—due to being in surgery, off-duty, or otherwise engaged—without a clear and reliable handover protocol. A pervasive and modern challenge is alert fatigue, where excessive clinical decision support (CDS) alerts within electronic health records lead to desensitization and habitual overrides, causing truly critical alerts to be lost in the noise (Ancker et al., 2017). Simple technological failures, such as a silenced phone or a dead pager battery, can also sever the connection. Ambiguous messaging that fails to convey adequate urgency or the absence of a mandatory, structured "read-back" or electronic acknowledgment protocol further compounds the risk, leaving confirmation of accurate data receipt to chance.

The most perilous failure mode is the action failure, which occurs after the result has been successfully transmitted, received, and acknowledged. In this scenario, the clinical information achieves awareness but does not precipitate the required therapeutic intervention. The reasons for such inaction are often rooted in the complex cognitive and social environment of clinical care. They include cognitive overload, where a provider temporarily forgets the alert amidst competing demands; a misunderstanding of the clinical significance of the value; ambiguity about which team member holds responsibility for entering subsequent orders; or a decision to defer action based on flawed clinical judgment without appropriate consultation (Callen et al., 2012). This final breakdown represents the ultimate defeat of the safety system, where knowledge exists but fails to translate into patient care (Meng et al., 2022).

It is crucial to recognize that catastrophic sentinel events are rarely the result of a single, isolated failure. More commonly, they are the product of multiple, sequential failures across these modes—a classic alignment in Reason's Swiss Cheese Model, where latent holes in each layer of defense (policy, technology, human verification) momentarily line up to permit a trajectory of accident (Reason, 2016). For instance, a cascade might begin with a laboratory technologist calling a wrong number (a transmission flaw). The nurse who receives this misdirected call might then fail to identify the correct responsible provider (a reception flaw). Finally, the covering intern who is belatedly

notified might misprioritize the alert amid other urgent tasks (an action flaw). This sequential vulnerability underscores why solutions cannot be monolithic but must be designed to specifically fortify each node in the chain and, critically, the linkages between them, creating a resilient network rather than a fragile sequence.

The Laboratory as the Sentinel

The clinical laboratory is the sentinel, bearing the primary duty to accurately generate results and initiate the alert according to rigorously defined policies. This responsibility extends beyond analytic accuracy to encompass the entire post-analytic communication pathway. Key challenges at this node are manifold. First, defining and maintaining an evidence-based, clinically relevant critical value list that is harmonized across care settings (inpatient, outpatient, emergency department) is an ongoing struggle; lists that are too expansive cause alert fatigue, while overly narrow lists risk missing actionable dangers (Saini et al., 2010). Second, the "call list"—the directory of who to contact—is notoriously dynamic and error-prone, especially in teaching hospitals with rotating residents and complex service structures. Relying on manual lookups or outdated on-call schedules is a high-risk practice (Vesper et al., 2016).

Technology is both a challenge and a solution here. Modern Laboratory Information Systems (LIS) and middleware are integral, automating the identification of critical values and initiating notifications via integrated secure messaging, automated phone calls, or interfaced alerts to the electronic health record (EHR) (Ialongo et al., 2017). However, these systems require meticulous configuration and validation to ensure they are "fail-safe." This includes building in redundancy (e.g., alerting both the primary nurse and the covering provider), escalation logic (if the first recipient does not acknowledge within a defined time window, the alert escalates to a supervisor or rapid response team), and closed-loop tracking (the LIS/EHR maintains an auditable trail documenting who was alerted, when, and who acknowledged) (Yu et al., 2019). The laboratory's quality management system must treat the communication process with the same rigor as analytic testing, performing regular audits of call logs, acknowledgment rates, and turnaround times from result verification to notification. This data is vital for identifying systemic weak points.

The Duty of Nursing to Acknowledge, Interpret, and Act

The nursing role in the CLV chain is that of the crucial nexus, often serving as the first point of clinical contact and the guarantor of the "last mile" to patient intervention. Upon receiving a critical alert—whether directly from the lab, via an EHR inbox, or from another provider—the nurse has a multi-part duty: immediate acknowledgment, clinical interpretation in the context of the patient, and decisive action or escalation. Acknowledgment is the fundamental safety step that closes the loop, confirming to the sender that the message has landed in a responsible clinician's cognitive space. In digital systems, this is often a simple button click, but its importance cannot be overstated; its absence triggers escalation protocols.

The nurse's role, however, transcends passive receipt. It involves interpretation: a critical potassium level of 6.5 mEq/L in a stable chronic kidney disease patient may require a different immediate response than the same value in an acidotic trauma patient. The nurse must therefore possess, or have immediate access to, the clinical judgment and institutional protocols to triage the urgency (Sheehan et al., 2022). Finally, the duty entails action or escalation. If the nurse is authorized and protocols exist (e.g., administering dextrose for critical hypoglycemia), they act. If not, they must immediately escalate to the physician, advanced practice provider, or rapid response team (Kennedy et al., 2023). A critical failure point here is the "unreachable provider." Nursing policies must be unequivocal: if the primary provider cannot be contacted within a defined, brief timeframe (e.g., 15-30 minutes), the chain of command is activated—charge nurse, supervising physician, house officer, or a hospital-wide medical emergency team (Henneman et al., 2010). This removes the burden of indefinite waiting from the nurse and builds a systemic safety net. Alert fatigue is a major threat to this node; when nurses are bombarded with low-priority EHR alerts, they may become desensitized to the truly critical ones, a phenomenon well-documented in clinical decision support literature (Movahedi et al., 2023).

Engineering the Fail-Safe System and Leading the Forensic Response

This review proposes a pivotal, reconceptualized role for Health Care Security—not in the traditional sense of physical safety, but as the function responsible for the security and integrity of the patient safety system itself. In this model, Health Care Security (often housed within or partnering closely with Quality, Patient Safety, and Risk Management) is the architect and auditor of the fail-safe communication infrastructure. Their mandate is to treat the CLV pathway as a critical security protocol, akin to protecting sensitive data or a controlled substance, where any failure is a reportable breach.

Their duties are threefold: Design, Audit, and Respond. In the design phase, security professionals collaborate with clinical, laboratory, and IT stakeholders to engineer resilient systems. This involves principles of high-reliability organization (HRO) theory and human factors engineering: building redundant communication

channels (e.g., secure text message *and* EHR alert *and* a backup pager system); designing user interfaces that minimize cognitive error (clear display of the value, the patient, and required action); and establishing unambiguous, hardwired escalation algorithms that function automatically (Weick & Sutcliffe, 2015).

In the audit phase, security leads proactive surveillance. This means not just monitoring compliance rates, but actively "penetration testing" the system—simulating critical value failures to see where the process breaks down, auditing call logs for near-misses, and analyzing data from the LIS/EHR to identify patterns of delay or non-acknowledgment (Almasi et al., 2021).

When a failure occurs, Health Care Security leads the forensic response. This is a shift from a blame-oriented investigation to a systems-based Root Cause Analysis (RCA) (Kushwaha et al., 2022). The RCA, following methodologies from fields like aviation safety, seeks to uncover the latent conditions—the flawed policies, inadequate training, or technological gaps—that allowed the active error to reach the patient (Peerally et al., 2017). The outcome is not disciplinary action, but the implementation of corrective controls: a change in software configuration, a rewrite of an ambiguous policy, the introduction of a mandatory read-back for verbal reports, or the implementation of a new escalation tool (Sartini et al., 2022). In this framework, every CLV communication failure is a sentinel event for the *system's* security, demanding a containment and remediation response (Table 1).

Table 1: Failure Modes in Critical Value Communication and Corresponding Systemic Safeguards

Failure Mode	Common Causes (Active & Latent)	Affected Node	Proposed Systemic Safeguards & Security Controls
Transmission Failure	Incorrect contact info in LIS; Technologist oversight; Auto-notification system crash.	Laboratory	**Security Control:** Regular audit/update of provider call lists. **System Safeguard:** Automated, rules-based notification from LIS with mandatory fields. **Redundancy:** Primary (EHR alert) + Secondary (secure SMS) pathway.
Reception Failure	Alert fatigue; Silenced phone/pager; Provider off-duty/unavailable.	Nursing/Provider	**Security Control:** Configure "escalation routing" with timeouts (e.g., if unack in 10 min, alert charge nurse). **System Safeguard:** Differentiation of CLV alerts via visual/auditory distinctiveness to combat fatigue.
Acknowledgment Failure	No closed-loop requirement; Ambiguous alert that isn't recognized as critical.	Nursing/Provider	**Security Control:** Mandate "closed-loop" verification; system tracks acknowledgment. **System Safeguard:** Alerts require a structured response (e.g., "Acknowledge" or "View Result").
Interpretation/Handoff Failure	Misheard value (e.g., "1.4" vs. "7.4"); Lack of clinical context; Unclear who is responsible.	All	**Security Control:** Enforce **"read-back" protocol** for verbal reports. **System Safeguard:** EHR alert links directly to patient chart for context; clearly identifies ordering provider.
Action Failure	Cognitive overload/forgetting; Decision to defer; Assumption another will act.	Provider	**Security Control:** Automated creation of a "Critical Result Follow-up" task in EHR. **System Safeguard:** Time-stamped tracking of result receipt to order entry; regular audits of action delays.
Systemic Process Failure	Unclear policies; Lack of integrated technology; No defined escalation path.	Organizational	**Security Lead:** Conduct proactive FMEA (Failure Mode and Effects Analysis) on CLV process. **Corrective Control:** Redesign process using human factors principles; implement organization-wide training on new protocol.

The Technological Backbone: Integrating Systems for Safety and Auditability: The technological infrastructure underpinning critical value communication serves as a double-edged sword; it can enable seamless safety or introduce catastrophic points of failure. Effective risk mitigation demands a fully integrated approach, ensuring robust interoperability between the Laboratory Information System (LIS), the Electronic Health Record (EHR), and secure communication platforms. The ideal state

is a fully automated, "hands-off" pathway where the LIS autonomously identifies a critical value and pushes a structured alert to the EHR. This system then utilizes intelligent routing rules to notify the patient's assigned nurse and covering provider simultaneously via a secure, preferred channel such as a mobile device. For optimal efficacy, these alerts must be both persistent and intrusive enough to demand immediate attention, while remaining sufficiently contextual to facilitate rapid action. Key contextual information includes the patient's name, location, the critical value with its reference range, and a direct link to the patient's chart for immediate clinical review.

Within this integrated framework, several key technological safeguards are non-negotiable. The first is automatic escalation, a logic-driven failsafe where, if a primary recipient does not acknowledge an alert within a pre-configured timeframe (e.g., 5-10 minutes), the system automatically notifies a secondary recipient—such as a charge nurse, backup provider, or rapid response team—without requiring human intervention, thereby closing a critical accountability gap (Singh et al., 2013). Equally vital is the maintenance of a closed-loop audit trail. Every discrete step in the communication sequence—from result generation and transmission to receipt, acknowledgment, and any subsequent chart access or order entry—must be time-stamped and logged in an immutable digital record. This audit trail is forensically indispensable for rigorous Root Cause Analysis (RCA) and provides defensible documentation for legal and accreditation purposes. To maintain system integrity, rigorous configuration management is essential.

Health Care Security and Information Technology departments must jointly control and meticulously document any changes to notification rules, recipient lists, or escalation logic, as an unvetted modification constitutes a direct threat to patient safety (Harrison et al., 2007). Finally, the architecture must embody redundancy and resilience, incorporating a defined fallback protocol for primary system failures like EHR downtime. This redundancy may involve a pre-established phone tree initiated by the laboratory or a secure, standalone messaging platform (Ogundaini et al., 2022). It is critical to acknowledge, however, that technology is not a panacea. Poorly designed or overly sensitive alerting systems are a primary generator of alarm fatigue, which remains the single greatest technological threat to effective critical value communication. To preserve the salience of truly critical alerts, they must be highly specific, clinically validated, and intelligently tiered by urgency to prevent desensitization among clinical staff (Wright et al., 2016).

The Security-Led Root Cause Analysis and Corrective Control Implementation

When a critical laboratory value communication failure results in actual or potential patient harm, the organizational response must be immediate, systematic, and relentlessly focused on system repair rather than individual blame. A Security-led Root Cause Analysis (RCA) provides a structured methodology for this response. The process begins with containment, taking immediate steps to mitigate any ongoing patient harm and to secure all relevant digital evidence, such as freezing audit logs and preserving communication devices. This is followed by the assembly of a cross-functional team that includes laboratory leadership, nursing management, the involved clinicians, and representatives from Health Care Security, Information Technology, and Quality Management to ensure all perspectives are considered. The core investigative phase involves timeline reconstruction, utilizing the immutable digital audit trail to meticulously reconstruct the precise sequence of events from result verification to the failed intervention. With the sequence established, the team engages in the identification of root causes, employing analytical tools like the "5 Whys" or cause-and-effect diagrams to drill past the apparent active error (e.g., "the nurse didn't call") to uncover the latent conditions (e.g., "the nurse was unaware of the escalation policy because training is only annual and not scenario-based") and deeper systemic factors (e.g., "the EHR alert does not display the patient's location, confusing assignment") that created the preconditions for failure (Driesen et al., 2022). The final step is action plan development, where the team identifies and prioritizes specific, measurable corrective controls designed to prevent recurrence of the identified failure mode and similar vulnerabilities (Karkoszka, 2023).

These corrective controls are the tangible output of the RCA and must be tailored to address the root causes. They typically fall into four categories. Policy controls involve revising official protocols to mandate specific safety behaviors, such as requiring a mandatory "read-back" of the value and patient identifiers for all verbal critical value reports. Technological controls entail reconfiguring systems to harden the safety process; an example is reprogramming the LIS to automatically route critical blood culture alerts to an infectious diseases pharmacist in addition to the primary team, thereby creating a parallel, expert verification pathway. Process controls redesign workflows, such as implementing a daily "critical value log review" huddle between laboratory shift supervisors and nursing charge nurses to proactively reconcile any unacknowledged alerts from the previous 24 hours. Finally, training controls focus on building competency through just-in-time, simulation-based education modules for new staff on unit-specific escalation protocols (Bates & Singh, 2018). The overarching role of Health Care Security in this

model is to ensure these controls are not merely recommended but are fully implemented, their effectiveness actively monitored over time, and the entire investigative and improvement process thoroughly documented to foster organizational learning and meet accreditation standards (Table 2).

Table 2: The Tripartite Security-Based Framework for Critical Value Communication

Domain & Lead Function	Core Responsibilities	Key Performance Indicators (KPIs) & Audit Activities	Interventions & Corrective Controls
1. Laboratory (Sentinel & Initiator)	• Define & maintain evidence-based CV list. • Ensure accurate result generation. • Initiate notification via secure, verified channels. • Escalate per protocol if acknowledgment fails.	• % of critical values notified within policy timeframe (e.g., 15 min). • Audit trail completeness for all notifications. • Regular review of "call list" accuracy.	• Automated notification rules with redundancy. • Integration of middleware for intelligent routing. • Monthly audits of notification timeliness.
2. Nursing/Clinical (Nexus & Actor)	• Immediately acknowledge receipt of CV alert. • Interpret result in patient context. • Act per protocol or escalate to provider. • Employ read-back for verbal reports. • Escalate via chain of command if provider unreachable.	• Acknowledgment rate for CV alerts by unit/provider. • Time from acknowledgment to provider notification or intervention. • Compliance with read-back protocol (observed).	• Clear, unit-specific escalation policies. • Training on alert fatigue management. • Integration of CV alerts into nurse handoff tools.
3. Health Care Security (Architect & Auditor)	• Design/approve fail-safe communication infrastructure. • Lead RCAs of failures (treat as system breaches). • Proactively audit system performance & near-misses. • Mandate and verify implementation of corrective controls. • Report on system integrity to executive leadership.	• Number of CLV communication failures (actual harm & near-miss). • Time to complete RCA and implement controls. • Results of proactive "penetration testing." • Control effectiveness (reduction in failure rate post-intervention).	• System-wide FMEA on CLV process. • Configuration management for alerting systems. • Security-led simulation drills. • Standardized RCA toolkit and reporting.

Human Factors and Just Culture: The Psychological Underpinnings of a Safe System

Technological and procedural safeguards will fail if they do not account for human cognition and the organizational culture. Human Factors Engineering (HFE) principles are critical for designing workflows that fit how people actually think and work, not an idealized version. This means simplifying processes, standardizing communication formats (e.g., SBAR: Situation, Background, Assessment, Recommendation), minimizing unnecessary alerts to combat fatigue, and designing interfaces that make the critical information salient and the required action obvious (Russ et al., 2013).

Equally important is fostering a Just Culture. A punitive culture that blames individuals for CLV failures drives reporting underground, prevents learning, and guarantees recurrence (Makary, 2019). A Just Culture distinguishes between human error (unintentional slips), at-risk behavior (cutting corners due to system design), and reckless behavior (conscious disregard of risk) (Lawrence, 2018). The system's response differs for each: consoling and redesign for human error, coaching and process change for at-risk behavior, and disciplinary action only for true recklessness. When nurses and lab techs trust that reporting a near-miss or their own error will lead to system improvement rather than punishment, the organization gains invaluable data for proactive risk reduction. Health Care Security plays a key role in championing and operationalizing Just Culture principles within the safety investigation process (Weiss, 2017).

Conclusion

The communication of critical laboratory values is a fundamental, high-stakes clinical process that has languished as an administrative checklist item for too long. This narrative review argues that its repeated failure is a symptom of systemic vulnerability, not individual unreliability. To fortify this lifeline, we must reconceptualize it through the lenses of systems analysis, human factors engineering, and security science. The proposed tripartite model—integrating the Clinical Laboratory as the sentinel, Nursing as the responsible nexus, and Health Care Security as the architect and forensic guardian of the system—provides a robust framework for accountability and action.

The path forward requires moving from passive policy compliance to active system engineering. It demands investing in integrated, intelligent, and redundant technology that includes closed-loop tracking and automatic escalation. It necessitates a shift in investigative philosophy, led by security and safety professionals, to treat each failure as a breach requiring root cause analysis and the implementation of durable corrective controls. Finally, it must be grounded in human factors design and a Just Culture that supports the people operating within this complex system. By hardening the critical value chain as a key security protocol within the healthcare environment, we can transform it from a recurrent point of failure into a demonstrated, reliable pillar of patient safety.

References

1. Almasi, S., Rabiei, R., Moghaddasi, H., & Vahidi-Asl, M. (2021). Emergency department quality dashboard; a systematic review of performance indicators, functionalities, and challenges. *Archives of academic emergency medicine*, *9*(1), e47. https://doi.org/10.22037/aaem.v9i1.1230
2. AlSadah, K., El-Masry, O. S., Alzahrani, F., Alomar, A., & Ghany, M. A. (2019). Reporting clinical laboratory critical values: a focus on the recommendations of the American College oF Pathologists. *Journal of Ayub Medical College Abbottabad*, *31*(4), 612-618. https://ayubmed.edu.pk/jamc/index.php/jamc/article/view/6379
3. Ancker, J. S., Edwards, A., Nosal, S., Hauser, D., Mauer, E., Kaushal, R., & With the HITEC Investigators. (2017). Effects of workload, work complexity, and repeated alerts on alert fatigue in a clinical decision support system. *BMC medical informatics and decision making*, *17*(1), 36. https://doi.org/10.1186/s12911-017-0430-8
4. Bates, D. W., & Singh, H. (2018). Two decades since to err is human: an assessment of progress and emerging priorities in patient safety. *Health Affairs*, *37*(11), 1736-1743. https://doi.org/10.1377/hlthaff.2018.0738
5. Callen, J. L., Westbrook, J. I., Georgiou, A., & Li, J. (2012). Failure to follow-up test results for ambulatory patients: a systematic review. *Journal of general internal medicine*, *27*(10), 1334-1348. https://doi.org/10.1007/s11606-011-1949-5
6. Driesen, B. E., Baartmans, M., Merten, H., Otten, R., Walker, C., Nanayakkara, P. W., & Wagner, C. (2022). Root cause analysis using the prevention and recovery information system for monitoring and analysis method in healthcare facilities: a systematic literature review. *Journal of patient safety*, *18*(4), 342-350. *DOI:* 10.1097/PTS.0000000000000925
7. Getawa, S., Aynalem, M., Melku, M., & Adane, T. (2023). Blood specimen rejection rate in clinical laboratory: A systematic review and meta-analysis. *Practical laboratory medicine*, *33*, e00303. https://doi.org/10.1016/j.plabm.2022.e00303
8. Gosselin, R. C., Adcock, D., Dorgalaleh, A., Favaloro, E. J., Lippi, G., Pego, J. M., ... & Siguret, V. (2020, June). International council for standardization in haematology recommendations for hemostasis critical values, tests, and reporting. In *Seminars in Thrombosis and Hemostasis* (Vol. 46, No. 04, pp. 398-409). Thieme Medical Publishers. DOI: 10.1055/s-0039-1697677
9. Harrison, M. I., Koppel, R., & Bar-Lev, S. (2007). Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *Journal of the American medical informatics Association*, *14*(5), 542-549. https://doi.org/10.1197/jamia.M2384
10. Henneman, E. A., Roche, J. P., Fisher, D. L., Cunningham, H., Reilly, C. A., Nathanson, B. H., & Henneman, P. L. (2010). Error identification and recovery by student nurses using human patient simulation: Opportunity to improve patient safety. *Applied Nursing Research*, *23*(1), 11-21. https://doi.org/10.1016/j.apnr.2008.02.004
11. Ialongo, C., Pieri, M., & Bernardini, S. (2017). Artificial neural network for total laboratory automation to improve the management of sample dilution: smart automation for clinical laboratory timeliness. *SLAS TECHNOLOGY: Translating Life Sciences Innovation*, *22*(1), 44-49. https://doi.org/10.1177/2211068216636635
12. Karcher, D. S., & Lehman, C. M. (2014). Clinical consequences of specimen rejection: a College of American Pathologists Q-Probes analysis of 78 clinical laboratories. *Archives of Pathology & Laboratory Medicine*, *138*(8), 1003-1008. https://doi.org/10.5858/arpa.2013-0331-CP
13. Karkoszka, T. (2023). Operational Control Model Based on Integrated Failure Analysis and Risk Assessment in Sustainable Technological Processes. *Sustainability*, *15*(24), 16848. https://doi.org/10.3390/su152416848
14. Kennedy, G. A., Pedram, S., & Sanzone, S. (2023). Improving safety outcomes through medical error reduction via virtual reality-based clinical skills training. *Safety Science*, *165*, 106200. https://doi.org/10.1016/j.ssci.2023.106200

15. Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). Systematic review of security vulnerabilities in ethereum blockchain smart contract. *Ieee Access*, *10*, 6605-6621. https://doi.org/10.1109/ACCESS.2021.3140091
16. Lippi, G., Adcock, D., Simundic, A. M., Tripodi, A., & Favaloro, E. J. (2017). Critical laboratory values in hemostasis: toward consensus. *Annals of medicine*, *49*(6), 455-461. https://doi.org/10.1080/07853890.2016.1278303
17. Lawrence, M. B. (2018). The Social Consequences Problem in Health Insurance and How to Solve It. *Harv. L. & Pol'y Rev.*, *13*, 593.
18. Makary, M. (2019). *The price we pay: what broke American health care--and how to fix it*. Bloomsbury Publishing USA.
19. Meng, Y., Zhuge, W., Huang, H., Zhang, T., & Ge, X. (2022). The effects of early exercise on cardiac rehabilitation-related outcome in acute heart failure patients: a systematic review and meta-analysis. *International Journal of Nursing Studies*, *130*, 104237. https://doi.org/10.1016/j.ijnurstu.2022.104237
20. Movahedi, A., Sadooghiasl, A., Ahmadi, F., & Vaismoradi, M. (2023). Smart care for dealing with nurses' alarm fatigue in the intensive care unit. *Journal of Nursing Scholarship*, *55*(4), 825-833. https://doi.org/10.1111/jnu.12870
21. Ogundaini, O., de la Harpe, R., & McLean, N. (2022). Unintended consequences of technology-enabled work activities experienced by healthcare professionals in tertiary hospitals of sub-Saharan Africa. *African Journal of Science, Technology, Innovation and Development*, *14*(4), 876-885. https://hdl.handle.net/10520/ejc-aa_ajstid_v14_i4_a876
22. Peerally, M. F., Carr, S., Waring, J., & Dixon-Woods, M. (2017). The problem with root cause analysis. *BMJ quality & safety*, *26*(5), 417-422. https://doi.org/10.1136/bmjqs-2016-005511
23. Saffar, H., Sefidbakhat, S., Mirzaian, E., Najafabadi, M. K., & Saffar, H. (2022). Laboratory Critical Values; Brief review of definitions, diagnosis, utility of repeat testing, confirmation and reporting. *Clinical Excellence*, *11*(4), 1-12.
24. Saini, K. S., Kaushik, A., Anil, B., & Rambabu, S. (2010). Harmonized medical device regulation: need, challenges, and risks of not harmonizing the regulation in Asia. *Journal of Young Pharmacists*, *2*(1), 101-106.https://doi.org/10.4103/0975-1483.62221
25. Sartini, M., Carbone, A., Demartini, A., Giribone, L., Oliva, M., Spagnolo, A. M., ... & Cristina, M. L. (2022, August). Overcrowding in emergency department: causes, consequences, and solutions—a narrative review. In *Healthcare* (Vol. 10, No. 9, p. 1625). MDPI. https://doi.org/10.3390/healthcare10091625
26. Sheehan, P., Joy, A., Fleming, A., Vosper, H., & McCarthy, S. (2022). Human factors and patient safety in undergraduate healthcare education: a systematic review. *Human factors in healthcare*, *2*, 100019. https://doi.org/10.1016/j.hfh.2022.100019
27. Stankovic, A. K., Blond, B. J., Coulter, S. N., Long, T., & Lindholm, P. F. (2023). Preanalytic Competency Assessment: A Q-Probes Study Involving 46 Health Care Institutions, 447 Blood Collectors/Phlebotomists, and 2212 Individual Assessments. *Archives of Pathology & Laboratory Medicine*, *147*(3), 304-312. https://doi.org/10.5858/arpa.2021-0436-CP
28. Vesper, H. W., Myers, G. L., & Miller, W. G. (2016). Current practices and challenges in the standardization and harmonization of clinical laboratory tests. *The American journal of clinical nutrition*, *104*, 907S-912S. https://doi.org/10.3945/ajcn.115.110387
29. Weiss, P. M. (2017). TRUST: How to build a support net for ObGyns affected by a medical error. *OBG Management*, *29*(1), 25-31.
30. Yu, H. Y. E., Lanzoni, H., Steffen, T., Derr, W., Cannon, K., Contreras, J., & Olson, J. E. (2019). Improving laboratory processes with total laboratory automation. *Laboratory Medicine*, *50*(1), 96-102. https://doi.org/10.1093/labmed/lmy031.