Saudi Journal of Medicine and Public Health

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

https://doi.org/10.64483/202412730

Cybersecurity of Electronic Health Records: Implications for Nursing Practice, Dental Services, and Patient Safety

Abdu Bakri Hassan Sumayli[(1)] , Ahmed Mohammed Nasser Someli[(2)] , Mohammed Ibrahim Ali Hakami[(3)] , Fatimah Mohammed Ibrahim Hakami[(4)] ,Aisha Ali Ail Hakamy[(5)] ,Moudhi Alsaif[(6)] , Mashael Waslallah Al-Otibi[(7)] , Fadwa Mahmoud Kamel Jawda[(8)] , Tahani Suliman Alzeed[(9)] , Sara Hamdan Al Fahhad[(8)] , Hissah Abdulaziz Alyahya[(10)] , Ebtihaj Metab Mohsen Mutairi[(11)]

(1)Al-Tawal General Hospital, Ministry of Health, Saudi Arabia
(2)Umm Al-Shanoun Primary Health Care Center, Samtah Sector, Jazan,Ministry of Health , Saudi Arabia
(3)Erada Hospital for Mental Health in Jazan, Ministry of Health, Saudi Arabia
(4)Al-Qa'ariyah Primary Health Care Center - Jazan Health Cluster, Ministry of Health, Saudi Arabia
(5)Jazan - Al-Ardah Hospital, Ministry of Health, Saudi Arabia
(6)King Salman Hospital, Riyadh, Ministry of Health, Saudi Arabia
(7)Al-Ardah Complex for Mental Health and Addiction – Riyadh, The Third Health Cluster,Ministry of Health , Saudi Arabia
(8)Erada Complex for Mental Health, Riyadh, Ministry of Health, Saudi Arabia
(9)Erada Complex for Mental Health, Ministry of Health, Saudi Arabia
(10)Third Health Cluster, Erada Complex,Ministry of Health , Saudi Arabia
(11)Al-Barzeh Primary Health Care Center,Ministry of Health , Saudi Arabia

Abstract

Background: The digital transformation of healthcare through Electronic Health Records (EHRs) has revolutionized clinical data management but simultaneously exposed the sector to escalating cybersecurity threats. **Aim:** This narrative review aims to synthesize recent evidence on the nature, frequency, and impact of cybersecurity threats to EHRs, with a specific focus on the clinical and operational implications for nursing practice and dental services. **Methods:** A structured literature review was conducted, analyzing peer-reviewed articles, governmental reports, and industry white papers published predominantly between 2015 and 2024. Databases including PubMed, CINAHL, and IEEE Xplore were searched using keywords related to EHR cybersecurity, data breaches, ransomware, and clinical practice. **Results:** Findings reveal a surge in sophisticated cyberattacks, notably ransomware, leading to significant data breaches, operational downtime, and financial losses. The clinical implications are profound, manifesting as workflow disruptions, clinician burnout, and increased patient safety risks due to diagnostic and treatment delays. The review identifies critical vulnerabilities in both hospital and dental practice settings, ranging from human factors to legacy system deficiencies. **Conclusion:** Cybersecurity is an emergent patient safety imperative, not merely a technical concern. A paradigm shift towards a resilient culture of security, encompassing robust technological safeguards, continuous interdisciplinary education, and clear regulatory compliance, is essential to mitigate these evolving threats and ensure continuity of safe, high-quality care.

Keywords: Electronic Health Records, cybersecurity, nursing informatics, dental informatics, patient safety.

Introduction

The integration of Electronic Health Records (EHRs) into the fabric of modern healthcare represents one of the most significant paradigm shifts in medical history. Transitioning from paper-based silos to interconnected digital ecosystems has yielded undeniable benefits, including enhanced clinical decision support, improved care coordination, and greater patient engagement (Kruse et al., 2018). However, this digital transformation is a double-edged sword. The very features that make EHRs invaluable—centralized data repositories, network connectivity, and interoperability—also render them a prime target for malicious cyber actors. The healthcare sector now finds itself in an adversarial landscape where the confidentiality, integrity, and availability of digital health information are under constant, sophisticated attack.

The escalating frequency and severity of cyberattacks on healthcare infrastructure have transformed cybersecurity from a niche technical issue into a core enterprise risk management and patient safety crisis. A single successful ransomware attack can cripple a hospital network for weeks, forcing the cancellation of surgeries, diverting emergency patients, and reverting clinicians to cumbersome paper-based systems (Slayton, 2018; Triplett, 2022). The implications cascade beyond operational disruption, directly corroding the trust that is fundamental to the therapeutic relationship. When

*Corresponding author absayli@moh.gov.sa (Abdu Bakri Hassan Sumayli).
Receive Date: 22 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

patients hesitate to share sensitive information for fear of exposure, the diagnostic process is fundamentally compromised (Khan, 2023).

This narrative review is structured to provide a comprehensive and clinically grounded synthesis of the cybersecurity challenges facing EHR systems, with a deliberate and specific focus on the implications for nursing practice and dental services. While the entire clinical ecosystem is affected, these two disciplines represent the largest segment of the healthcare workforce and a uniquely vulnerable small-business model, respectively. They are often the first and last lines of defense in the clinical data lifecycle, yet their specific perspectives are frequently underrepresented in cybersecurity discourse. This review aims to bridge that gap by exploring the nature of contemporary threats—from data breaches and privacy erosion to crippling ransomware—and, more importantly, by analyzing their tangible consequences on clinical workflows, professional morale, and patient safety outcomes. Through a critical synthesis of literature from 2015 to 2024, this paper will argue that cybersecurity is not merely an information technology (IT) department responsibility but an emergent clinical competency and a fundamental pillar of patient-centered care. Finally, it will propose a multi-layered framework of technological, educational, and policy-driven strategies to cultivate a resilient culture of security across diverse healthcare settings.

Methods

This study employed a narrative review methodology to allow for a broad and integrative synthesis of a complex, multi-disciplinary topic that spans technical, clinical, and behavioral sciences. Unlike a systematic review, this approach is suited for interpreting a body of literature that is heterogeneous in study design and methodology, with the aim of generating new conceptual insights and identifying practical implications (Green et al., 2006). The review was guided by a structured search strategy to ensure rigor and replicability.

A comprehensive literature search was conducted across four electronic databases: PubMed (biomedical and clinical sciences), CINAHL (nursing and allied health), IEEE Xplore (engineering and cybersecurity technology), and Scopus (multi-disciplinary). The search employed a combination of controlled vocabulary terms and keywords in three conceptual blocks. The first block targeted the technology of interest: “Electronic Health Records,” “EHR,” “Electronic Dental Records,” “EDR,” “Hospital Information Systems.” The second block defined the threat landscape: “Computer Security,” “Data Breach,” “Ransomware,” “Phishing,” “Malware,” “Privacy,” “HIPAA.” The third block focused on clinical implications: “Patient Safety,” “Nursing Practice,” “Dental Practice,” “Workflow,” “Clinical Errors,” “Burnout.” Boolean operators (AND, OR) were used to combine terms within and between blocks.

The inclusion criteria were: (a) peer-reviewed articles, government reports, and authoritative industry white papers; (b) published in English between January 2015 and April 2024; (c) primary focus on cybersecurity threats to digital health records and their downstream effects on clinical care delivery, particularly in nursing and dentistry. Exclusion criteria comprised: editorials, commentaries, and non-peer-reviewed opinion pieces; studies focused exclusively on medical device security without an EHR component; and research on cybersecurity awareness among non-clinical staff. The search was supplemented by a manual review of reference lists from key articles to identify seminal works not captured by the initial database query. The initial search yielded over 1,400 potentially relevant records. After removing duplicates, 850 abstracts were screened, and 220 full-text articles were assessed for eligibility. The final synthesis for this review draws upon 37 core sources that provided the most direct and robust evidence on the clinical implications of EHR cybersecurity, with a deliberate selection of recent publications (post-2020) to reflect the rapidly evolving threat landscape. Thematic analysis was used to synthesize findings into the narrative structure that follows, organizing data into domains of threats, technological controls, and discipline-specific clinical impacts.

The Evolving Threat Landscape: From Data Breaches to Ransomware

The cyber threat landscape targeting healthcare has undergone a profound evolution, shifting from incidental data theft by opportunistic individuals to a mature, industrialized ecosystem of organized crime and nation-state-sponsored espionage. The Health Insurance Portability and Accountability Act (HIPAA) Breach Reporting Tool consistently shows a year-over-year increase in major health data breaches, with 2023 marking a record high (US Department of Health and Human Services, 2019; Yeo & Banfield, 2022). Understanding the distinct types of threats is foundational to appreciating their differential clinical impacts.

Data Breaches and Privacy Erosion

Data breaches, defined as unauthorized access, use, or disclosure of protected health information (PHI), remain the most common form of cyber incident. They can be categorized into “hacking/IT incidents,” which are external and malicious, and “unauthorized access/disclosures,” which often involve internal actors or simple human error (Wikina, 2014). A large-scale analysis by Bai et al. (2017) found that nearly 70% of hospital data breaches involved sensitive demographic or financial information that could lead to medical identity theft, a crime in which a victim's identity is used to obtain medical services or prescription drugs. The consequence for the patient extends beyond financial

harm; the corruption of their medical record with another person's clinical data—wrong blood type, allergies, or diagnoses—can create lethal clinical decision-making traps (Sulmasy et al., 2017).

The privacy harm is equally corrosive. When a patient's deeply personal health information—mental health records, HIV status, genetic predispositions—is exposed, it inflicts a psychological trauma that can shatter trust in the healthcare system. Khan (2023) frame this as a betrayal of the Hippocratic oath in the digital age, demonstrating that patients aware of breaches at their provider are significantly more likely to withhold information from their clinicians or even avoid care altogether. For nurses, who are the primary custodians of sensitive patient data at the bedside, this erosion of trust manifests as a direct barrier to therapeutic communication. A patient may refuse to answer a critical psychosocial screening question, not because they are non-adherent, but because they fear the data will not be kept secure (Kim et al., 2022). This chilling effect transforms a cybersecurity failure into an antecedent of suboptimal clinical outcomes.

The Ransomware Epidemic

While data theft undermines confidentiality, ransomware destroys availability—and in healthcare, data availability is synonymous with life-saving care. Ransomware is a type of malware that encrypts files and systems, rendering them unusable until a ransom, typically in cryptocurrency, is paid. The healthcare sector has become the primary target for ransomware gangs because the high-stakes nature of clinical operations makes downtime intolerable and the likelihood of payment higher (Neprash et al., 2022). The 2017 WannaCry attack, which crippled the UK's National Health Service, was a global wake-up call, demonstrating how an indiscriminate cyber weapon could cause regional-scale healthcare disruption, cancelling an estimated 19,000 appointments and costing £92 million (Ghafur et al., 2019).

The ransomware-as-a-service (RaaS) model has since professionalized these attacks, with sophisticated criminal syndicates like Conti, REvil, and BlackCat targeting large hospital chains and integrated delivery networks. A study by Dameff et al. (2023) of a community hospital's ransomware attack documented a near-total cessation of electronic operations for over two weeks. The immediate consequence was a perilous transition to paper-only workflows: medication administration records went from barcode-scanned safety systems to handwritten logs; radiology was reduced to X-ray films viewed on lightboxes without digital comparison; and laboratory results were phoned to units, often with critical delays. The study quantified a significant increase in near-miss events and a subjective sense of chaos among staff, linking the cyberattack directly to a degradation in the standard of care. Financially, the cost of remediation, system restoration, reputational damage, and litigation far exceeds the ransom demand itself. The Ponemon Institute's (2022) annual report pegged the average total cost of a healthcare data breach at over $10 million, the highest of any industry for the 12th consecutive year. The true "ransom," however, is paid in patient outcomes when timely, data-driven care is catastrophically interrupted.

Insider Threats and Human Factors

The firewall is not always the point of failure; often, it is the human behind the keyboard. Insider threats, both malicious and unintentional, account for a significant portion of security incidents (Hassandoust et al., 2021). The malicious insider—a disgruntled employee who sells PHI for profit or snoops on a celebrity's record—represents a direct abuse of privileged access. However, the far more pervasive threat is the unwitting insider who falls victim to social engineering. Phishing, a tactic where attackers send deceptive emails to trick users into revealing credentials or installing malware, remains the primary attack vector for initiating a ransomware deployment or data exfiltration (Gordon et al., 2019).

The healthcare environment is uniquely susceptible to phishing. Clinicians, particularly nurses in fast-paced acute care settings, are conditioned to respond rapidly to information. An email that appears to be an urgent patient update, a drug recall notice from the pharmacy, or a COVID-19 protocol change from management exploits this instinct to prioritize clinical urgency over security scepticism (Priestman et al., 2019). A cleverly crafted, context-aware "spear-phishing" email can have a click rate as high as 30% among busy clinical staff. The consequence of a single click can be the compromise of an entire hospital network. This is not a failure of policy but a collision between the culture of clinical efficiency and the culture of cyber vigilance—a collision that requires a fundamentally different educational approach than the typical, compliance-driven annual training module.

Technological Safeguards for Secure EHR Systems

Defending EHR systems against this complex threat landscape necessitates a defense-in-depth strategy, where multiple, overlapping security controls compensate for the failure of any single layer. This is not a problem solved by a single silver-bullet technology but by a coherent architecture of safeguards spanning data, network, and endpoint (Table 1).

Encryption, Access Control, and Authentication

Encryption is the last line of defense for data confidentiality. When properly implemented, it renders stolen data unreadable gibberish without the decryption key. The HIPAA Security Rule mandates "addressable" implementation specifications for data encryption at rest (on servers and databases) and in transit (across networks) (Cohen & Mello, 2018). While almost all major EHR vendors now offer encryption, a concerning number of healthcare organizations fail to implement it correctly on legacy systems or mobile devices, leaving data in "cleartext." This is a catastrophic failure of basic cyber hygiene.

Equally critical is the principle of least privilege, enforced through robust access controls. Role-Based Access Control (RBAC) assigns permissions based on a person's job function, ensuring a dental hygienist cannot access a patient's psychiatric notes. However, RBAC is often implemented too broadly, granting excessive access that creates an overly permissive data environment. In emergency "break-the-glass" scenarios, where a clinician needs immediate access to a restricted record, the access must be provided instantly but logged exhaustively for retrospective audit. A systematic review by Fernández-Alemán et al. (2013) highlighted that overly restrictive systems can endanger patients, forcing clinicians to work around security, while overly lax systems invite abuse. The future lies in adaptive, context-aware access control, where the system evaluates the user's location, time of day, device security posture, and behavioral biometrics to dynamically adjust authentication requirements (Almas et al., 2023).

Network Segmentation and Endpoint Detection

A flat, unsegmented hospital network is a ransomware operator's dream. Without internal walls, a single compromised device on a nursing unit can propagate encryption laterally to the data center's EHR servers in minutes. Network segmentation creates digital partitions that isolate critical clinical systems, HVAC controls, and guest Wi-Fi networks into separate security zones, with a firewall inspecting traffic between them (Ayala, 2016). For instance, a vulnerability in an Internet of Things (IoT) smart infusion pump should not become a pivot point to attack the EHR.

Endpoint Detection and Response (EDR) systems represent an evolution beyond traditional signature-based antivirus. EDR platforms continuously monitor endpoint devices—nurses' workstations-on-wheels (WOWs), dental office PCs—for behavioral anomalies indicative of an attack, such as a process attempting to encrypt hundreds of files in rapid succession (Hassan et al., 2020). This "behavioral fingerprinting" can detect novel, zero-day malware that no traditional antivirus would recognize. For clinical environments, it is vital that any EDR solution is rigorously tested for performance impact on clinical applications, as a system-induced delay during a medication scan is operationally and clinically unacceptable.

Immutable Backups and Disaster Recovery

Ultimately, the most decisive defense against ransomware is not preventing the attack—an impossible standard—but possessing the ability to recover without paying the ransom. The 3-2-1 backup rule is a foundational principle: maintain at least three copies of data, on two different types of media, with one copy stored off-site and offline or "immutable" (Whitman & Mattord, 2009). An immutable backup cannot be altered or deleted, even by an attacker with administrative credentials. Cloud-based backup services with object locking features now provide this capability, creating a digital "bunker" from which a clean copy of the EHR can be restored. A robust disaster recovery plan, tested through regular, unannounced drills that simulate a total EHR outage, is the operationalization of this technical capability. The recovery point objective (RPO—how much data can be lost) and recovery time objective (RTO—how quickly systems must be restored) must be defined not by IT in a vacuum, but through a clinical impact analysis that translates minutes of downtime into direct patient risk (Sittig & Singh, 2016).

Table 1: Key Cybersecurity Threats, Technological Safeguards, and Primary Clinical Targets

Threat Vector	Description	Key Safeguard(s)	Primary Clinical Target for Disruption
Phishing/Social Engineering	Deceptive emails or messages tricking users into revealing credentials or deploying malware.	AI-powered email filtering, Multi-Factor Authentication (MFA), context-aware security training.	Nursing Workflows, Front-Desk Dental Staff
Ransomware	Malware encrypting files/systems, demanding payment for a decryption key.	Network Segmentation, Endpoint Detection & Response (EDR), Immutable 3-2-1 Backups.	Entire Clinical Operations, Emergency Department, Dental Practice Management
Insider Threat (Unwitting)	Staff accidentally causing a breach through error (e.g., misdirected email, lost device).	Robust Access Controls (RBAC), Data Loss Prevention (DLP) tools, full-disk encryption.	Patient Confidentiality, Privacy Compliance
Insider Threat (Malicious)	Authorized user deliberately accessing/exfiltrating data for personal gain.	User and Entity Behavior Analytics (UEBA), rigorous audit log review, least-privilege policies.	VIP Patient Privacy, Medical Identity Theft
Legacy System Vulnerability	Unpatched or unsupported software (e.g., Windows 7, old database servers).	Rigorous Patch Management, network	Dental Imaging Systems, Specialized Medical Devices linked to EHR

	micro-segmentation, virtual patching.

Clinical Implications for Nursing Practice

Nursing, as the 24/7, bedside-sharp-end of healthcare, is disproportionately affected by EHR cybersecurity failures. The impact is not a theoretical metric on a dashboard; it is a lived, somatic experience of a profession under siege, where the tools designed to create safety and efficiency become vectors of risk and frustration.

Workflow Disruption and Patient Safety Risks During Downtime

When an EHR goes offline due to a ransomware attack or other cyber incident, the clinical environment regresses by decades, but the complexity of contemporary patients—with their polypharmacy, multi-morbidity, and high-tech treatments—remains unchanged. A study by Campbell et al. (2006) on the unintended consequences of EHRs presciently noted that the system's benefits create a deep dependency; remove the system, and you have not just a paper problem but a knowledge and coordination vacuum. In a cyber-induced downtime, the meticulously designed safety net of the EHR—barcode medication administration (BCMA), allergy checking, drug-drug interaction alerts—vanishes instantly.

Nurses are forced into manual, generic processes. Handwritten medication administration records (MARs) must be created from a patient's last known printed chart, which may be hours old. This eliminates the real-time safety checks that prevent the estimated 5-7% of medication errors that BCMA stops in modern systems (Poon et al., 2010). Larsen et al. (2018) documented the near-miss events in a simulated EHR downtime scenario, finding that transcription errors, missed doses, and incorrect infusion rate calculations increased tenfold. Diagnostic results return to being shouted down a phone line or hand-delivered on paper slips, a process prone to miscommunication, illegibility, and failure to follow up on critical values (Alanazi et al., 2023). The cognitive load on the nurse shifts from clinical judgment to logistical survival, creating a fertile ground for error. The concept of "resilience" in this context is perverse; it is nurses heroically bridging a systemic failure with their own cognitive and emotional labor, a strategy that is unsustainable and masks underlying system brittleness (Varpio et al., 2015; Tiongco, 2022).

Burnout, Moral Distress, and the Erosion of Professional Identity

The relationship between poorly designed EHRs and clinician burnout is well-documented (Melnick et al., 2020). Cybersecurity adds a new, corrosive dimension to this relationship. It is not just the inefficiency of a clunky interface but the existential dread that a wrong click could paralyze the entire hospital. This constant state of low-grade hypervigilance, combined with the actual, acute trauma of practicing during an attack, generates a unique form of techno-stress. The phenomenon of "security fatigue," where users become desensitized to constant warnings and alerts, leads to risky workarounds like sharing passwords on a sticky note to expedite patient care (Coventry & Branley, 2018).

More profoundly, cyberattacks trigger moral distress in nurses—the psychological disequilibrium that occurs when one knows the ethically correct action but is institutionally constrained from taking it. A nurse during a ransomware attack knows their patient needs pain relief or a critical antibiotic, but cannot verify the order, the allergy, or administer the drug through a safe, documented process. The resulting sense of failing one's patient, even in circumstances beyond individual control, leaves lasting psychological scars (Rushton et al., 2017). This trauma is a driver of the accelerating exodus from the nursing profession. Cybersecurity is thus not merely a threat to data, but a threat to the very soul of the nursing workforce, transforming a caring profession into one of constant digital risk management.

Specific Implications for Dental Services

Dental practices represent a distinct and uniquely vulnerable node in the healthcare cyber ecosystem. Often structured as small to medium-sized enterprises (SMEs) with limited IT budgets and no dedicated security personnel, they are seen as "soft targets" by cybercriminals (Table 2). The clinical and business model of dentistry presents specific security challenges, particularly regarding digital imaging, patient communication, and practice management (Melon & Hernandez, 2020).

Vulnerabilities in the Dental Practice Management Ecosystem

The centralized core of a modern dental practice is the practice management software (PMS), an integrated suite handling scheduling, billing, charting, digital imaging (radiographs, intraoral photos), and clinical notes. This consolidation creates a high-value, single point of failure. A ransomware attack does not just encrypt billing records; it encrypts the entire clinical archive—every radiograph, treatment plan, and periodontal chart for every patient (Sittig et al., 2020). The business impact is existential; studies show that over 60% of small businesses that suffer a major cyberattack file for bankruptcy within six months (Franco et al., 2022).

The threat vector is overwhelmingly phishing, often targeted at front-desk administrative staff who handle a high volume of external emails from patients, insurers, and suppliers. An email disguised as a new patient inquiry or an insurance remittance carries a malicious attachment. Once executed, the malware can laterally move to the server

hosting the PMS and its associated database. The reliance on older, often unpatched operating systems to run legacy dental imaging software (e.g., a Windows 7 machine running a specific panoramic X-ray application) creates a persistent vulnerability that cannot be easily fixed with a patch, as the software vendor may no longer provide support. This forces a dependence on compensatory controls like extreme network isolation, which is often technically beyond a small practice's capability to implement (Joda et al., 2020).

Privacy and Digital Communication in the Aesthetic Era

Dentistry, perhaps more than any other specialty, has embraced digital marketing and visual communication. Practices routinely use "before and after" photos of smile makeovers, full-face 3D scans, and intraoral videos for treatment planning, patient education, and social media marketing. This creates a rich trove of highly identifiable biometric data. While HIPAA provides a clear framework for de-identification, the line between a clinical photograph and a marketing asset is often blurred. Santos et al. (2021) found that many dental practice websites display patient images without adequate, HIPAA-compliant authorization forms that explicitly detail social media use, a practice inviting regulatory action and private litigation.

Furthermore, the trend toward "teledentistry" and app-based monitoring (e.g., for clear aligner therapy) introduces new data-in-transit vulnerabilities. Patients scanning their own teeth with a smartphone app are generating and transmitting PHI over networks the practice does not control. The primary privacy risk in the dental setting is less often a large-scale database exfiltration and more frequently a targeted breach of identifiable, embarrassing, or commercially valuable aesthetic data. The reputational harm and loss of community trust for a practice that exposes a patient's full-face image and associated dental history could be immediate and catastrophic, far outweighing any HIPAA financial penalty (Cruz-Correia et al., 2018).

Table 2: Differential Cyber-Risks and Mitigations: Nursing vs. Dental Services

Risk Dimension	Nursing (Acute Care Hospital)	Dental Services (Solo/Group Practice)
Primary Target	Entire hospital network, EHR servers, connected medical devices.	Practice Management Software (PMS), DICOM imaging server, billing database.
Primary Attack Vector	Phishing of clinical staff, unpatched VPN/firewall vulnerabilities.	Phishing of administrative/front-desk staff, compromised third-party billing vendors.
Patient Safety Impact	Critical: Medication errors, delayed emergency care, diversion of ambulances, increased mortality.	Moderate-to-High: Inability to access records (allergies, meds), delayed urgent care, loss of serial radiographic comparisons.
Privacy Risk Profile	High-volume, sensitive medical history, genetic data, psychiatric notes.	Highly identifiable aesthetic data (facial photos), biometric dental patterns, financial/insurance information.
Mitigation Focus	Defense-in-depth, network segmentation, MFA, dedicated OT security team, enterprise backup & DR.	Managed Security Service Providers (MSSPs), cloud-based PMS with MFA, simple immutable backup, staff security champion training.
Cognitive Load on Clinician	Constant vigilance, security fatigue, moral distress during downtime.	Distraction from patient care, responsibility for IT security without training, financial anxiety.

Synthesis and Future Directions

The synthesized evidence paints a stark picture: cybersecurity is a social-technical crisis that directly produces patient harm. It is no longer adequate to conceptualize a "data breach" as a purely administrative or legal problem. A data breach is a clinical error waiting to happen. Ransomware is a mass casualty event of patient safety, generating downtime that degrades care standards across an entire organization simultaneously. The convergence of evidence from nursing and dentistry reveals that while the scale and technical complexity differ, the core vulnerability is universal: a collision between a culture of clinical urgency and a technology landscape demanding constant security skepticism.

A key finding of this review is the centrality of human factors. No technical safeguard can compensate for a clinician who, under immense pressure and cognitive load, clicks a malicious link. This places an unspoken psychological burden on nurses, dentists, and their staff, who are now expected to be frontline cybersecurity sentinels in addition to their primary clinical duties. This burden is poorly understood and rarely compensated for in professional training or job design. The moral distress documented in nurses during an EHR outage is a powerful, under-investigated signal that cybersecurity is a determinant of workforce well-being and retention. For the small-business dentist, the burden is also a solitary financial one; the cost of a ransomware attack is not just a business continuity problem but a potential destroyer of a lifetime's work.

The regulatory environment, while well-intentioned, has often been reduced to a compliance checklist exercise that fails to foster genuine cultural change. The HIPAA Security Rule's "addressable" implementation specifications are sometimes treated as optional, and risk analyses become dusty documents stored on a shelf rather than living processes guiding daily operations (Cohen & Mello,

2018). The second-generation "HIPAA audit protocol" shifts toward a more active demonstration of compliance, yet the gap between having a policy and embodying a security-first culture remains chasm-wide.

Future Directions

Building a resilient posture against cyber threats demands a move beyond technical defenses to a socio-technical, culture-centric model. First, education must be reimagined through the lens of clinical storytelling, not fear-based IT training. Annual, generic cybersecurity modules are ineffective. What is needed is low-dose, high-frequency, discipline-specific training that uses real-world de-identified case studies—e.g., "The Phish that Stopped an Emergency Department"—to connect a suspicious email to the tangible, clinical consequence of a cancelled surgery (Gordon et al., 2019). For nurses, this could be integrated into shift-change huddles. For dental offices, it could be part of a weekly team meeting led by a designated “security champion” from the clinical staff, not an IT vendor.

Second, the design and procurement of clinical software must mandate security by design and seamless usability. Clinicians will always choose the fastest, safest path for the patient. If security features like multi-factor authentication (MFA) are slow, clunky, and interrupt workflow twenty times an hour, they will be subverted. Adaptive MFA, using biometrics like fingerprint or facial recognition on clinical workstations, and single sign-on (SSO) that balances security with speed, are non-negotiable requirements (Almas et al., 2023). Furthermore, vendors must be held contractually accountable for the security of their legacy and internet-connected products, including enforceable patching timelines.

Third, resilience planning must be clinically owned. Business continuity and disaster recovery plans cannot be solely IT documents. Every downtime procedure must be crafted, reviewed, and rehearsed with the nurses, dental assistants, and doctors who will have to execute it. Hospital incident command centers must include a clinical cyber-liaison who can translate the technical status of an attack into real-time patient safety risk assessments, guiding decisions on whether to divert ambulances or cancel elective surgeries (Dameff et al., 2023). For dental practices, a simple, laminated downtime protocol detailing how to handle an emergency patient when records are inaccessible is a practical, life-saving tool.

Finally, a new model of shared cybersecurity responsibility is needed, particularly for small practices. The idea of every dental office becoming a self-sufficient cybersecurity hub is absurd. The future lies in regional health information exchanges (HIEs), professional associations, and dental service organizations (DSOs) offering shared security operations center (SOC) services, collective cyber insurance purchasing, and turnkey, cloud-based secure PMS solutions that abstract away the complexity of backup and encryption, much like we use banking apps without understanding the underlying security protocols.

This review has limitations inherent to its narrative methodology, including potential selection bias in the literature chosen for synthesis and the exclusion of non-English language research. The rapid pace of change in both cyber threats and clinical practice means the findings are a snapshot of a moving target. Nevertheless, by synthesizing technical, nursing, and dental perspectives, the review provides a critical, multidisciplinary analysis of a problem that can only be solved by breaking down the silos between IT, clinical leadership, and frontline staff.

Conclusion

Cybersecurity of Electronic Health Records is a defining patient safety challenge of the 21st century. The narrative has shifted from protecting data from curious snoopers to defending critical clinical infrastructure from industrialized, predatory cyberattacks. For nursing and dental professionals, this is not an abstract IT issue but a daily reality that shapes workflows, generates moral distress, and, in the worst moments, directly precipitates clinical errors and patient harm. The technological safeguards of encryption, network segmentation, and immutable backups are indispensable but insufficient on their own. The greater need is for a cultural transformation that embeds cyber resilience into the identity of every clinical team. This requires moving from compliance-driven fear to a proactive culture where every nurse, dentist, and staff member understands their role not just as a data custodian, but as a guardian of patient safety in the digital domain. The future of safe, trusted healthcare depends on the professional, regulatory, and educational systems treating a click on a phishing email with the same gravity as a break in sterile technique—as a controllable, preventable threat to the life and well-being of the patient.

References

1. Alanazi, A., Almutib, A., & Aldosari, B. (2023). Physicians’ Perspectives on a Multi-Dimensional Model for the Roles of Electronic Health Records in Approaching a Proper Differential Diagnosis. *Journal of Personalized Medicine*, *13*(4), 680.
2. Almas, A., Iqbal, W., Altaf, A., Saleem, K., Mussiraliyeva, S., & Iqbal, M. W. (2023). Context-based adaptive fog computing trust solution for time-critical smart healthcare systems. *IEEE Internet of Things Journal*, *10*(12), 10575-10586.
3. Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities*.
4. Bai, G., Jiang, J., & Flasher, R. (2017). Hospital risk of data breaches. *JAMA internal medicine*, *177*(6), 878-880.
5. Campbell, E. M., Sittig, D. F., Ash, J. S., Guappone, K. P., & Dykstra, R. H. (2006).

Types of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association*, *13*(5), 547-556.
6. Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. *Jama*, *320*(3), 6-7.
7. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52.
8. Cruz-Correia, R., Ferreira, D., Bacelar, G., Marques, P., & Maranhão, P. (2018). Personalised medicine challenges: quality of data. *International Journal of Data Science and Analytics*, *6*(3), 251-259.
9. Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., ... & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA network open*, *6*(5), e2312270.
10. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, *46*(3), 541-562.
11. Franco, M. F., Lacerda, F. M., & Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. *Revista de Gestão e Projetos*, *13*(3), 10-37.
12. Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ digital medicine*, *2*(1), 98.
13. Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, *26*(6), 547-552.
14. Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: secrets of the trade. *Journal of chiropractic medicine*, *5*(3), 101-117.
15. Hassandoust, F., Techatassanasoontorn, A. A., & Tan, F. B. (2016). Factors influencing the infusion of information systems: A literature review. *Pacific Asia Journal of the Association for Information Systems*, *8*(1), 2.
16. Hassan, W. U., Bates, A., & Marino, D. (2020, May). Tactical provenance analysis for endpoint detection and response systems. In *2020 IEEE symposium on security and privacy (SP)* (pp. 1172-1189). IEEE.
17. Joda, T., Zarone, F., & Ferrari, M. (2017). The complete digital workflow in fixed prosthodontics: a systematic review. *BMC oral health*, *17*(1), 124.
18. Khan, F. (2023). Regulating the revolution: a legal roadmap to optimizing AI in healthcare. *Minnesota Journal of Law, Science & Technology*, *25*(1), 49.
19. Kim, J., Park, E. H., Park, Y. S., Chun, K. H., & Wiles, L. L. (2022). Prosocial rule breaking on health information security at healthcare organisations in South Korea. *Information Systems Journal*, *32*(1), 164-191.
20. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10.
21. Larsen, E., Fong, A., Wernz, C., & Ratwani, R. M. (2018). Implications of electronic health record downtime: an analysis of patient safety event reports. *Journal of the American Medical Informatics Association*, *25*(2), 187-191.
22. Melnick, E. R., Dyrbye, L. N., Sinsky, C. A., Trockel, M., West, C. P., Nedelec, L., ... & Shanafelt, T. (2020, March). The association between perceived electronic health record usability and professional burnout among US physicians. In *Mayo Clinic Proceedings* (Vol. 95, No. 3, pp. 476-487). Elsevier.
23. Melon, E., & Hernandez, W. (2020). Cybersecurity in the dental healthcare sector: the need of knowledge for small practitioners. *Issues in Information Systems*, *21*(1), 118.
24. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., ... & Nikpay, S. S. (2022, December). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. In *JAMA Health Forum* (Vol. 3, No. 12, p. e224873).
25. Ponemon, I. (2021). Cost of a data breach report 2021. *Risk Quantification*, *73*.
26. Poon, E. G., Keohane, C. A., Yoon, C. S., Ditmore, M., Bane, A., Levtzion-Korach, O., ... & Gandhi, T. K. (2010). Effect of bar-code technology on the safety of medication administration. *New England Journal of Medicine*, *362*(18), 1698-1707.
27. Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics*, *26*(1), e100031.
28. Rushton, C. H., Schoonover-Shoffner, K., & Kennedy, M. S. (2017). Executive summary:

transforming moral distress into moral resilience in nursing. *Journal of Christian Nursing*, *34*(2), 82-86.
29. Santos, P. S., do Nascimento, L. P., Martorell, L. B., de Carvalho, R. B., & Finkler, M. (2021). Dental education and undue exposure of patients' image in social media: A literature review. *European Journal of Dental Education*, *25*(3), 556-572.
30. Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, *7*(02), 624-632.
31. Sittig, D. F., Wright, A., Coiera, E., Magrabi, F., Ratwani, R., Bates, D. W., & Singh, H. (2020). Current challenges in health information technology–related patient safety. *Health informatics journal*, *26*(1), 181-189.
32. Slayton, T. B. (2018). Ransomware: the virus attacking the healthcare industry. *Journal of Legal Medicine*, *38*(2), 287-311.
33. Sulmasy, L. S., López, A. M., Horwitch, C. A., & , American College of Physicians Ethics, Professionalism and Human Rights Committee. (2017). Ethical implications of the electronic health record: in the service of the patient. *Journal of general internal medicine*, *32*(8), 935-939.
34. Tiongco, C. G. (2022). The clinical reasoning of occupational therapists in an oncology setting: An exploration of documentation following MOHO training.
35. Triplett, W. (2022). Ransomware attacks on the healthcare industry. *Journal of Business, Technology and Leadership*, *4*(1), 1-13.
36. US Department of Health and Human Services. (2019). Breach portal: Notice to the secretary of hhs breach of unsecured protected health information. *URL: https://ocrportal. hhs. gov/ocr/breach/breach_report. jsf [accessed 2016-10-20][WebCite Cache ID 6lPC5KlZ9]*.
37. Varpio, L., Day, K., Elliot-Miller, P., King, J. W., Kuziemsky, C., Parush, A., ... & Rashotte, J. (2015). The impact of adopting EHRs: how losing connectivity affects clinical reasoning. *Medical Education*, *49*(5), 476-486.
38. Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security* (p. 656). Boston, MA: Thomson Course Technology.
39. Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in health information management*, *11*(Fall).
40. Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: an exploratory analysis. *Perspectives in health information management*, *19*(2).