JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2026, VOL 9, NO 4

Balancing Patient Privacy And Data Accessibility In Healthcare CRM: A Risk And Crisis Communication Framework For Trust And Transparency

Jaymin Harishkumar Sutarwala

Independent Researcher, USA

Abstract

Privacy incidents in healthcare customer relationship management (CRM) systems—including data breaches, unauthorized access events, and consent failures—constitute recurring organizational risks that can escalate into full-scale crises, eroding patient trust, damaging institutional reputation, and compromising care continuity. These events pose distinctive communication challenges: organizations must translate complex technical information for diverse stakeholders under time pressure, manage uncertainty about incident scope and impact, and coordinate messaging across legal, clinical, and administrative functions while satisfying regulatory notification requirements. Despite extensive scholarship on healthcare information privacy and on crisis and risk communication, limited research integrates these domains to explain how communication practices interact with privacy control environments to shape trust outcomes following incidents. This paper addresses that gap through an integrative literature review synthesizing health information technology privacy scholarship with crisis and risk communication theory, culminating in the development of the Privacy–Access–Communication (PAC) Framework. Grounded in Situational Crisis Communication Theory and Crisis and Emergency Risk Communication principles, the PAC Framework links technical privacy controls to governance structures and communication practices, providing a systematic approach to privacy risk communication in healthcare CRM contexts. This paper makes three contributions: (1) a theoretically grounded framework integrating technical, governance, and communication dimensions of privacy management; (2) identification of recurring communication patterns connecting access-control mechanisms to stakeholder messaging strategies; and (3) a readiness checklist enabling practitioners to assess communication preparedness for privacy incidents. Implications for crisis communication preparedness in healthcare organizations are discussed, along with directions for empirical validation.

Keywords: Risk Communication; Crisis Communication; Healthcare CRM; Patient Trust; Privacy Transparency; Data Governance; Consent Communication; SCCT/CERC.

1. Introduction

When a healthcare organization discovers unauthorized access to patient records, the technical dimensions of the incident—identifying the vulnerability, containing the breach, assessing the scope of exposure—represent only one aspect of the organizational response. Equally critical, and often more consequential for long-term institutional outcomes, is the communication response: how the organization conveys information about the incident to affected patients, coordinates internal messaging across departments,

satisfies regulatory notification requirements, and undertakes the sustained work of trust repair. Privacy incidents in healthcare settings create profound uncertainty for patients who cannot independently verify what information was accessed, by whom, or for what purposes. This uncertainty, combined with the sensitive nature of health information and the vulnerability inherent in patient-provider relationships, makes privacy incidents particularly potent threats to organizational trust and legitimacy.

The challenge of privacy protection in healthcare information systems extends beyond technical implementation to encompass policy transparency and user awareness. Research examining mobile health applications has demonstrated systematic deficiencies in the availability and understandability of privacy policies, with many health technology platforms lacking sufficient information regarding data collection, usage, and sharing practices (Huckvale et al., 2015). This lack of transparency undermines patient autonomy and informed consent, creating environments where individuals cannot make educated decisions about their health information disclosure. Such challenges manifest in healthcare CRM implementations where institutional privacy policies often remain inaccessible to patients or employ technical language that obscures actual data handling practices. The absence of clear, understandable privacy frameworks erodes trust between healthcare organizations and the communities they serve (Huckvale et al., 2015).

The scale of healthcare privacy incidents underscores the urgency of communication preparedness. Research indicates that 75% of surveyed healthcare organizations in the United States reported at least one security breach affecting fewer than 500 individuals, while 21% reported incidents affecting more than 500 individuals (Keshta & Odeh, 2021). These security incidents originated from both insider threats (53.7% of organizations) and external threats (63.6% of organizations), demonstrating that privacy risks emerge from multiple vectors requiring differentiated communication responses (Keshta & Odeh, 2021). The financial consequences are substantial, with healthcare data breaches costing hospitals between $250,000 and $2.5 million in settlement payments alone—a fraction of the overall reputational and operational burden these incidents impose (Keshta & Odeh, 2021).

Healthcare CRM platforms differ from electronic health records in that they operationalize relationship maintenance through outreach, coordination, and messaging—functions that are directly implicated when privacy incidents become crises. Unlike electronic health record systems focused primarily on clinical documentation, CRM platforms explicitly emphasize relationship management—the ongoing cultivation of trust, communication, and engagement between healthcare organizations and the patients they serve. These systems integrate patient demographics, clinical histories, communication preferences, appointment records, and interaction logs to enable coordinated, personalized engagement across multiple touchpoints and care episodes. The relationship-centered design of CRM platforms makes them simultaneously valuable for trust-building activities and consequential when privacy failures occur. A breach affecting a CRM system is not merely a data security incident; it is a relationship rupture that demands communication-centered repair.

Where national electronic health record architectures have emerged, fundamental tensions have become evident between data accessibility imperatives and privacy protection requirements. Comparative analysis of healthcare information infrastructure development in the United States and Australia demonstrates that centralized data repositories create significant privacy risks and governance challenges while simultaneously offering enhanced capabilities for care coordination (Gunter & Terry, 2005). National-scale implementations must negotiate federal oversight with regional autonomy, coordinate disparate institutional security practices, and balance conflicting stakeholder interests regarding data access rights (Gunter & Terry, 2005). Healthcare CRM systems operating within these broader architectural contexts inherit systemic tensions requiring solutions that address both local institutional needs and ecosystem-wide interoperability demands.

The scholarly literature addressing healthcare privacy and data accessibility has developed predominantly within health informatics and information security domains, generating sophisticated technical solutions—attribute-based access control, field-level encryption, comprehensive audit logging, anomaly detection systems—while treating communication as a secondary implementation concern rather than a core design principle. Current health information technology infrastructure comprises predominantly closed, monolithic systems that function as data silos rather than platforms enabling flexible access patterns (Mandl

& Kohane, 2012). This architectural constraint limits organizations' ability to implement context-aware access controls reflecting institutional policies and clinical workflows. Proprietary system designs resist interoperability, preventing integration of innovative access management solutions and inhibiting deployment of sophisticated authorization logic that could support nuanced communication about access decisions (Mandl & Kohane, 2012).

Concurrently, crisis and risk communication scholarship has developed robust theoretical frameworks for understanding how organizations should communicate during adverse events, yet this literature has rarely been applied systematically to healthcare privacy contexts. This fragmented approach creates implementation gaps where technically sound privacy architectures fail to support effective crisis communication when incidents occur.

This paper addresses this gap by developing an integrated framework that connects technical privacy controls to communication practices through the lens of crisis and risk communication theory. Drawing on Situational Crisis Communication Theory (SCCT) and Crisis and Emergency Risk Communication (CERC) principles, the Privacy-Access-Communication (PAC) Framework provides healthcare organizations with a systematic approach to managing privacy as both a technical and communicative challenge.

This paper makes three contributions:

First, it provides a theoretically grounded framework—the PAC Framework—that integrates technical privacy controls, governance structures, and communication practices into a coherent system for healthcare CRM privacy management. Second, it identifies specific communication patterns that link access control mechanisms (such as break-glass protocols and audit logging) to stakeholder messaging strategies, enabling organizations to anticipate communication needs based on technical system design. Third, it offers an evaluation checklist that practitioners can use to assess organizational communication readiness for privacy incidents, supporting proactive preparation rather than reactive crisis response.

The remainder of this paper is organized as follows: Section II reviews literature from both health IT privacy and crisis/risk communication domains, identifying the gap this paper addresses. Section III presents the theoretical framework grounding the analysis. Section IV describes the methodological approach. Section V presents the PAC Framework in detail. Sections VI through VIII examine technical controls, governance structures, and communication practices respectively, with attention to their interconnections. Section IX discusses implications for crisis communication in healthcare organizations. Section X addresses limitations and future research directions, and Section XI concludes.

2. Literature Review

2.1 Health Information Technology Privacy and Access Scholarship

Healthcare information systems present distinctive privacy challenges stemming from the sensitive nature of health data and the diverse access requirements of clinical workflows. Research has documented that physicians demonstrate significant concern about unauthorized access to patient information stored in electronic medical records, with many preferring paper records due to perceived superior security and confidentiality (Keshta & Odeh, 2021). This concern reflects broader tensions between accessibility requirements—clinical staff need rapid access to support care delivery—and privacy protection imperatives that demand careful access restriction.

Systematic assessment of privacy practices across health information technologies reveals concerning patterns. Privacy policy risk assessment studies demonstrate that health technology platforms frequently fail to adequately disclose data collection scope, retention periods, third-party sharing arrangements, and user rights regarding access and erasure of information (LaMonica et al., 2021). These policy transparency deficiencies extend beyond mobile applications to institutional healthcare CRM implementations, where privacy frameworks often prove inaccessible or incomprehensible to patients attempting to understand how their information is handled (LaMonica et al., 2021). The absence of clear privacy documentation undermines the informed consent foundation upon which legitimate health data processing depends.

Patient perspectives on healthcare data security underscore the significance of these transparency gaps. Research examining patient concerns regarding mHealth applications identifies unauthorized access, data breaches, inadequate encryption standards, and insufficient transparency regarding record access as primary sources of apprehension (Alhammad et al., 2024). These concerns reflect justifiable uncertainty about technical vulnerabilities in healthcare information systems and highlight the need for robust audit mechanisms that not only document access patterns but also provide patients with visibility into record access history through transparent audit interfaces (Alhammad et al., 2024). Patient-facing audit transparency mechanisms enable individuals to review who accessed their records, helping deter unauthorized access while demonstrating organizational accountability.

The technical literature has developed sophisticated access control mechanisms to address privacy-access tensions. Attribute-based access control (ABAC) represents an evolution from traditional role-based permission models, evaluating dynamic contextual attributes such as department assignment, active patient-provider relationships, current care episode status, time-of-access constraints, and purpose-of-use declarations (Keshta & Odeh, 2021). Field-level encryption provides differentiated protection for particularly sensitive data categories, including psychiatric notes, genetic testing results, and substance abuse treatment records. Comprehensive audit logging creates retrospective accountability by recording every access event with user identity, records accessed, and temporal metadata.

Break-glass protocols address emergency access requirements by allowing clinicians to bypass standard authentication during time-critical care episodes while generating enhanced audit trails for retrospective review. These mechanisms acknowledge that rigid access restrictions can compromise patient safety when immediate information availability is clinically necessary. However, the communication implications of break-glass usage—how organizations explain these exceptional access events to patients, how they investigate potential misuse, and how they maintain accountability—receive limited attention in technical literature.

The shift toward patient-centered health information management introduces additional architectural considerations. Contemporary approaches position the personal health record as an active tool supporting patient self-management rather than a passive repository of clinician-generated documentation (Brennan et al., 2010). Healthcare CRM architectures must accordingly support bidirectional data flow, where patients contribute observations about symptoms, medication adherence, and daily health measurements while maintaining control over information disclosure to clinical teams (Brennan et al., 2010). This patient-centric approach requires access control models supporting patient-defined permissions, selective data sharing based on trust relationships, and transparency mechanisms enabling patients to audit record access history and purposes.

The current health information technology infrastructure presents fundamental barriers to flexible access control implementation. The predominance of closed, monolithic systems creates data silos rather than platforms enabling diverse applications and access patterns (Mandl & Kohane, 2012). This architectural constraint results in healthcare CRM implementations where organizations must operate within rigid access paradigms dictated by vendor design choices rather than implementing context-aware controls reflecting workflow-driven institutional policies (Mandl & Kohane, 2012). Closed systems preclude deployment of innovative access management solutions; limited or absent application programming interfaces inhibit integration of third-party security tools or custom authorization logic. The absence of platform-based architectures supporting substitutable applications perpetuates vendor lock-in, preventing organizations from adopting superior access control technologies without wholesale system replacement (Mandl & Kohane, 2012).

2.2 Privacy Challenges in Specialized Healthcare Contexts

The protection of patient privacy extends beyond structured data in electronic health records to encompass clinical images, video recordings, and detailed case descriptions increasingly incorporated into healthcare CRM systems for documentation, education, and quality improvement purposes. Visual documentation presents heightened privacy concerns because of the inherently identifiable nature of facial images and distinguishing physical features that resist conventional anonymization techniques (Robinson et al., 2014).

Regulatory frameworks governing clinical images must address consent requirements explaining permissible uses, storage security protecting against unauthorized access or distribution, and patient rights to withdraw consent or request destruction of images not serving legitimate clinical purposes (Robinson et al., 2014).

Healthcare CRM implementations incorporating multimedia capabilities for documentation must implement technical controls restricting image access to authorized clinical staff, watermarking mechanisms deterring unauthorized distribution, and audit trails documenting every instance of image viewing or export (Robinson et al., 2014). Visual documentation raises ethical considerations regarding power dynamics inherent in clinical relationships, where patients may feel coerced into providing consent for photography despite misgivings about long-term image use beyond initially disclosed purposes (Robinson et al., 2014). Communication about visual documentation policies requires particular sensitivity to these power imbalances.

Algorithmic decision systems embedded within healthcare CRM platforms introduce additional privacy and equity concerns. Research has documented significant racial bias in algorithms used to manage population health, where training data deficiencies, feature selection choices, and optimization targets can inadvertently perpetuate healthcare disparities affecting marginalized populations (Obermeyer et al., 2019). Clinical decision support algorithms recommending treatment pathways, resource allocation tools prioritizing patient scheduling, and risk stratification models identifying high-risk individuals require robust bias testing examining differential performance across demographic groups (Obermeyer et al., 2019). Addressing these algorithmic dimensions requires interdisciplinary governance structures integrating technical security expertise, clinical domain knowledge, bioethical analysis, and community representation to ensure that healthcare CRM implementations serve population health needs equitably while respecting individual privacy rights (Obermeyer et al., 2019).

2.3 Crisis and Risk Communication Scholarship

Crisis communication scholarship provides theoretical frameworks for understanding how organizations should respond when adverse events threaten stakeholder relationships and institutional reputation. Situational Crisis Communication Theory (SCCT), developed by Coombs (2007), offers an evidence-based framework for maximizing reputational protection through post-crisis communication. SCCT is grounded in Attribution Theory, which posits that people search for causes of events, especially those that are negative and unexpected, and that attributions of responsibility generate emotional reactions that motivate behavioral responses (Coombs, 2007).

SCCT identifies three crisis clusters based on attributions of organizational responsibility: the victim cluster (natural disasters, workplace violence, product tampering, rumors) generates weak attributions with mild reputational threat; the accidental cluster (technical-error accidents, technical-error product harm, challenges) generates minimal attributions with moderate reputational threat; and the preventable cluster (human-error accidents, human-error product harm, organizational misdeed) generates strong attributions with severe reputational threat (Coombs, 2007). Crisis history and prior relational reputation serve as intensifying factors that can amplify reputational threat regardless of initial crisis type (Coombs, 2007).

SCCT prescribes response strategies matched to reputational threat levels. Denial strategies (attack the accuser, denial, scapegoating) seek to remove organizational connection to the crisis. Diminish strategies (excuse, justification) argue that the crisis is not as severe as perceived or that the organization lacked control. Rebuild strategies (compensation, apology) offer material and symbolic aid to victims, accepting greater organizational responsibility (Coombs, 2007). Research demonstrates that using overly accommodative strategies when unnecessary provides no greater reputational benefit than strategies matched to the situation, and may even worsen outcomes by suggesting the crisis is more severe than stakeholders initially believed (Coombs, 2007).

Crisis and Emergency Risk Communication (CERC) merges traditional health and risk communication with crisis and disaster communication, recognizing that health emergencies require communication approaches spanning pre-event preparation through post-event recovery (Reynolds & Seeger, 2005). The CERC model outlines five developmental stages with distinct communication activities: pre-crisis (risk

messages, warnings, preparation), initial event (uncertainty reduction, self-efficacy, reassurance), maintenance (ongoing uncertainty reduction, feedback correction), resolution (updates, discussions of cause and new risk understandings), and evaluation (assessment of response adequacy, lessons learned) (Reynolds & Seeger, 2005).

CERC emphasizes that crisis communication is most effective when integrated into decision-making processes rather than treated as post-hoc messaging (Seeger, 2006). Best practices identified through expert panel processes include: pre-event planning, partnerships with the public, listening to public concerns, honesty and openness, collaboration with credible sources, meeting media needs, communicating with compassion, accepting uncertainty, and providing messages of self-efficacy (Seeger, 2006). These practices acknowledge that crises are inherently uncertain situations where overconfident statements may undermine credibility as events evolve unexpectedly.

Recent scholarship challenges static interpretations of crisis communication theories, arguing that effective responses must anticipate and adapt to evolving dynamics in ongoing crises (Jong, 2025). Research demonstrates that stakeholder perceptions of crisis responsibility can shift as new information emerges about causes, as contributing factors come to light, and as multiple actors' relative responsibilities become clearer through investigation (Jong, 2025). This dynamic perspective suggests that initial crisis responses should leave room for adaptation rather than committing to positions that may prove untenable as circumstances evolve (Jong, 2025).

2.4 Gap Identification

Despite extensive development in both domains, limited scholarship integrates health IT privacy and crisis communication perspectives to address how communication practices affect trust outcomes during privacy incidents. Technical literature treats communication as an implementation detail rather than a design principle. Crisis communication literature has not systematically addressed healthcare privacy incidents as a distinctive crisis type requiring tailored theoretical application.

This gap has practical consequences. Organizations implementing sophisticated technical controls may lack communication protocols for explaining access decisions, responding to breach discoveries, or maintaining transparency about data handling practices. The three security-safeguard themes—administrative, physical, and technical—that structure healthcare information security have not been extended to incorporate communication safeguards as a fourth dimension (Keshta & Odeh, 2021). Privacy incidents require not only technical containment but also communicative response addressing stakeholder uncertainty, maintaining trust, and supporting relationship repair.

Healthcare privacy incidents possess characteristics complicating direct application of general crisis communication frameworks. Unlike industrial accidents or product failures where harm is often immediately visible, privacy breaches involve invisible information exposure whose consequences may be delayed, difficult to quantify, and variably significant depending on what information was accessed. Attribution of responsibility may be complicated by technical complexity that stakeholders cannot easily evaluate. Multiple actors—healthcare organizations, technology vendors, regulatory bodies, individual employees—may share responsibility in ways that evolve as investigations proceed (Jong, 2025).

This paper addresses the identified gap by developing a framework integrating technical privacy mechanisms with crisis communication theory, providing healthcare organizations with guidance for managing privacy as both a technical and communicative challenge. Across health IT privacy scholarship, robust technical mechanisms are well specified (e.g., access controls, audit logging, encryption), but their communication consequences—what organizations can credibly explain, how uncertainty is managed, and how trust repair unfolds—are rarely treated as core design constraints. Across crisis and risk communication scholarship, frameworks such as SCCT and CERC provide evidence-based guidance for response strategy selection and phase-based messaging, yet healthcare privacy incidents are under-theorized as a distinct class of "invisible harm" crises characterized by technical opacity, delayed consequences, and shifting responsibility attributions. The PAC Framework is proposed to integrate these strands by specifying how privacy control environments enable or constrain communication strategies and, in turn, shape stakeholder trust outcomes.

3. Theoretical Framework

This paper grounds its analysis in two complementary theoretical frameworks from crisis and risk communication scholarship: Situational Crisis Communication Theory (SCCT) as the primary framework for understanding crisis response strategy, and Crisis and Emergency Risk Communication (CERC) as a supporting framework for understanding developmental communication needs across crisis phases.

3.1 Situational Crisis Communication Theory

SCCT provides the primary theoretical lens for analyzing healthcare privacy incidents because it offers evidence-based guidance for matching communication responses to situational factors affecting stakeholder perceptions (Coombs, 2007). The theory's foundation in Attribution Theory is particularly relevant to privacy contexts where patients must assess organizational responsibility for incidents they cannot directly observe or evaluate.

Healthcare privacy incidents map onto SCCT's crisis typology with important nuances. External cyber attacks where the organization maintains appropriate security may be perceived as victim crises with weak responsibility attributions. Technical failures in access control systems, even without malicious intent, may be perceived as accidental crises with moderate responsibility attributions. Incidents involving inadequate security practices, ignored warnings, or prioritization of convenience over protection may be perceived as preventable crises with strong responsibility attributions and severe reputational threat.

SCCT's intensifying factors—crisis history and prior relational reputation—are particularly salient in healthcare contexts where organizations maintain ongoing relationships with patient populations. An organization experiencing repeated privacy incidents will face intensified attributions regardless of the circumstances of any individual event. Similarly, organizations with poor prior reputations for transparency or patient care will face greater reputational threat from privacy incidents than organizations with established trust reserves (Coombs, 2007).

The theory's response strategies provide a framework for analyzing healthcare privacy communication:

Denial strategies may be appropriate when organizations can demonstrate that alleged incidents did not occur or that the reported scope is inaccurate. However, denial strategies carry significant risk in healthcare contexts where regulatory requirements mandate breach notification and where denial proven false would catastrophically damage credibility.

Diminish strategies may be appropriate when organizations can legitimately demonstrate limited control over incident causes (sophisticated external attacks despite appropriate security) or can contextualize incident severity (accessed information was limited in sensitivity). These strategies require careful calibration to avoid appearing dismissive of patient concerns.

Rebuild strategies involving compensation and apology are appropriate when organizational responsibility is clear or when reputational threat is severe, regardless of actual responsibility. In healthcare contexts, rebuild strategies may include credit monitoring services, enhanced access controls, and concrete policy changes demonstrating organizational commitment to improvement.

Table 1. SCCT Crisis Clusters Applied to Healthcare Privacy Incidents [Coombs, 2007]

Crisis Cluster	Reputational Threat	Healthcare Privacy Examples	Recommended Response
Victim (Organization viewed as victim; weak attributions)	Mild	External cyber attack despite robust security; sophisticated ransomware; third-party vendor breach	Bolstering; Victimage; Emphasize security investments
Accidental (Unintentional event; minimal attributions)	Moderate	Technical system failure; software vulnerability; misconfigured access controls; unintentional employee error	Excuse; Justification; Corrective action focus
Preventable (Negligent or purposeful; strong attributions)	Severe	Insider snooping; ignored security warnings; inadequate encryption; failure to patch known vulnerabilities	Full apology; Compensation; Concrete corrective actions

3.2 Crisis and Emergency Risk Communication

CERC complements SCCT by providing a developmental perspective, recognizing that communication needs evolve across crisis phases (Reynolds & Seeger, 2005). Where SCCT focuses on matching response strategies to crisis situations, CERC emphasizes that communication activities should align with temporal stages of crisis development.

The pre-crisis phase in healthcare privacy contexts involves communicating about privacy policies, explaining access controls to patients, and building an understanding of data handling practices that will support trust maintenance if incidents occur. Organizations that have established clear privacy communication during routine operations possess reputational capital, providing a buffer during crises (Coombs, 2007).

The initial event phase requires rapid communication addressing stakeholder uncertainty about what happened, what information was affected, and what immediate protective actions patients should take. CERC emphasizes empathy, reassurance, and provision of self-efficacy information enabling stakeholders to take protective action (Reynolds & Seeger, 2005). In privacy contexts, this may include guidance on monitoring financial accounts, changing passwords, or requesting credit freezes.

The maintenance phase involves ongoing communication as investigation proceeds, new information emerges, and the full scope of incidents becomes clearer. CERC recognizes that initial communications may require correction as facts develop, emphasizing the importance of acknowledging uncertainty rather than over-committing to positions that may prove inaccurate (Reynolds & Seeger, 2005).

The resolution phase involves communicating about completed investigations, implemented corrective actions, and changed policies or procedures. This phase connects to trust repair and organizational learning, demonstrating that the organization has addressed root causes rather than merely responding to immediate incident demands.

3.3 Propositions Guiding Framework Development

Drawing on these theoretical foundations, five propositions guide the development of the PAC Framework:

Proposition 1: Routine transparency about access controls and data handling practices is associated with lower perceived privacy risk and greater reputational capital, which buffers trust loss during subsequent privacy incidents.

Proposition 2: Timely incident communication is associated with reduced uncertainty and lower trust erosion by signaling organizational accountability and response capability.

Proposition 3: Incident messages that acknowledge appropriate organizational responsibility while explicitly communicating uncertainty (rather than over-committing to incomplete facts) are associated with higher perceived credibility over the course of an evolving investigation.

Proposition 4: Communication channel selection is associated with patient comprehension and emotional response, with channel effectiveness contingent on incident severity and patient population characteristics (e.g., digital access, health literacy).
Proposition 5: Coordinated internal communication across legal, compliance, clinical operations, information security, and public affairs is associated with greater external message consistency and more effective trust maintenance.
These propositions connect technical privacy mechanisms to communication practices by identifying how system design choices (such as audit logging capability, break-glass protocols, or access notification features) create or constrain communication options during privacy incidents.

Table 2. CERC Communication Phases for Healthcare Privacy Incidents (Reynolds & Seeger, 2005).

Phase	Timing	Communication Objective	Key Messages	Recommended Channels
Pre-Crisis	Ongoing (before incidents)	Build trust; establish transparency	"How we protect your information"; "Your privacy rights"	Privacy policies; patient portals; onboarding materials
Initial Event	0-72 hours post-discovery	Reduce uncertainty; provide self-efficacy	"What we know"; "What we are doing"; "What you can do"	Direct notification; press release; hotline
Maintenance	72 hours - investigation end	Provide updates; correct misinformation	"Investigation continues" "What we have learned"	Scheduled updates; FAQ; portal notifications
Resolution	Post-investigation	Communicate findings; support trust repair	"Root cause identified"; "Changes implemented"	Comprehensive report; patient outreach; media statement
Evaluation	Post-resolution	Document lessons; communicate improvements	"What we learned"; "How we have improved"	Internal reports; public transparency reports

4. Method and Approach

4.1 Research Design
This paper employs integrative literature review combined with conceptual framework development to address the identified gap between health IT privacy scholarship and crisis communication theory. Integrative review methodology synthesizes diverse literature streams to generate new frameworks and perspectives, making it appropriate for bridging established but disconnected research domains.
4.2 Data Sources and Search Strategy
Literature was gathered from academic databases including PubMed, Communication Abstracts, Web of Science, and Google Scholar. Search terms combined privacy and security terminology (electronic health records, healthcare CRM, data breach, access control, audit logging, HIPAA) with communication terminology (crisis communication, risk communication, trust, transparency, stakeholder messaging, breach notification). Date parameters extended from 2005 to 2025 to capture both foundational theoretical work and recent empirical developments.
Source selection followed a purposive approach consistent with integrative review methodology. Initial searches identified relevant literature addressing healthcare information privacy, access control

mechanisms, and crisis communication theory. Additional sources were identified through backward citation tracking of seminal works and forward citation searches to locate recent scholarship extending foundational frameworks. Sources were evaluated for inclusion based on their relevance to the intersection of healthcare privacy and crisis communication, methodological rigor, and contribution to the constructs central to the proposed framework. Priority was given to peer-reviewed empirical studies, foundational theoretical articles establishing SCCT and CERC frameworks, and systematic reviews synthesizing evidence on healthcare information security practices. The final synthesis incorporated 15 sources spanning health informatics, communication studies, and information security domains.

4.3 Inclusion Criteria

Articles were included if they addressed: (a) healthcare information privacy or security with attention to organizational or communication dimensions, (b) crisis or risk communication theory with potential application to organizational incidents, (c) patient perspectives on healthcare privacy, trust, or communication, or (d) regulatory frameworks governing healthcare privacy with communication requirements. Technical articles focused exclusively on cryptographic methods or system architecture without organizational or communication dimensions were excluded.

4.4 Synthesis Process

Thematic analysis identified recurring constructs across literature streams: access control mechanisms appeared in technical literature while accountability and transparency appeared in communication literature, suggesting connection points for integration. Framework development proceeded iteratively, with initial category structures refined through repeated engagement with source materials. The resulting PAC Framework emerged from synthesis of technical privacy mechanisms, governance structures identified in regulatory literature, and communication practices derived from crisis communication theory.

4.5 Framework Validation Approach

Framework coherence was examined through structured plausibility checks against documented classes of privacy incidents (e.g., external attacks, accidental misconfiguration, insider misuse), assessing whether PAC constructs capture key response constraints and communication demands described in incident reports and scholarly accounts. This step is intended as conceptual triangulation rather than empirical validation; the propositions and framework relationships require future hypothesis testing and field-based evaluation to establish predictive validity.

5. The Privacy-Access-Communication (PAC) Framework

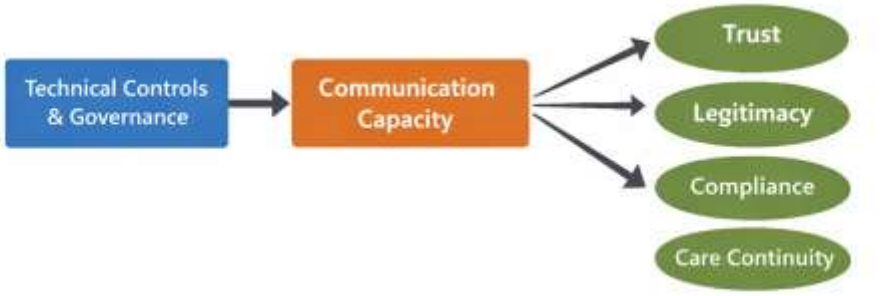
The PAC Framework integrates three interconnected layers—Technical Controls, Governance Structures, and Communication Practices—that collectively determine organizational capacity for managing privacy as both security and communication challenge. Each layer influences the others: technical controls create governance requirements and communication opportunities; governance structures determine how technical controls are implemented and how communication is authorized; communication practices affect stakeholder perceptions that ultimately determine whether technical and governance measures achieve their intended trust outcomes.

5.1 Framework Overview

Technical Controls Layer encompasses the mechanisms regulating data access, protecting information security, and creating audit records documenting system interactions. These controls—including attribute-based access control, field-level encryption, audit logging, break-glass protocols, and anomaly detection—are typically designed for security purposes but possess significant communication implications often under-recognized.

Governance Layer encompasses policies, oversight structures, and procedural frameworks determining how technical controls are configured, how exceptions are handled, and how incidents are escalated and investigated. Governance structures establish organizational authority for communication decisions, determining who can authorize public statements, what information can be disclosed, and how regulatory notification requirements are satisfied.

Communication Practices Layer encompasses the messages, channels, and interaction patterns through which organizations communicate with stakeholders about privacy matters. This includes routine communication about data handling practices, incident notification and response communication, and ongoing trust maintenance activities.



Technical controls and governance structures shape communication capacity, which in turn inffluences trust, legitimacy, compliance, and care continuity outcomes.

Figure 1: The PAC Framework Diagram

Figure 1 summarizes the PAC Framework by depicting how technical controls and governance structures shape communication capacity, which in turn influences trust, legitimacy, compliance, and care continuity outcomes.

5.2 Framework Relationships

The framework posits bidirectional relationships among layers:

Technical controls enable communication by creating audit records shareable with patients, access logs documenting accountability, and system features (such as patient portals) facilitating transparency. Technical controls also constrain communication by determining what information is available about access events and by shaping what explanations are possible when incidents occur.

Governance structures authorize communication by establishing approval processes for public statements, defining spokesperson roles, and determining escalation pathways. Governance structures also require communication through policies mandating breach notification, patient access rights, and transparency about data handling.

Communication practices inform governance by surfacing stakeholder concerns requiring policy adjustment and providing feedback about approach effectiveness. Communication practices depend on technical controls for information necessary to construct accurate and complete messages about system access, incident scope, and remediation actions.

5.3 Outcome Orientation

The framework identifies four outcome domains affected by the interaction of technical controls, governance structures, and communication practices:

Trust reflects stakeholder confidence in organizational commitment to privacy protection and honest communication about data handling. Trust serves as a reputational capital providing buffer during incidents (Coombs, 2007).

Perceived Legitimacy reflects stakeholder assessment that organizational privacy practices are appropriate, fair, and consistent with reasonable expectations. Legitimacy supports cooperation with organizational policies and acceptance of necessary data sharing.

Compliance reflects patient willingness to share accurate health information and engage fully with care processes. Privacy concerns undermining compliance may compromise care quality and research participation.

Care Continuity reflects maintenance of effective patient-provider relationships despite privacy incidents or concerns. Where trust repair succeeds, care relationships may continue; where it fails, patients may seek alternative providers or withhold information.

6. Technical Controls and Communication Implications

Healthcare information systems employ multiple technical control categories, each possessing distinct communication implications extending beyond their primary security functions. This section examines major control types through the lens of communication enablement, communication risks, and connections to crisis communication theory.

6.1 Attribute-Based Access Control

Technical Function: Attribute-based access control (ABAC) evaluates multiple contextual factors—user credentials, organizational role, patient-provider relationships, time of access, access location, and declared purpose—to make dynamic authorization decisions. Unlike role-based systems granting static permissions based on job title, ABAC adjusts access rights based on situational context (Keshta & Odeh, 2021).

Communication Enablement: ABAC's contextual evaluation creates detailed records explaining why access was granted or denied, not merely whether access occurred. These explanations support patient-facing transparency: organizations can describe access policies in terms patients understand ("your cardiologist can see your cardiac records during your appointment") rather than abstract technical terms. When patients request information about record access, ABAC systems can provide context-rich responses identifying treatment relationship, care episode, and access purpose.

Communication Risks: ABAC's complexity creates explanation challenges. Patients may struggle to understand why the same provider had access in one situation but not another. System decisions appearing arbitrary from patient perspectives require careful explanation to maintain legitimacy. Additionally, ABAC policy configurations are organizational choices that may be contested—patients may disagree with decisions about which attributes should authorize access, creating communication demands beyond technical explanation. In patient-facing communication, organizations should distinguish clearly between routine multi-staff access patterns and anomalous access indicators to avoid unintentionally alarming patients with technically accurate but context-poor audit disclosures.

Theoretical Connection: ABAC supports SCCT's rebuild strategies by demonstrating organizational sophistication in protecting patient information. When incidents occur, organizations can point to ABAC systems as evidence of privacy commitment, potentially moderating attributions of organizational responsibility. However, ABAC failures may intensify attributions precisely because sophisticated systems were in place but did not prevent the incident.

6.2 Audit Logging and Anomaly Detection

Technical Function: Comprehensive audit logging records every access event with user identity, patient records accessed, specific data fields viewed or modified, timestamp, access location, and declared purpose. Anomaly detection systems analyze audit logs for suspicious patterns, including bulk record downloads, accesses without documented treatment relationships, unusual timing or location patterns, and sequential accesses suggesting systematic data collection (Keshta & Odeh, 2021).

Communication Enablement: Audit logs create the evidentiary foundation for incident communication. Without detailed logs, organizations cannot answer patient questions about who accessed records, what was viewed, or when access occurred. Robust audit capabilities enable specific, factual breach notifications rather than vague statements acknowledging unknown exposure. Anomaly detection supports proactive communication by identifying potential incidents before they become crises, enabling early notification that may moderate trust damage.

Research indicates that patients demonstrate significant concern about who can view their personal health information and want transparency regarding record access (Alhammad et al., 2024). The development of patient-facing audit portals where individuals can review access history responds to these concerns. Audit transparency mechanisms enable patients to discover suspicious access patterns, supporting collaborative monitoring between organizations and patients (Alhammad et al., 2024).

Communication Risks: Raw audit data may overwhelm or confuse patients unfamiliar with healthcare system operations. Showing that dozens of staff members accessed records during hospitalization may alarm patients, not understanding the routine care team composition. Anomaly detection systems generate false positives, potentially triggering investigation communications that prove unnecessary and create patient anxiety without justification. Alert fatigue among security staff may delay response to genuine incidents, extending the period before notification occurs.

Theoretical Connection: Audit logging supports SCCT's rebuild strategies through demonstrated accountability—organizations can show exactly what happened during incidents, supporting apology and compensation communications with factual foundations. CERC's emphasis on reducing uncertainty aligns with audit capabilities, enabling specific rather than vague incident communication.

6.3 Break-Glass Protocols

Technical Function: Break-glass protocols allow clinicians to bypass standard authentication during emergencies when immediate access to patient information may affect safety. These protocols acknowledge that rigid access restrictions can compromise care during time-critical episodes. Break-glass access generates enhanced audit trails and triggers supervisory notification for retrospective review.

Communication Enablement: Break-glass systems create documented evidence that access occurred under emergency circumstances, supporting explanations to patients concerned about unusual access events. The enhanced audit trail enables organizations to demonstrate that emergency access was reviewed appropriately, reinforcing accountability despite bypassed controls. Clear break-glass policies communicated to patients in advance may increase acceptance of emergency access as legitimate.

Communication Risks: Break-glass mechanisms represent potential abuse vectors—staff may invoke emergency justifications inappropriately to access records for non-clinical purposes. When misuse is discovered, organizations must communicate to affected patients about access that bypassed normal protections, a particularly difficult message acknowledging control weakness while maintaining overall credibility. The retrospective review process creates a delay between access and any notification, potentially undermining trust if patients learn of access through other means before organizational communication.

Theoretical Connection: Break-glass incidents may be framed as victim crises (the organization is also affected by emergency circumstances requiring exceptional measures) or preventable crises (the organization failed to prevent misuse of emergency protocols), depending on circumstances (Coombs, 2007). Communication strategy must align with the appropriate crisis type, requiring investigation completion before response strategy selection. This aligns with Jong's (2025) emphasis on anticipating how perceptions may shift as additional information emerges.

6.4 Field-Level Encryption

Technical Function: Field-level encryption protects particularly sensitive data categories—psychiatric notes, genetic testing results, substance abuse treatment records, HIV status—with cryptographic methods preventing access even by database administrators or during system breaches. Encrypted fields require both appropriate permissions and valid decryption credentials (Keshta & Odeh, 2021).
Communication Enablement: Field-level encryption supports messaging about differentiated protection: organizations can communicate that particularly sensitive information receives additional safeguards beyond general security measures. In breach notifications, organizations may be able to specify that certain data categories remained protected even though other records were exposed, potentially limiting trust damage.
Communication Risks: Key management complexity creates operational challenges, potentially affecting system availability, which could compromise care communication by delaying access to protected information during treatment. Encryption provides technical protection but not communication guidance—patients concerned about sensitive information need reassurance about organizational culture and staff behavior, not merely cryptographic guarantees. Over-reliance on technical protection messaging may appear defensive if patients question why encryption was necessary rather than preventing sensitive information collection.
Theoretical Connection: Field-level encryption supports diminish strategies by allowing organizations to argue that breach severity was limited because sensitive categories remained protected (Coombs, 2007). This framing acknowledges incident occurrence while contesting scope.

6.5 Summary: Technical Controls Communication Matrix

Technical privacy controls in healthcare CRM systems serve primary security functions while simultaneously creating communication opportunities and constraints. Each control mechanism affects organizational capacity to explain access decisions, respond to incidents, and maintain transparency with patients. Table 3 summarizes the communication implications of major technical controls, identifying what each control enables from a communication perspective, the associated communication risks, and connections to crisis communication theory.

Table 3. Technical Controls Communication Matrix

Control	Communication Enablement	Communication Risks	SCCT Connection
ABAC	Context-rich access explanations; policy transparency	Complexity creates confusion; contested policy choices	Rebuild (demonstrates commitment)
Audit Logging	Evidentiary foundation; patient portals; proactive detection	Data overwhelm; false positive anxiety; alert fatigue	Rebuild (accountability evidence)
Break-Glass	Emergency justification documentation; review accountability	Abuse communication difficulty; notification delay	Variable (victim vs. preventable framing)
Field Encryption	Differentiated protection messaging; limited scope claims	Availability impacts: organizational culture deflection	Diminish (severity limitation)

7. Governance Structures and Communication Authorization

Governance structures determine how technical controls are operationalized, how incidents are investigated and escalated, and how communication decisions are authorized. Healthcare organizations operate within regulatory frameworks mandating specific privacy protections while creating communication obligations.

7.1 Regulatory Communication Requirements (U.S. HIPAA Focus)

The Health Insurance Portability and Accountability Act (HIPAA) establishes privacy protections through three safeguard categories: administrative safeguards (security officer designation, contingency planning, audit procedures), physical safeguards (access controls to facilities and equipment), and technical safeguards (network security, encryption, authentication) (Keshta & Odeh, 2021). While these safeguards focus primarily on protection rather than communication, HIPAA also creates notification obligations establishing baseline communication requirements.

The HITECH Act expanded breach notification requirements, mandating that covered entities notify affected individuals, the Secretary of Health and Human Services, and (for breaches affecting 500 or more individuals) prominent media outlets (Keshta & Odeh, 2021). HITECH establishes breach-notification requirements, including timeliness expectations and minimum content elements for notices to affected individuals.

These regulatory requirements establish minimum communication standards but do not address communication quality, timing optimization, or trust repair strategy. Organizations may satisfy regulatory notification while failing to maintain stakeholder relationships—technically compliant communication perceived as evasive, delayed, or insufficiently empathetic.

7.2 Visual Documentation and Consent Communication

The protection of patient privacy in clinical photographs, video recordings, and detailed case descriptions requires specific governance attention. Visual documentation presents heightened privacy concerns because facial images and distinguishing physical features resist conventional anonymization techniques (Robinson et al., 2014). Governance frameworks must address:

Consent Communication: Patients must receive clear explanation of permissible uses for visual documentation, including clinical care, education, research, and publication purposes. Consent processes should acknowledge power dynamics in clinical relationships that may cause patients to agree despite reservations (Robinson et al., 2014).

Access Restriction: Technical and administrative controls must restrict image access to authorized clinical staff with legitimate need. Watermarking mechanisms can deter unauthorized distribution while supporting accountability (Robinson et al., 2014).

Withdrawal Rights: Patients should understand their right to withdraw consent or request destruction of images not serving legitimate clinical purposes. Healthcare CRM systems incorporating multimedia capabilities must support these rights operationally (Robinson et al., 2014).

7.3 Algorithmic Governance and Bias Communication

Healthcare CRM systems increasingly incorporate algorithmic decision support for patient risk stratification, resource allocation, and care pathway recommendations. Governance frameworks must address the documented risk of algorithmic bias perpetuating healthcare disparities (Obermeyer et al., 2019).

Bias Testing Requirements: Clinical decision support algorithms require robust testing examining differential performance across demographic groups before deployment and through ongoing monitoring (Obermeyer et al., 2019).

Transparency About Algorithmic Decisions: Patients affected by algorithmic recommendations deserve understandable explanation of how decisions were reached and what factors influenced outcomes.

Accountability Structures: Interdisciplinary governance bodies integrating technical expertise, clinical knowledge, bioethical analysis, and community representation should oversee algorithmic systems affecting patient care (Obermeyer et al., 2019).

7.4 Communication Governance Triggers

Effective privacy communication governance establishes clear triggers for communication activities:

Routine Transparency Triggers: Patient onboarding should include explanation of data handling practices, access policies, and patient rights. Care episode conclusion should include a summary of information accessed and created. Annual privacy notices should be supplemented with accessible explanations rather than serving only regulatory compliance functions.

Incident Investigation Triggers: Anomaly detection alerts should initiate investigation protocols with defined timelines. Break-glass usage should trigger supervisory review within 24 hours with communication decisions within a defined timeframe. Confirmed unauthorized access should escalate to the incident response team with communication authority.

Breach Notification Triggers: Confirmed breaches meeting regulatory thresholds should initiate notification preparation immediately. Communication should be staged: internal coordination first, then regulatory notification, then affected individual notification, then public communication if required.

7.5 Organizational Coordination Requirements

Privacy incidents require coordination across organizational functions with different priorities and expertise:

Legal Counsel focuses on liability minimization, regulatory compliance, and privilege protection. Legal involvement shapes communication by establishing what can and cannot be said, particularly regarding fault admission.

Compliance Officers focus on regulatory requirement satisfaction and documentation. Compliance involvement ensures notification timelines are met and required content elements are included.

Clinical Operations focuses on care continuity and provider communication. Clinical involvement ensures affected patients continue receiving appropriate care and that clinical staff understand how to address patient questions.

Communications/Public Relations focuses on stakeholder relationships, media management, and message consistency. Communication involvement shapes tone, channel selection, and messaging strategy.

Information Security focuses on technical investigation, containment, and remediation. Security involvement provides a factual foundation for communication content.

CERC's best practices emphasize that communication should be integrated into decision-making processes rather than treated as an implementation function after decisions are made (Seeger, 2006). Organizations involving communication expertise in incident investigation and response planning develop more effective messaging than those treating communication as a final-stage activity.

8. Communication Practices for Privacy Incidents

This section applies crisis communication theory to healthcare privacy contexts, providing guidance for communication practices across incident phases.

8.1 Pre-Incident Communication: Building Trust Reserves

SCCT identifies prior relational reputation as an intensifying factor affecting crisis response (Coombs, 2007). Organizations with established trust relationships possess reputational capital, providing a buffer during incidents. Pre-incident communication builds this capital through:

Policy Transparency: Privacy policies should be accessible, understandable, and honest rather than merely compliant. Research demonstrates that privacy policies often suffer from deficiencies in clarity, completeness, and accessibility, with many platforms failing to disclose data collection scope, retention periods, third-party sharing, and user rights (LaMonica et al., 2021). Healthcare CRM implementations should remedy these deficiencies through privacy frameworks clearly stating data governance principles, specifying protection mechanisms, explaining disclosure conditions, and providing accessible channels for exercising privacy rights (Huckvale et al., 2015; LaMonica et al., 2021).

Access Explanation: Patients should understand who may access their records, under what circumstances, and for what purposes before incidents occur. When patients understand routine access patterns, they are better positioned to evaluate incident communications and less likely to perceive normal operations as suspicious.

Rights Communication: Patient rights regarding access, correction, and restriction should be clearly communicated and easily exercised. Organizations demonstrating respect for patient autonomy build trust, supporting relationship maintenance during difficult communications.

8.2 Initial Incident Communication: Addressing Uncertainty

CERC emphasizes that initial crisis communication should address stakeholder uncertainty by establishing what is known, acknowledging what remains unknown, and providing self-efficacy information enabling protective action (Reynolds & Seeger, 2005). For privacy incidents:

Timely Acknowledgment: Communication should occur as rapidly as feasible once incident scope is sufficiently understood to enable meaningful notification. Seeger's (2006) best practices emphasize that accepting uncertainty is preferable to delaying communication until complete information is available. Initial statements should acknowledge the incident, describe what is currently known, and commit to ongoing communication as the investigation proceeds. Within the PAC Framework, initial-event messaging quality is constrained by the availability of credible audit evidence (Technical Controls), the clarity of escalation and approval pathways (Governance), and pre-established channel readiness (Communication Practices).

Empathetic Tone: Reynolds and Seeger (2005) emphasize that crisis communication should begin by addressing stakeholder emotional needs. Privacy incidents create anxiety about invisible exposure with uncertain consequences. Initial communication should acknowledge patient concerns, express genuine organizational concern about the incident, and demonstrate that patient welfare is prioritized.

Self-Efficacy Information: Patients need actionable guidance about protective steps: monitoring accounts for suspicious activity, considering credit freezes, and watching for phishing attempts leveraging disclosed information. CERC emphasizes that messages of self-efficacy help restore control in uncertain situations (Reynolds & Seeger, 2005), reducing anxiety by enabling purposeful action.

Uncertainty Acknowledgment: Seeger's (2006) best practices advise accepting uncertainty rather than making overconfident statements that may prove inaccurate as investigation proceeds. Jong (2025) emphasizes that initial crisis responses should leave room for adaptation as circumstances evolve. Statements such as "our investigation is ongoing, and we will provide additional information as it becomes available" maintain credibility across evolving understanding.

8.3 Maintenance Phase Communication: Ongoing Updates

As incidents unfold and investigations proceed, organizations must maintain communication momentum:

Regular Updates: Even when the investigation status has not changed significantly, scheduled updates reassure stakeholders that the organization remains engaged. CERC's maintenance phase emphasizes ongoing uncertainty reduction and correction of misunderstandings (Reynolds & Seeger, 2005).

Fact Correction: Initial communications may require correction as investigations reveal additional information. Acknowledging and correcting errors directly is preferable to allowing inaccurate perceptions

to persist. Seeger's (2006) best practices emphasize honesty and openness, requiring acknowledgment when earlier statements were incomplete or inaccurate.
Scope Refinement: Initial incident scope estimates often require adjustment. Communication should explain methodology used to determine affected records and acknowledge limitations in scope determination.

8.4 Resolution Phase Communication: Trust Repair

Resolution phase communication connects to SCCT response strategies (Coombs, 2007):
For victim-framed incidents (external attacks despite appropriate security): Communication emphasizes organizational victimhood while demonstrating robust response. Bolstering strategies remind stakeholders of organizational security investments and record. Victim strategies note that the organization suffered alongside patients.
For accidental-framed incidents (technical failures without negligence): Communication acknowledges the incident while emphasizing the lack of intent and limited organizational control. Excuse strategies note circumstances beyond organizational control. Justification strategies contextualize incident severity relative to potentially worse outcomes.
For preventable-framed incidents (negligence, inadequate security, ignored warnings): Communication accepts organizational responsibility and emphasizes corrective action. Apology strategies take full responsibility and request forgiveness. Compensation strategies offer concrete remediation including credit monitoring, enhanced protections, and policy changes.
Research demonstrates that more accommodative strategies than the situation requires provide no additional reputational benefit and may worsen perceptions by suggesting the crisis is more severe than stakeholders believed (Coombs, 2007). Matching response strategy to appropriate crisis type requires accurate assessment of how stakeholders perceive organizational responsibility—a dynamic determination that may shift as information emerges (Jong, 2025).

8.5 Channel Strategy

Privacy incident communication must reach affected stakeholders through appropriate channels:
Written Notification (Mail/Email): Required for regulatory compliance; provides documentation; allows detailed information; may seem impersonal for serious incidents; email may be missed or filtered.
Patient Portal Notifications: Persistent availability for patient review; supports documentation; reaches engaged patients; may miss patients who do not regularly access portals.
Direct Telephone Contact: Personal touch appropriate for serious incidents or vulnerable populations; resource-intensive; documentation challenges; patients may not answer unknown numbers.
In-Person Communication: Highest trust potential; appropriate for ongoing care relationships; allows immediate question answering; limited scalability; requires provider preparation.
Public Announcements (Media/Website): Required for large breaches; demonstrates transparency; reaches broad audiences; risk of media framing distortion; less personalized.
CERC notes that crisis messages often take advantage of whatever communication channel is available (Reynolds & Seeger, 2005), but strategic channel selection based on incident severity, affected population characteristics, and relationship context improves communication effectiveness.

9. Discussion: Crisis Communication Implications

9.1 Trust Repair Strategies

Healthcare privacy incidents threaten the trust foundation underlying effective patient-provider relationships. SCCT provides evidence-based guidance for trust repair, but healthcare contexts present distinctive challenges:
Attribution Complexity: Privacy incidents often involve multiple potential responsible parties—the healthcare organization, technology vendors, individual employees, external attackers. Stakeholder attributions may be unstable, shifting as investigation reveals additional information about cause and

contributing factors (Jong, 2025). Organizations should anticipate attribution dynamics rather than committing to responsibility framings that may prove inconsistent with subsequent findings.

Invisible Harm: Unlike industrial accidents with visible damage, privacy incidents involve information exposure whose consequences may be delayed, indirect, and variably significant. Trust repair must address anxiety about uncertain future harm, not merely demonstrated past damage.

Ongoing Relationship Context: Healthcare relationships continue after incidents—patients may need ongoing care from the same organization. Trust repair must support relationship continuation, not merely organizational reputation protection.

9.2 Dynamic Perceptions and Adaptive Response

Jong (2025) challenges static interpretations of crisis communication theory, demonstrating that perceptions of crisis responsibility shift as new information emerges about causes and as multiple actors' relative responsibilities become clearer. Healthcare privacy incidents frequently involve evolving understanding:

- Initial reports may underestimate scope; subsequent investigation may reveal broader exposure
- External attack attribution may shift to organizational negligence if inadequate security is discovered
- Single-actor incidents may become multi-actor as vendor or partner involvement emerges
- Technical failure attribution may shift to human error as investigation proceeds

Organizations should craft initial communications leaving room for adaptation rather than making commitments constraining future messaging. Jong (2025) notes that statements like "feeling responsible" allow subsequent refinement of responsibility attribution, while "being responsible" creates binary commitment that may prove inconsistent with investigation findings.

9.3 Emerging Technology Communication Challenges

Emerging privacy technologies introduce new communication considerations:

Artificial Intelligence Monitoring: AI-based anomaly detection enables proactive incident identification but creates uncertainty messaging challenges. False positives may trigger unnecessary patient communications eroding confidence. Algorithmic explanations may be difficult to translate into stakeholder-appropriate language. AI bias in monitoring may create inequitable incident detection across patient populations, raising concerns documented in broader algorithmic bias research (Obermeyer et al., 2019).

Blockchain Audit Trails: Distributed ledger technology provides tamper-resistant documentation supporting accountability claims. However, blockchain's technical complexity complicates patient explanation. Claims of immutable audit trails require accessible translation to support credibility rather than mystification.

Differential Privacy Analytics: Mathematical privacy guarantees enable population health research while protecting individual records. Communicating privacy guarantees to lay audiences presents significant challenges—mathematical formulations providing meaningful protection may not provide meaningful reassurance without translation.

Homomorphic Encryption: Computation on encrypted data addresses some fundamental privacy-access tensions but introduces performance limitations and implementation complexity. Organizations may struggle to communicate why certain operations are possible while others require plaintext access.

These technologies offer genuine privacy enhancements but require communication strategies translating technical capabilities into stakeholder-meaningful terms. Technical sophistication that cannot be explained may undermine rather than support trust.

9.4 Organizational Learning and Improvement

CERC's evaluation phase emphasizes documenting lessons learned and communicating improvements (Reynolds & Seeger, 2005). Privacy incidents provide organizational learning opportunities that should be captured and communicated:

Root Cause Analysis: Beyond immediate incident response, organizations should analyze systemic factors contributing to incidents and communicate findings to relevant stakeholders.
Policy and Procedure Updates: Changes implemented in response to incidents should be communicated to demonstrate organizational learning and improvement commitment.
Training Enhancement: Staff training improvements addressing incident contributing factors demonstrate organizational commitment to prevention.
Technology Investment: Security technology enhancements made in response to incidents support organizational credibility when communicated appropriately.

10. Implications for Practice

10.1 Communication Playbook Components

Healthcare organizations should develop privacy incident communication playbooks, preparing for incidents before they occur:
Pre-Approved Message Templates: Draft notification templates reviewed by legal, compliance, and communications functions enable rapid response without real-time approval delays. Templates should include placeholder elements for incident-specific details while establishing tone, structure, and required content elements.
Spokesperson Identification and Training: Designated spokespersons should be identified and trained before incidents occur. Training should address media interaction, patient communication, and message consistency maintenance under pressure. Seeger (2006) emphasizes that media training should be completed prior to crisis onset.
Channel Selection Decision Trees: Pre-established criteria for channel selection based on incident characteristics (severity, scope, affected population) enable rapid communication decisions.
Coordination Protocols: Clear escalation pathways and coordination procedures among legal, compliance, clinical, communications, and security functions prevent delays and inconsistencies.

10.2 Message Components

Effective privacy incident notifications should include:
What Happened: Factual description of incident circumstances at an appropriate detail level. Avoid technical jargon; provide an accessible explanation.
What Information Was Involved: Specific identification of data categories potentially affected. Distinguish between accessed and exfiltrated data where possible.
What the Organization Is Doing: Concrete actions taken to investigate, contain, and remediate. Include timeline commitments where feasible.
What Patients Can Do: Actionable self-efficacy guidance. Credit monitoring instructions, account monitoring recommendations, and phishing awareness.
Contact Information: Clear channels for patient questions. Dedicated hotline for significant incidents. Email, phone, and in-person options.
Ongoing Communication Commitment: Commitment to provide updates as the investigation proceeds. Scheduled communication, if possible.
Messages should avoid:

- Technical jargon without explanation
- Defensive or blame-shifting language
- Minimizing language contradicting the patient experience
- Overconfident statements that may require correction
- Vague timeline commitments that cannot be satisfied

10.3 Evaluation Checklist

Organizations can assess communication readiness using the following checklist:

Pre-Incident Preparedness:

- Privacy policies accessible and understandable to patients

- Patient rights are clearly communicated and easily exercised
- Staff trained on privacy communication responsibilities
- Incident communication playbook developed and tested
- Spokesperson identified and media-trained
- Coordination protocols established among organizational functions

Technical Control Communication Integration:

- Audit logging is sufficient to support incident communication needs
- The patient portal enables patients to review audit/access logs and understand record access history
- Break-glass protocols include communication triggers
- Anomaly detection integrated with communication escalation

Incident Response Capability:

- Notification templates pre-approved and ready for customization
- Multiple communication channels available and tested
- Regulatory notification procedures established
- Media communication protocols defined
- Patient support resources identified (hotline, FAQ, counseling)

Post-Incident Learning:

- Root cause analysis procedures established
- Lesson documentation and sharing protocols defined
- Policy update and communication procedures are documented, version-controlled, and communicated to relevant stakeholder groups
- Training enhancement processes defined

Table 4. Privacy Incident Communication Readiness Checklist (Reynolds & Seeger, 2005; Seeger, 2006).

Readiness Dimension	Key Indicators of Preparedness	Common Gaps to Address
Policy Foundation	Plain-language privacy policies; multiple formats available; patient comprehension verified	Technical jargon; inaccessible formats; incomplete disclosure
Technical Infrastructure	Patient-facing access portals; detailed audit logging; anomaly detection with escalation	Limited logging; no patient visibility; manual review only
Response Protocols	Tested playbooks; regular drills; trained spokespersons; pre-approved templates	Ad hoc response; unclear authority; untrained spokespersons
Coordination Mechanisms	Cross-functional protocols; clear decision authority; communication approval workflows	Siloed functions; approval delays; inconsistent messaging
Stakeholder Channels	Verified contact information; multiple tested channels; accessibility accommodations	Outdated contacts; single-channel reliance; accessibility gaps

11. Limitations and Future Research

11.1 Limitations

This paper's framework development is conceptual rather than empirical. While the PAC Framework draws on established crisis communication theory and healthcare privacy scholarship, the specific propositions connecting technical controls to communication outcomes require empirical validation. The framework has not been tested through observation of actual privacy incident responses or measurement of trust outcomes following different communication approaches.

The analysis focuses primarily on U.S. regulatory context (HIPAA/HITECH). Healthcare privacy regulations vary significantly across jurisdictions, and communication requirements, cultural expectations, and trust dynamics may differ in non-U.S. contexts. Comparative analysis of national electronic health record architectures suggests significant variation in how different countries balance privacy protection and data accessibility (Gunter & Terry, 2005), indicating that framework applicability across regulatory regimes requires assessment.

The integrative literature review methodology, while appropriate for framework development, does not provide systematic evidence synthesis. Relevant literature may have been missed, and weighting of evidence across sources reflects authorial judgment rather than formal quality assessment. As with many integrative reviews, database coverage and publication bias may skew available evidence toward well-documented incidents and more frequently studied settings, potentially underrepresenting smaller organizations and non-U.S. contexts.

The framework addresses organizational communication but does not fully develop individual-level factors affecting patient reception of privacy communications. Patient health literacy, prior trust levels, personal privacy sensitivity, and incident characteristics all likely moderate communication effectiveness in ways not fully captured.

11.2 Future Research Directions

Several research directions would advance understanding of healthcare privacy crisis communication:

Empirical Trust Outcome Studies: Research measuring patient trust levels before and after privacy incidents, comparing outcomes across different communication approaches, would provide evidence for framework propositions. Longitudinal designs capturing trust trajectories over time would be particularly valuable.

Message Framing Experiments: Experimental research testing different notification message frames—varying in responsibility acknowledgment, technical detail, empathy expression, and self-efficacy guidance—would identify effective communication elements.

Channel Effectiveness Evaluation: Research comparing patient outcomes across different communication channels would inform channel selection guidance. This could include comprehension testing, anxiety measurement, and protective action adoption.

Timing Studies: Research examining effects of notification timing—comparing rapid notification with incomplete information versus delayed notification with complete information—would address a persistent practitioner dilemma.

Cross-Cultural Comparison: Research comparing privacy communication expectations and trust dynamics across cultures would extend framework applicability beyond the U.S. context.

Algorithmic Transparency Communication: Given documented concerns about algorithmic bias in healthcare (Obermeyer et al., 2019), research examining effective communication strategies for explaining algorithmic decisions to patients would address an emerging challenge.

Conclusion

Privacy incidents in healthcare CRM systems create crises demanding both technical response and communication response. This paper developed the Privacy-Access-Communication (PAC) Framework to integrate these dimensions, connecting technical privacy controls to communication practices through Situational Crisis Communication Theory and Crisis and Emergency Risk Communication principles.

The framework makes three contributions. First, it provides a theoretically grounded structure integrating technical controls, governance structures, and communication practices into a coherent system for healthcare privacy management. By connecting mechanisms such as attribute-based access control, audit logging, and break-glass protocols to their communication implications, the framework enables

organizations to anticipate communication needs based on system design choices. Second, it identifies communication patterns linking access control mechanisms to stakeholder messaging strategies. Technical controls not only protect information but also enable or constrain communication options during incidents—audit logs provide evidentiary foundations for notification, while break-glass protocols create explanation challenges requiring careful management. Third, it offers an evaluation checklist enabling practitioners to assess organizational communication readiness, operationalizing crisis communication best practices for healthcare privacy contexts.

The theoretical grounding in Situational Crisis Communication Theory guides matching communication responses to stakeholder attributions of organizational responsibility, whether incidents are perceived as victim, accidental, or preventable crises. Crisis and Emergency Risk Communication principles emphasize that communication needs evolve across phases—from pre-crisis trust building through initial uncertainty reduction to resolution-phase trust repair.

The framework acknowledges limitations requiring future research, including empirical validation of propositions connecting technical controls to communication outcomes and assessment of applicability across different regulatory contexts. Future directions include studies measuring patient trust trajectories following incidents, experimental research on message framing effectiveness, and evaluation of channel and timing strategies.

The PAC Framework provides healthcare organizations with a systematic approach to building and maintaining trust through integrated attention to technical controls, governance structures, and communication practices. By bridging health information technology and crisis communication scholarship, this paper advances understanding of privacy management as a fundamentally communicative endeavor requiring sustained attention to transparency, accountability, and relationship maintenance.

References

1. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: Preserving security and privacy. Journal of Big Data, 5, Article 1. https://doi.org/10.1186/s40537-017-0110-7
2. Alhammad, N., Alajlani, M., & Abudawood, A. A. (2024). Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: Systematic review. Journal of Medical Internet Research, 26(1), e50715. https://doi.org/10.2196/50715
3. Brennan, P. F., Downs, S., & Casper, G. (2010). Project HealthDesign: Rethinking the power and potential of personal health records. Journal of Biomedical Informatics, 43(5 Suppl), S3–S5. https://doi.org/10.1016/j.jbi.2010.09.001
4. Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049
5. Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. Journal of Medical Internet Research, 7(1), e3. https://doi.org/10.2196/jmir.7.1.e3
6. Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P.-J., & Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. BMC Medicine, 13, Article 214. https://doi.org/10.1186/s12916-015-0444-y
7. Jong, W. (2025). Beyond the snapshot: Rethinking crisis communication theories in dynamic crisis situations. Public Relations Review, 51, Article 102586. https://doi.org/10.1016/j.pubrev.2025.102586
8. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003
9. LaMonica, H. M., Roberts, A. E., Lee, G. Y., Davenport, T. A., & Hickie, I. B. (2021). Privacy practices of health information technologies: Privacy policy risk assessment study and proposed guidelines. Journal of Medical Internet Research, 23(9), e26317. https://doi.org/10.2196/26317

10. Mandl, K. D., & Kohane, I. S. (2012). Escaping the EHR trap—The future of health IT. The New England Journal of Medicine, 366(24), 2240–2242. https://doi.org/10.1056/NEJMp1203102
11. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453. https://doi.org/10.1126/science.aax2342
12. Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. Journal of Health Communication, 10(1), 43–55. https://doi.org/10.1080/10810730590904571
13. Robinson, J. K., Bhatia, A. C., & Callen, J. P. (2014). Protection of patients' right to privacy in clinical photographs, video, and detailed case descriptions. JAMA Dermatology, 150(1), 14–16. https://doi.org/10.1001/jamadermatol.2013.8605
14. Seeger, M. W. (2006). Best practices in crisis communication: An expert panel process. Journal of Applied Communication Research, 34(3), 232–244. https://doi.org/10.1080/00909880600769944
15. Wukich, C. (2016). Government social media messages across disaster phases. Journal of Contingencies and Crisis Management, 24(4), 230–243. https://doi.org/10.1111/1468-5973.12119