White Paper

Ensuring Uptime:

Business Continuity Strategies in AI Medical Coding Systems

XpertDox
Clinical, Education, Research

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

Table of Content

A. Introduction

Hospitals, clinics, and other healthcare practices ("Hospitals") rely heavily on accurate and timely medical coding to get paid. Traditionally, providers and medical coders determine the ICD codes, CPT codes, HCPCS codes, and their modifiers, and units for a given claim ("Medical Coding"), enter charges into the practice management system ("Charge Entry") and send them to the clearinghouse. More recently, companies are beginning to use computer-assisted or fully autonomous medical coding to make manual coding more efficient and eliminate the need for humans to do Medical Coding and Charge Entry ("AI-Vendors"). AI-Vendors leverage software to automate charge entry similar to automated medical coding ("AI-Medical Coding").

As Hospitals adopt AI Medical Coding, hospitals are increasingly dependent on AI Vendors for both patient care and revenue. Sudden disruptions such as power outages, cyberattacks, and natural disasters can cause the underlying AI-Medical Coding solution to fail, leading to significant financial losses, legal repercussions, and delaying patient care. The following pages examine the importance of business continuity in AI-Medical Coding systems and explore strategies to achieve it.

B. Scope of the Problem

Downtime in AI-Medical Coding can severely affect healthcare organizations. Financial losses occur due to delaying reimbursements, billing errors, and potential fines for non-compliance with regulations. Legal repercussions may arise from inaccurate coding, leading to claim denial and audits. Most importantly, patient care suffers due to delays in diagnosis, treatment, and the potential for medication errors. These are not just hypothetical scenarios but have happened multiple times, including:

A. **Cyberattack on a Hospital in 2021:** Hackers gained access to the hospital's network, including its medical records and billing systems (Gallagher, 2023). The attack shut down the coding system for a week, causing delays in patient care and significant financial losses. It took the hospital several weeks to fully recover from the attack.

B. **Data Breach:** In 2020, a data breach at Premera Blue Cross exposed the personal information of 11 million individuals, costing the company an estimated $10 million in fines and settlements (Jim Finkle, 2015).

C. **Natural Disaster:** In 2017, Hurricane Harvey caused widespread damage to healthcare facilities in Texas (The Western Journal of Emergency Medicine, 2020). The storm caused power outages, flooding, and structural damage to medical hospitals, clinics, and other healthcare facilities. The damage caused by the hurricane resulted in the cancellation of appointments, surgeries, and other essential medical services.

C. The Solution: Business Continuity Plan

Business continuity is an organization's ability to maintain critical operations during disruption. A comprehensive Business Continuity Plan outlines the steps to minimize downtime, recover quickly, and ensure the continuity of essential services. A Hospital partnering with an AI-Vendor needs a testament of the AI-Vendor's resilience and commitment to maintaining critical services. From a Hospital's perspective, the benefits of their partnering AI-Vendor implementing a Business Continuity Plan include:

A. **Reducing Downtime in AI-Medical Coding:** A robust Business Continuity Plan helps AI-Vendors recover from disruptions quickly and minimize the impact on the Hospital's operations and patient care.

B. **Improving Financial Performance for Hospitals:** Minimizing downtime in AI-Medical Coding will lead to fewer errors, faster reimbursements, and cost reductions associated with incident response.

C. **Improving Patient Safety and Satisfaction:** Continuous operation of AI-Medical Coding will ensure accurate coding, leading to timely diagnosis, treatment, and improving patient outcomes.

D. **Enhancing Regulatory Compliance:** An AI-Vendor with a Business Continuity Plan demonstrates a commitment to regulatory compliance, reducing the risk of fines and audits for the Hospital. Adherence to BCMS, SOC2, ISMS, and HIPAA standards reflects the AI-Vendor's commitment to data security, privacy, and operational resilience.

Business Continuity Plan	
Reducing Downtime in AI-Medical Coding	Improving Financial Performance for Hospitals
Improving Patient Safety and Satisfaction	Enhancing Regulatory Compliance

D. Components of the Business Continuity Plan

Now we delve into the indispensable strategies AI-Vendors use to achieve uninterrupted operations and essential functionalities of AI-Medical Coding systems through the creation and maintenance of a Business Continuity Plan. Through a comprehensive exploration, we will outline strategies AI-Vendors use to maintain consistent uptime. These strategies include conducting thorough risk assessments, implementing robust data backup and recovery plans, devising comprehensive disaster recovery strategies, ensuring technology and infrastructure availability, focusing on employee training, and fortifying cybersecurity measures. Each segment provides actionable insights for AI-Vendors to prepare and navigate challenges that interfere with business operations.

a. Risk Assessment:

AI-Vendors must prioritize risk assessment for the resilience of their systems. To build resilience, AI-Vendors need to conduct a comprehensive risk assessment to identify potential threats and vulnerabilities that could disrupt the availability of AI-Medical Coding. The risk assessment should encompass natural disasters, cyberattacks, power outages, network failures, and software failures. Two different types of risk assessments can help identify potential risks within AI-Medical Coding infrastructure:

i. **Annual Assessments:** AI-Vendors should perform a thorough risk assessment annually to address potential threats and vulnerabilities across all systems. The approach ensures ongoing awareness and preparedness for evolving risks

ii. **Change-Based Assessments:** AI-Vendors should conduct additional assessments when new changes occur within the AI-Medical Coding infrastructure. The approach ensures prompt and effective adaptations for emerging risks and minimizes potential disruptions

b. Data Backup and Recovery:

i. Hospitals consider medical data sensitive and crucial, thus AI-Vendors benefit from developing processes to safeguard vital information against systematic AI-Medical Coding failures. To safeguard against such failures, AI-Vendors should implement a comprehensive data backup and recovery plan. The plan should include routinely duplicating data and storing it in secure locations outside the existing environment. It will ensure that data recovery is manageable, quick, and effective for minimizing downtime. Proactively backing up data guarantees the continuous availability of critical information and maintains the smooth operations of essential tasks.

ii. Layering cloud storage with local data storage provides the best data backup and recovery results. Utilizing traditional and cloud technologies for data storage provides flexibility in data availability through redundancy in case of unforeseen data loss in one of the storage solutions.

D. Components of the Business Continuity Plan

iii. To add another layer of confidence to the existing data security strategies, AI-Vendors will conduct regular restoration tests from backup images. The proactive testing ensures that the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) remain within acceptable limits, enhancing system uptime and AI-Medical Coding infrastructure availability.

c. Disaster Recovery Plan:

AI-Vendors need a Disaster Recovery Plan specifying the actions to protect themselves and the Hospitals dependent on their services in case of an incident. The Disaster Recovery Plan should encompass system restoration procedures and communication protocols that clearly define roles and responsibilities for all personnel in the AI-Vendor's organization.

Key Areas for AI-Vendors to Review Annually:

i. Mitigating Risks: Carefully analyze risks and implement appropriate mitigation strategies to minimize their potential impact. Mitigation strategies include improving security measures, adding redundancy in critical systems, and creating alternative communication channels.

ii. Communication Clarity: Continuously refine communication plans to ensure timely and accurate information reaches all relevant stakeholders during a crisis. Include clear roles and responsibilities for various teams and define escalation paths for critical updates.

iii. Backup and Restoration: Regularly test and update restoration procedures to ensure data backup systems are working. Maintain secure offsite backups and optimize restoration times for critical systems.

iv. Testing and Maintenance: Regularly conduct drills and simulations to test a Disaster Recovery Plan's effectiveness and identify improvement areas. Create a scope for refining the recovery plan, continuing personnel training, and instilling confidence in everyone's role during an emergency.

v. Continuous Maintenance: Understand that a Disaster Recovery Plan is not a static document. Incorporate changes in infrastructure, technology, and business processes into the Disaster Recovery Plan.

Drawing insights through developing the Business Continuity Plan enhances the Disaster Recovery Plan and strengthens the immediate response of an AI-Vendor to a disaster. Refreshing the procedures, roles, and asset information within the Disaster Recovery Plan is essential. Proactively updating relevant information in the Disaster Recovery Plan qualifies the AI-Vendor's ability to address potential disruptions and minimize their impact on operations. An ongoing commitment to preparedness ensures business continuity for the AI-Vendor while protecting the valuable data of the Hospitals they service.

D. Components of the Business Continuity Plan

d. Technology and Infrastructure Availability:

AI-Medical Coding fortifies continuous operations of the AI-Vendor through cloud infrastructure. Leveraging cloud-based solutions, implementing failsafe systems, and securing data centers ensures critical systems are always up and running, even in the face of unexpected challenges. Key benefits of cloud-based solutions include reduced downtime, improved disaster recovery, increased flexibility, and reduced costs.

For example, AI-Vendors may take inspiration from how XpertDox has migrated its critical systems to a leading cloud provider and achieved a 99.99% uptime rate by:

i. Using a secure data center that keeps XpertDox running 24/7.

ii. Proactively monitoring and evaluating systems to identify and address potential issues before they impact operations.

iii. Investing in industry-standard security solutions to protect patient data and proprietary information from unauthorized access and cyber threats.

D. Components of the Business Continuity Plan

e. Employee Training: A well-trained workforce is crucial for effective business continuity for AI-Vendors. Training all AI-Vendor employees on the Business Continuity Plan and equipping them with the knowledge and skills necessary to respond effectively during disruptions are essential for a smooth and coordinated recovery. A trained workforce can respond effectively to disruptions, minimizing downtime and maximizing operational resilience. A robust Business Continuity Plan and employee training manual should equip each employee with the knowledge and skills to face any disruption and should include:

i. **Everyone knows Their Role:** Comprehensive training clarifies individual responsibilities during emergencies, enabling a swift and coordinated response.

ii. **Ready to Act:** Regular refresher sessions keep Business Continuity Plan knowledge fresh, allowing employees to react confidently when necessary.

iii. **Empowerment and Resilience:** Training prepares employees to contribute effectively and reduce downtime during disasters.

f. Cyber-security: AI-Vendors handle sensitive patient data, making them prime cyberattack targets and must implement robust cybersecurity measures to protect the sensitive information they handle. Globally, there is an 8% surge in weekly Cyber attacks, the highest in 2 years (Check-Point Research, 2023). AI-Vendors that implement the following suite of cybersecurity tools and processes strengthen their defense against cyber attacks:

I. **Endpoint Security:** AI-Vendors need endpoint security measures to protect devices from threats like malware, phishing, ransomware, and spyware. Endpoint security quarantines devices in contact with malicious software and prevents lateral movement from the affected device connected to other devices on the network. Endpoint security also involves preventative controls that safeguard a device from coming in contact with malicious software in the first place.

II. **Web Application Firewalls (WAFs):** AI-Vendors deploy WAFs to shield web applications from common cyber attacks such as SQL injections, distributed denial of service, and cross-site scripting. The WAF acts as a gateway between servers that hold sensitive data and external devices. The gateway masks the actual location and characteristics of the server it protects and manages data requests for the server.

D. Components of the Business Continuity Plan

III. Strong authentication:

A. Multi-factor Authentication (MFA): AI-Vendors are responsible for incorporating MFA that adds one more layer of security by requiring multiple forms of user verification.

B. Single Sign-on (SSO): AI-Vendors implement SSO systems, simplifying access to multiple applications while maintaining high security standards.

C. Role-Based Access Control (RBAC): AI-Vendors that utilize RBAC ensure system access aligns with the defined user roles within the information security management framework, minimizing unauthorized data access risks.

IV. User Activity Tracking: AI-Vendors need to monitor user activities within their systems to detect any unusual or suspicious behavior, aiding in the early detection of potential security threats.

V. Data Encryption: AI-Vendors must enforce encryption protocols to secure sensitive patient data to prevent unauthorized access and breaches. Data encryption policies must include controls for data at rest and data in transmission.

VI . Tokenization: It's crucial for AI-Vendors to use tokenization in systems handling sensitive medical data, replacing critical information with non-sensitive tokens to enhance security.

VII. Advanced Network Security:

A. Next-generation Firewalls: AI-Vendors customize firewalls to filter and block malicious network traffic. Useful customizations include port filtering, URL filtering, threshold values for detecting distributed denial of service attacks, and traffic monitoring alarms.

B. Intrusion Prevention Systems (IPS): AI-Vendors must deploy IPS to proactively identify and mitigate attacks, ensuring continuous monitoring of their systems.

D. Components of the Business Continuity Plan

VIII. Vulnerability Management:

A. Regular Scans: Regular vulnerability scanning by AI-Vendors is essential to identify security gaps in AI Medical Coding systems and applications.

B. Prompt Patching: AI-Vendors must quickly address vulnerabilities to strengthen their security measures and mitigate risks.

IX. Data Loss Prevention (DLP): AI-Vendors use DLP strategies to prevent unauthorized data transfers, especially critical in handling sensitive medical records.

X. Regular Data Backups: Regular data backups by AI-Vendors are crucial in maintaining the integrity and availability of healthcare data, forming a key component of the Disaster Recovery Plan.

Key Areas for AI-Vendors to Review Annually	
Annual Assessments	Change-Based Assessments
Data Backup and Recovery	Testing and Maintenance
Continuous Maintenance	Everyone Knows Their Role
Ready to Act	Empowerment and Resilience
Cyber-Security	Endpoint Security
Regular Data Backups	Data Encryption
Advanced Network Security	Data Loss Prevention (DLP)

E. Regulatory Compliance

The cyberattack on Prospect Medical Holdings in August 2023 illustrates the severe implications of deficient business continuity strategies (Eaton-Robb, 2023). The incident led to the shutdown of emergency rooms, ambulance services, and electronic medical records. These significant operational disruptions underscore what is at stake when business continuity is taken lightly. The ISO 22301-Business Continuity Management System (BCMS) certification controls various operational risks and requires developing comprehensive risk management and disaster recovery plans. The resulting policies and documentation become an indispensable guide for reducing downtime and ensuring rapid recovery in various scenarios. For AI-Vendors, the ISO 22301 certification is only one among several standards necessary for managing data security, such as ISO 27001 and SOC2 Type 2. For HIPAA compliance, extensive contingency plans, including Disaster Recovery Plans and Emergency Mode Operation Plans, must be a priority to address potential disruptions.

F. XpertCoding Perspective

XpertDox distinguishes itself from most AI-Vendors by adhering to four leading industry certifications, including HIPAA, ISO:27001, ISO:22301, and SOC2 Type 2. Adherence to highest standards of security measures ensures an unparalleled level of data security and protection. XpertDox's XpertCoding platform boasts a well-rounded Business Continuity Management System equipped with essential certifications along with Web Application Firewalls (WAFs), Multi-Factor Authentication (MFA), Single Sign-On systems, and data encryption for effective healthcare data management and continuous uptime.

XpertDox leads the industry with over 200 controls and 1700 checks, setting a high standard for handling Protected Health Information (PHI) in AI-Medical Coding solutions. XpertDox significantly lowers vulnerability risks by conducting regular vulnerability scans, quickly applying patches, implementing data loss prevention strategies, and maintaining regular data backups. Notably, XpertDox maintains its essential systems through a prominent cloud service provider, resulting in a remarkable uptime rate of 99.99%, thereby enhancing scalability to support expansion. XpertDox's XpertCoding solution efficiently processes over 90% of claims, ensuring rapid claim submission within 24 hours while maintaining an impressive coding accuracy rate exceeding 95%.

XpertCoding offers a HIPAA-compliant dashboard for healthcare entities that facilitates real-time tracking of claim volumes and billing across various locations and providers. XpertCoding's analytics tool empowers Hospitals to make informed, data-driven operational decisions. The platform also includes a clinical documentation improvement module, providing essential feedback to the Healthcare providers to refine clinical documentation. The enhancement not only optimizes AI-Medical Coding but also amplifies reimbursement opportunities.

XpertCoding by XpertDox ensures complete transparency to Hospitals by providing a comprehensive audit trail for all claims in the system. XpertDox's comprehensive business continuity plan ensures AI-Medical Coding remains operational despite unforeseen disruptions. XpertDox updates its Business Continuity Plan twice annually to ensure its effectiveness and relevance.

G. Conclusion

David Childers aptly sums up the need for a Business Continuity Plan with his phrase, "You never need a business continuity plan until you do." It's crucial to establish the uptime of AI-Medical Coding systems for patient care, financial viability, and regulatory compliance. Hospitals that work with AI-Vendors focusing on business continuity reap numerous advantages. Firstly, working with these vendors ensures continuous operation of AI-Medical Coding in Hospitals, which leads to timely and accurate diagnoses, thus improving patient outcomes. It also reduces costs for Hospitals by minimizing downtime and increasing efficiency, which results in lower operational expenses and faster reimbursements. When a Hospital works with a certified AI-Vendor, it demonstrates the Hospital's commitment to regulatory standards, thus reducing the risk of penalties and audits. Another advantage includes increasing operational efficiency; a robust Business Continuity Plan ensures the smooth functioning of the AI-Vendor even during unforeseen disruptions, reducing workflow interruptions and maintaining productivity for the partnering Hospital. Hospitals can achieve optimal uptime and peace of mind by partnering with a business continuity-centric AI-Vendor like XpertDox. The partnership involves leveraging third-party expertise, which leads to improving patient care and operational excellence.

Contact us today to learn more about our solutions and how they can help you achieve optimal uptime and performance.

References

1. Gallagher, R. (2023, February 3). Ireland Hospital Ransomware Attack Fractured Hacker group conti. Bloomberg.com. https://www.bloomberg.com/news/features/2023-02-03/ireland-hospital-ransomware-attack-fractured-hacker-group-conti

2. Jim Finkle (2015). Premera Blue Cross breached, 11 MLN customers' data exposed -report. Reuters. https: www.reuters.com/article/cyberattack-premera-idINL2N0WJ1W420150317

3. NIH (2020). Impact of Hurricane Harvey on Healthcare Utilization and Emergency Department Operations. NIH. https:// www.ncbi.nlm.nih.gov/pmc/articles/PMC7234707/

4. Eaton-Robb, P. (2023, August 5). A cyberattack has disrupted hospitals and health care in several states. AP News. https://apnews.com/article/cyberattack-hospital-emergency-outage-4c808c1dad8686458ecbeababd08fecf

5. Check Point Team (2023). Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year. CheckPoint Research. Check Point. https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

Additional References

1. Business Continuity Guide for Clinical Practices: https://emergency.yale.edu/sites/default/files/files/BC-Guide-Clinical-Practices.pdf

2. Ponemon Institute Cost of Data Breach Study: https://www.ponemon.org/

3. Federal Emergency Management Agency (FEMA): https://www.fema.gov/

4. Department of Health and Human Services (HHS): https://www.hhs.gov/

5. Health Information Trust Alliance (HITRUST): https://hitrustalliance.net/

6. Business Continuity Institute (BCI): https://www.thebci.org/