XpertDox
Clinical, Education, Research

What Protects Patient Data in Autonomous AI Medical Coding

www.xpertdox.com info@xpertdox.com Ph.205.259.6045

Table of Content

Patient Data Security & Privacy in AI Medical Coding

Healthcare organizations that leverage artificial intelligence gain a steep advantage in the medical coding field. AI-enabled medical coding outputs medical billing codes using Natural Language Processing (NLP) to interpret the patient encounter notes written by healthcare providers. This saves healthcare organizations time and money and improves the accuracy of coding.

The benefits of AI in medical coding extend beyond mere efficiency. By automating the coding process, these systems substantially reduce the time healthcare staff spend on manual coding, allowing them to focus more on patient care and other crucial tasks. Moreover, the precision offered by AI-driven coding helps minimize errors that can lead to billing inaccuracies, claim denials, and potential compliance issues. Given the complex and ever-changing nature of medical coding standards and regulations, this accuracy is crucial.

The use of AI in medical coding, while offering numerous benefits, also brings with it a host of risks, particularly in the realm of data security. In the healthcare sector, where the confidentiality and integrity of patient data are paramount, the potential mishandling of Protected Health Information (PHI) poses significant challenges. The implications of data security vulnerabilities in this context are severe, with the healthcare industry facing disproportionately high costs in the event of data breaches.

On average, a data breach costs $4.45 million globally. However, this figure more than doubles in the healthcare sector, soaring to an alarming $10.93 million[5]. This heightened risk reflects the sensitive nature of healthcare data and the extensive regulations governing its protection, such as the Health Insurance Portability and Accountability Act (HIPAA). In recent years, HIPAA violations have led to substantial penalties, including a $5.55 million fine imposed on Advocate Health Care Network[5] that affected 4 million health records and a $3.9 million fine on The Feinstein Institute[6] for the improper disclosure of PHI of 13,000 research participants. Additionally, CardioNet[7] faced a fine of $2.5 million for inadequate HIPAA compliance and poor risk management, leading to the exposure of 1391 health records.

Ransomware Attacks	EHR vendor QRS acknowledged that 320,000 PHI data leaked due to one of the largest ransomware attacks in 2021 [14].
DDoS Attacks	Distributed denial-of-service (DDoS) attack on a Children's Hospital in 2014. Anonymous (a well-known hacktivist group) targeted Boston's Children's Hospital with a DDoS attack [13].
Sales of PHI	Data brokers and hackers selling mental health records at $275 per 1,000 contacts[12]

Patient Data Security & Privacy in AI Medical Coding

Given these risks, healthcare organizations leveraging AI in medical coding must prioritize the security of PHI. To ensure robust data protection, it's crucial not only to adhere to HIPAA guidelines but also to employ advanced cybersecurity strategies specifically designed for AI and digital data management. This includes conducting regular security audits, training employees in data handling, and incorporating state-of-the-art encryption and intrusion detection systems. Furthermore, as AI algorithms and tools evolve, continuous monitoring and updating of security protocols are essential to safeguard against emerging threats.

At first glance, AI-enabled medical coding appears to be a solution exclusively for enterprise-grade healthcare organizations. However, the industry shows promise of booming at a CAGR of 9.45% from 2023 to 2028, including small to large healthcare providers. The surge reflects AI's value to medical coding across the healthcare industry. As the market expands, the accessibility and applicability of AI coding solutions are also expected to increase, making these technologies more attainable for smaller and medium-sized healthcare entities. This projected growth is not just a financial statistic; it symbolizes a paradigm shift in how healthcare organizations, big and small, approach the crucial task of medical coding. As AI technologies become integrated with healthcare processes, they are set to transform the industry's operational landscape, making AI-enabled medical coding a standard practice rather than an exclusive advantage.

The integration of AI-powered medical coding represents a significant leap forward for the healthcare industry. As AI-enabled medical coding continues to gain traction, its impacts are felt across the spectrum - from large healthcare enterprises to smaller clinics. This advancement not only saves time and money for healthcare organizations but also markedly improves coding accuracy.

However, with these AI-driven solutions, an intricate landscape of cybersecurity risks arises. The high cost of data breaches in healthcare, which significantly exceeds the global average, underscores the critical need for robust cybersecurity measures. Recent incidents of data breaches and cyber-attacks highlight the vulnerability of healthcare data and the devastating impact such incidents can have on patient trust, organizational reputation, and financial stability.

Healthcare organizations are thus at a crucial juncture where they must balance the adoption of innovative AI technologies with stringent cybersecurity measures. This balance is not only a regulatory requirement, as dictated by laws like HIPAA, but also a crucial aspect of maintaining patient trust and safeguarding the integrity of healthcare services.

Exploring Data Security Risks

At XpertDox, we have identified three primary areas susceptible to potential data security vulnerabilities: **IT infrastructure, user error, and business administration processes.**

Our XpertCoding solution meets these challenges to set new standards in medical coding efficiency, precision, and data protection. It is designed with privacy as its core value and is reinforced by industry-leading certifications, including ISO 27001, ISO 22301, SOC2 Type 1, and Type 2. Each certification provides a framework that offers extensive guidelines in security controls, such as Information Security Management Systems (ISMS), Business Continuity Management (BCM), data access controls, and data encryption checks. Our systems' compliance with these certifications is routinely audited to ensure that patient data is safe.

In the sections, we delve into how our Software as a Service (SaaS) infrastructure handles these challenges while prioritizing security compliance.

A - Securing Healthcare IT Infrastructure: Addressing Vulnerabilities and Protecting PHI

Inherent vulnerabilities exist within any IT infrastructure, and the dangers are only accentuated in healthcare. The healthcare industry suffers from more costly data breaches than other sectors, with emails and network servers identified as the main targets for significant breaches [9]. The most common data security threats reported include unauthorized data alteration, data loss, and unauthorized access and distribution. PHI accessed by malicious hackers is the greatest cause for concern because of PHI's value. Data such as credit card information, SSNs, and phone numbers can be sold and exploited for profit [10].

XpertDox takes these risks seriously by confronting this dilemma with our Information Security Management System (ISMS). In short, an ISMS defines policies and procedures for managing sensitive data. What makes our approach exceptional is the system by which we audit our security. Integrating our ISMS into our IT infrastructure allows us to analyze data security assessment statistics that identify problem areas, which are then corrected to maintain 100% security compliance. Our system defines two types of checks: monitored and periodic.

Monitored checks detect immediate anomalies that trigger alerts for our security officers to control and are audited daily. A security officer is tasked with targeting these alerts arising from existing and new assets ranging from new user accounts to expanded server hardware. The officer then troubleshoots the asset and extinguishes the associated risks until the alert is gone. Monitoring continues for all assets that operate in our IT infrastructure. Periodic checks are designed for more infrequent security audits such as employee training, disaster recovery drills, and renewal of the security policies. These checks are reviewed on a schedule with deadlines to meet compliance.

Exploring Data Security Risks

Implementing our integrated ISMS allows us to stay organized, focused, and, most importantly, secure to maintain compliance with our SOC 2 and ISO 27001 certifications. Key vulnerabilities we can manage using this system include data encryption and backup, access control, network security, and endpoint security. Additionally, our ISMS encompasses safeguards for risks that can be introduced by user error.

B - Mitigating User Error in Healthcare IT with ISMS and SOC2

At XpertDox, we understand a robust defense in IT infrastructure can quickly be eroded by user error. We classify **user error** as unintentional action or inaction by users that consequently facilitates a security breach or data loss. We prioritize mitigation techniques and policy enforcement for user error because of the magnitude of impact it has on digital environments. One study of 141,252,797 medical records shows that "73.1 percent of all affected records resulted from breaches caused by unintentional factors" [11]. Using an obvious password, transferring unencrypted data, and interacting with a suspicious email are common examples of how users can unwittingly initiate a security threat.

Our resolution for threats introduced by human error is a multi-tiered strategy that combines our ISMS with logical, physical, and conceptual layers of protection. While our SOC 2 and ISO 27001 compliance controls effectively cover both IT infrastructure and user error prevention, a separate examination of user error is advantageous. This is particularly true given the intricate nature of human interactions with digital systems, which are originally designed for more predictable and finite interactions.

We use a conventional Identity and Access Management system (IAM) that characterizes users by appropriate access levels for their roles. This protects data from being accessed, altered, or deleted by unauthorized users on a logical level. It also allows user accounts to be disabled remotely if a mobile device is lost or stolen.

Next is physically securing assets in our IT Infrastructure using perimeter security measures. Perimeter security includes video surveillance, building access control, and locked doors. The physical layer of security ensures that all interactions are surveilled and only approved users can access locations where sensitive data is stored.

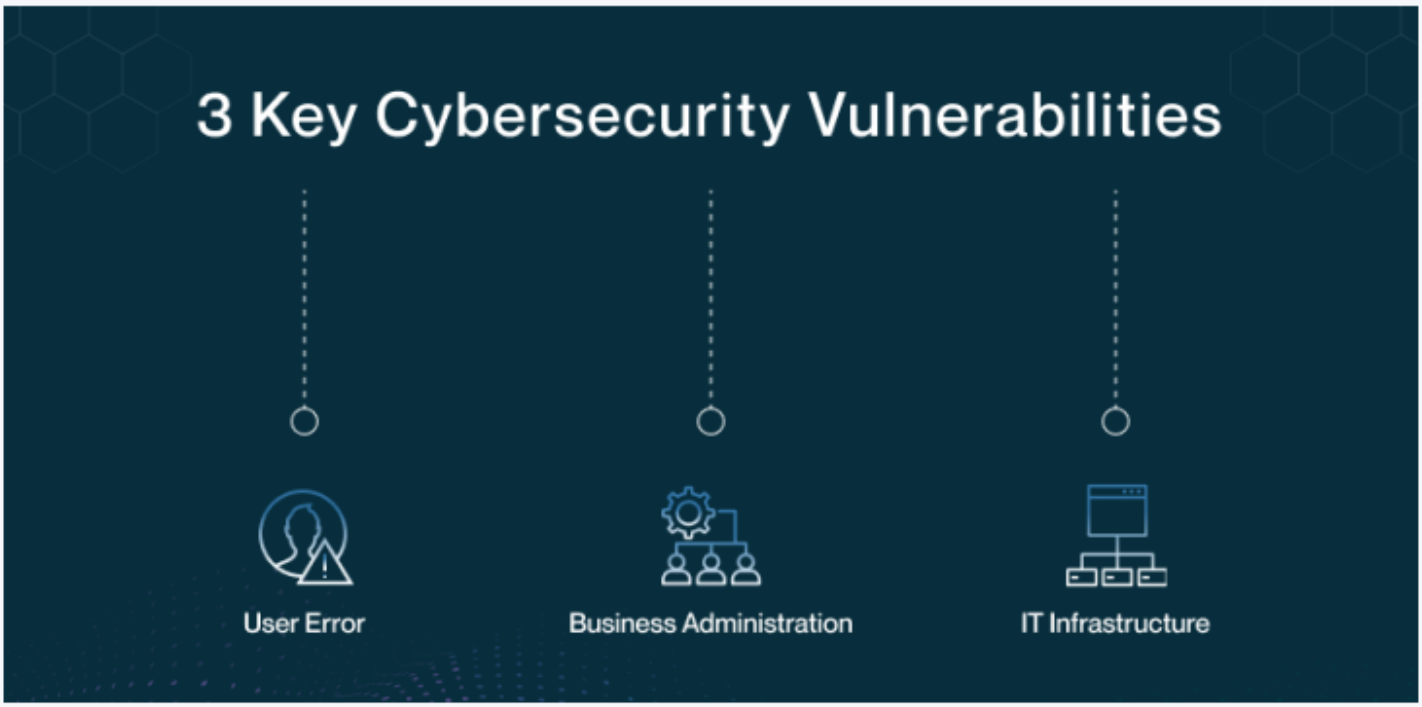
Lastly, we ensure users understand our company data protection policies and the fundamental concepts of PHI confidentiality. By default, new employees must be trained on what PHI is, how to maintain confidentiality, and what risks to be aware of when handling PHI. Moreover, the conceptual layer of security equips users with guidelines to remediate a data security violation and maintain data retention quickly. It emphasizes awareness of the prevailing data security threats that plague any IT infrastructure, such as phishing attacks, mobile device theft, and public network vulnerability.

Exploring Data Security Risks

C - Business Administration and Data Security: Balancing Remediation and Business Continuity with ISO 22301

Remediation for security violations and business continuity are crucial obligations in business administration. Business administration can either operate as the anchor of data security governance or become its breaking point and, because of its critical nature, presents another key data security challenge. Poor or absent remediation techniques coupled with ineffective company security policies can lead to PHI exposure and hefty fines, as was the fate of CardioNet in 2012. In this case, the cardiac health service provider failed to deactivate an employee's laptop stolen from their vehicle, exposing 1,391 customer records and $2.5 million in HIPAA violation penalties. Thus, the integrity of an organization's data and, by extension, the continuity of business operations heavily depend on the policies issued by business administrators.

Our compliance with industry-leading certifications is an investment in operating with the confidence of those we serve and molds our internal policies, resource allocation, development, and technology management. Most notably, our HIPAA-compliant data system requires encrypted cloud file storage, backup with versioning history, and secure onsite data backup. Our user account security policies force multi-factor authentication (MFA) and password requirements that ensure complexity. As a feature of our ISO 22301 compliance, we have developed our Business Continuity Management System (BCMS) to clearly define risks specific to our operations, incident management procedures, and a disaster recovery plan detailing impact analysis steps and subsequent remediation steps to regain full operation.



Evaluating XpertDox's XpertCoding Solution

Unlike most other autonomous medical coding platforms, which are only compliant with less than two security certifications or protocols, XpertCoding has set the benchmark with 4-industry-leading certifications, including HIPAA, ISO:27001, ISO:22301, and SOC2 Type 2, ensuring the highest level of data protection.

XpertCoding has a comprehensive data security & business continuity management system with all the necessary data security and privacy certifications for effective healthcare data management.

With 200+ controls and 1700+ checks, XpertCoding is leading the way on how healthcare software providers should handle PHI data. By automating the coding process for over 90% of claims, XpertCoding guarantees a faster claim submission process within 24 hours with a remarkable coding accuracy of more than 95%.

XpertDox vs Competition

Features	XpertDox	Others
Coverage	>90%	<90%
Cost	$	$$$
Free Pilot Program	Yes	No
Training Period	<1 month	>1 month
4 Step Quality Control	Yes	?
Audit Platform	Yes	?
Requires IT Support from Client	No	?
Within 24-Hour Claim Submission	Yes	No

For healthcare organizations, XpertCoding's HIPAA-compliant dashboard enables real-time monitoring of claim volume and billing levels across locations & providers. The analytics dashboard equips healthcare professionals to make data-driven decisions, optimizing operations across all your facilities. With XpertCoding's clinical documentation improvement module, you receive valuable feedback to enhance your clinical documentation, further optimizing medical coding and boosting your reimbursement potential. Additionally, XpertCoding provides an audit trail for all claims submitted through the platform for complete transparency.

Summary

The integration of artificial intelligence into medical coding represents a significant advancement in healthcare revenue cycle management. This innovative approach is an improvement and a transformation of existing processes, enhancing accuracy and efficiency in medical coding and revenue cycle. But with this transformation comes a heightened responsibility to protect patient privacy and data security.

Data security and privacy are critical concerns for small to large-scale healthcare providers, as evidenced by increasing public apprehension about data privacy and the costly consequences of data breaches, particularly in healthcare. Severe financial penalties imposed for HIPAA violations and the heightened vulnerability of healthcare data to cyber attacks, such as DDOS attacks, illicit selling of patient data, and ransomware, can be exacerbated as healthcare providers increasingly adopt AI technologies.

Recognizing the concerns of healthcare providers, XpertDox has implemented an Information Security Management System (ISMS) with ISO 27001 certification, supported by compliance with rigorous certifications like HIPAA, ISO 22301, and SOC2, which underscores a commitment to safeguarding patient information. Adherence to industry standards and regulations ensures the system is fortified against current and potential security threats. Going beyond compliance, an ingrained culture of security infuses all organizational layers.

The security infrastructure is versatile and adaptable, featuring end-to-end encryption, frequent security audits, and instantaneous threat detection. These elements guarantee that patient data is not only shielded from unauthorized access but also treated with utmost confidentiality and integrity.

This strategy embodies a fundamental belief: technological innovation in healthcare can be pursued without sacrificing stringent data protection measures. The path laid out demonstrates that it is possible to explore the vast potential of technological progress with AI in medical coding, clinical trials, and other industries while adhering to the ethical and privacy concerns essential to the healthcare industry.

[1]Medical coding market size, share & industry trends (no date) Medical Coding Market Size, Share & Industry Trends. Available at: https://www.mordorintelligence.com/industry-reports/medical-coding-market

[2]Newsroom- A global leader in consumer Cyber Safety. Available at: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-online-creeping/

[3]Data Transparency's Essential Role in Building Customer Trust - Cisco. Available at: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

[4]Global consumers want brands to do more to protect their privacy. Available at: https://content.truata.com/en/global-consumer-state-of-mind-report-2021

[5]Cost of a data breach 2023 (no date) IBM. Available at: https://www.ibm.com/reports/data-breach

[6](OCR), O. for C.R. (2021a) Advocate health care settles potential HIPAA penalties for $5.55, HHS.gov. Available at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html

[7](OCR), O. for C.R. (2021) Feinstein settlement, HHS.gov. Available at: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/feinstein/index.html

[8]2020-12-31 08:51: Archive of hhs.gov (no date) 2020-12-31 08:51 | Archive of HHS.gov. Available at: https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html

[9]Seh, A.H. et al. (2020) Healthcare data breaches: Insights and implications, Healthcare (Basel, Switzerland). Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/

[10] The value of personal medical information: Protecting against data breaches. Available at: https://www.naham.org/general/custom.asp?page=ConnectionsThe-Value-of-Personal-Medical-Information

[11]Yeo, L.H. and Banfield, J. (2022) Human factors in electronic health records cybersecurity breach: An exploratory analysis, Perspectives in health information management. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525

[12]Harwell, D. (2023) Now for sale: Data on your mental health, The Washington Post. Available at: https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/ =

[13]DDoS attacks: In the healthcare sector (2019) CIS. Available at: https://www.cisecurity.org/insights/blog/ddos-attacks-in-the-healthcare-sector

[14]McKeon, J. (2021) 320K impacted in EHR vendor breach, Ransomware Hits Health Systems, HealthITSecurity. Available at: https://healthitsecurity.com/news/320k-impacted-in-ehr-vendor-breach-ransomware-hits-health-systems