

Electronic Healthcare Records: As Systems Evolve, New Risks Emerge

Digital technology has transformed healthcare documentation, allowing most settings to progress from handwritten notes on paper to electronic healthcare records (EHRs) that can be readily accessed through workstations or personal devices. The speed, efficiency and flexibility of EHR systems have helped many medical offices, clinics, hospitals and aging services organizations avoid communication breakdowns, enhance teamwork, streamline data management, strengthen performance improvement efforts and encourage patients/clients/residents to be more involved in their own care. (See “A Quick Look at EHR Benefits” to the right.)

This edition of *AlertBulletin*® is designed to help healthcare organizations, administrators and providers balance innovation and safety by noting emerging EHR trends, highlighting common documentation-related risk exposures and suggesting related mitigation strategies.

New Capabilities

The diagram below lists some of the latest trends in EHR technology, along with their defining features and potential benefits:

A Quick Look at EHR Benefits

Patient/Client/Resident Safety

Built-in forcing functions, alerts and other tools help enhance compliance with critical clinical steps.

Real-time Data Access

Data banks offer timely access to information, helping prevent communication lapses and delays in care.

Coordination of Care

Advanced clinical information systems enhance team communication, productivity and care coordination.

Expanded Capabilities

Cloud-based EHR systems expand storage capacity, help prevent data loss and enable data integration.

Data Analytics

Uniform data formats and centralized storage facilitate the tracking of health outcomes and performance measurement.

Streamlined Coding and Billing

Standardized coding systems interface with billing software to improve accuracy, streamline billing and reduce fraud risk.

Integration of AI and machine learning

Algorithms flag early signs of high-acuity conditions, such as sepsis.

Predictive analytics help forecast clinical outcomes.

Machine learning features enhance the diagnostic process.

Interoperability features

Standardized data formats permit different IT systems to seamlessly share data.

Cloud-based EHRs integrate data from a variety of clinical IT sources.

Computer interfaces enable disparate systems to share data.

Voice recognition technology (VRT)

Innovative software allows providers to dictate notes directly into EHR systems.

Advanced algorithms utilize VRT to minimize transcription errors.

Integrated VRT functions expedite access to information in EHR databases.

Expansion of telemedicine and remote monitoring

Secure EHR messaging systems facilitate remote communication.

Integrated telehealth platforms enhance remote consultations.

Advanced data analytics support remote, real-time clinical monitoring and decision-making.

Advanced data security

Behavioral analytics monitor user profiles for unauthorized access or breaches.

Version-change software tracks EHR updates and monitors changes over time.

Blockchain-based EHRs improve data security and integrity, as well as personal control over data.

Risk Exposures and Mitigation Strategies

As EHR capabilities expand, healthcare organizations, administrators and providers need to remain current on emerging liabilities. The table below lists some of the major risk exposures and practical mitigation strategies relating to the use of EHR technology:

Risk Exposures	Mitigation Strategies
 System design flaws and/or lack of interoperability	• Thoroughly evaluate artificial intelligence (AI) systems prior to purchase, focusing on reliability of data analytics, AI outputs and natural language processing, among other key functions. • Pilot-test system interfaces to measure interoperability with other IT systems, including laboratories, diagnostic imaging centers and other partner organizations. • Hold regular forums for EHR users to offer comments, ask questions, suggest improvements and offer other input regarding system implementation and ongoing functioning.
 Staff resistance and misuse	• Assign qualified staff members to pilot new EHR modules, thereby identifying technical glitches and facilitating system improvements prior to implementation. • Monitor staff compliance with EHR-related protocols and determine root causes of observed misuse and unsafe workarounds. • Reinforce appropriate utilization via educational forums and written reminders.
 Issues involving templates and default settings	• Review vendor-developed templates and determine whether they align with organizational protocols, standards and regulations with respect to documentation. • Ensure that templates have input controls – such as right-left-bilateral confirmation, positive/negative notation and multiple-choice text selection – to avoid default notation. • Educate staff about the risks of copying and pasting historical information into templates, as well as filling in templates before actually providing indicated care. (See case scenario on page 4.)
 Outdated or incorrect information in the record	• During each healthcare encounter, review the active problem list and perform a thorough medication reconciliation, removing outdated entries, resolved conditions and discontinued drugs. • Identify any high-alert medications – such as opioids, insulin and anticoagulants – to help ensure proper dosage and adherence to prescribing, administering and monitoring guidelines. • Educate staff on the use of built-in correction features – such as late entries, addenda or amendments – when addressing incorrect or omitted information in the EHR. • Implement regular audits of EHRs to identify and correct outdated information. • Consult with legal counsel before making any corrections or late entries if there are treatment concerns or after a claim has been filed.
 Voice recognition (VR) software-related errors	• Select VR software that allows providers to correct errors as they dictate, reducing the likelihood of inaccuracies. • Adopt standardized dictation templates for common procedures and assessments, thus helping ensure that critical information is consistently captured in the EHR. • Ensure that VR systems comply with HIPAA Privacy and Security Rules, keeping in mind that unencrypted voice data can be intercepted or accessed by unauthorized users. • Prohibit use of VR systems in public or unsecured environments, where information about patients/clients/residents may be misheard, overheard or recorded unintentionally. • Audit VR documentation regularly for accuracy and to identify common lapses, such as failure to sign off before posting.
 Pre-populating data	• Educate providers and staff about the importance of verifying pre-populated information and supplementing it with manual entries whenever more clinical context is required. • Adjust or disable auto-fill capabilities in standardized templates used to document medications, chronic conditions, comorbidities, skin assessments and other high-risk areas. • Audit EHRs regularly to identify inappropriate pre-population practices.

Risk Exposures	Mitigation Strategies
 Overriding alerts and flags	• Educate providers and staff about the importance of alerts and the risks of ignoring or overriding them. • Limit alerts to high-risk conditions, which can help prevent “alert fatigue.” • Monitor alert override rates during routine performance improvement activities and ascertain their underlying causes. • Seek staff and provider feedback on the frequency of alerts, and utilize their comments when refining and improving alert systems.
 Overreliance on embedded AI platforms	• Ensure that AI-enabled platforms and AI-generated decisions are subject to human oversight to maintain accountability and guard against automatic acceptance of AI recommendations. • Instruct providers to document their rationale when accepting AI recommendations and to fact-check system outputs. • Monitor the utilization of clinical decision-support tools, checking for excessive or inappropriate use of AI-enabled technology.
 Security lapses	• Regularly conduct cybersecurity assessments of the EHR system to identify vulnerabilities and determine how protected health information is used, stored and secured. • Scrupulously enforce user authentication rules, data encryption requirements and device regulation protocols. • Inform staff members and providers of common cyber threats, including phishing attacks, decoding of encrypted data, and unauthorized or illicit disclosure of sensitive data. • Maintain up-to-date antivirus software to protect against malware, monitor data flow, detect irregularities and respond to potential cyberattacks.
 System outages and data loss	• Verify the adequacy of cloud-based backup capability with the EHR vendor and rectify any potential deficiencies. • Establish clear policies and procedures regarding data backup, as well as restoration of lost or compromised records. • Prioritize backup of critical EHR systems used to store, maintain or transmit electronic protected health information. • Regularly update outage-related policies and procedures and conduct downtime drills to ensure that staff members are aware of their assigned roles and responsibilities. • Address EHR outages in the organization’s business continuity plan, including a detailed incident response plan in the event of a cyberattack.
 Fraudulent activities	• Draft policies regarding proper use of copy-paste capabilities, with particular emphasis on preventing duplicate billing and retention of obsolete information. • Instruct providers and staff to validate data entered into the EHR system, thus avoiding inclusion of incorrect or misleading information. • Ensure that the EHR system is easily auditable and keeps a record of users, data input, and amendments and deletions made. • Utilize advanced algorithms to analyze billing patterns and flag unusual activities, e.g., phantom billing, upcoding of services provided, unbundling of related services that should be billed together and signs of potential identity theft.

This table serves as a reference for healthcare organizations seeking to evaluate risk exposures associated with electronic healthcare records. The content is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your organization and risks may be different from those addressed herein, and you may wish to modify the activities and questions noted herein to suit your individual organizational practice and patient/client/resident needs. The information contained herein is not intended to establish any standard of care, or address the circumstances of any specific healthcare organization. It is not intended to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. The material presented is not intended to constitute a binding contract. These statements do not constitute a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice, including advice of legal counsel, given after a thorough examination of the individual situation, encompassing a review of relevant facts, laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

As electronic record systems continue to evolve in terms of both capabilities and complexity, providers and healthcare organizations of every type need to examine and update their own EHR-related risk management approaches. This article is intended to serve as a basis for internal discussions about trends in record-keeping technology, current and emerging liability exposures, and proactive strategies to reduce risk and enhance regulatory compliance.

Quick Links to CNA Resources

- *inBrief*® 2025-Issue 1, "[Patient/Client Portals: Maximizing Benefits, Minimizing Risks.](#)"
- *inBrief*® 2023-Issue 1, "[Cybersecurity: Protect Patients by Preventing Data Breaches.](#)"
- *Vantage Point*® 2026-Issue 1, "[Documentation Deficiencies: Creating a Reliable Record of Care.](#)"
- *Vantage Point*® 2025-Issue 2, "[Artificial Intelligence: A Second Look at an Evolving Technology.](#)"
- *Vantage Point*® 2024-Issue 2, "[Telemedicine Update: Coordinating Remote and In-person Care.](#)"

Did someone forward this newsletter to you? If you would like to receive future issues of *AlertBulletin*® by email, please register for a complimentary subscription at go.cna.com/HCSubscribe.

Liability Scenario: Copy-Paste Error

A patient with a history of receiving anticoagulation therapy for atrial fibrillation was admitted to the hospital for pneumonia. Progress notes from a prior admission indicated a normal International Normalized Ratio (INR) level. Following the patient's transfer to an intensive care unit (ICU), these normal results were copied and pasted by a provider into the electronic ICU admission note, even though a more recent test had revealed an abnormal INR level. A subsequent anticoagulation dose was erroneously based upon the patient's prior normal level, which was then carried over in the daily ICU progress notes for two additional days.

Shortly thereafter, the patient exhibited stroke symptoms. A repeat INR revealed that the abnormal INR had been overlooked and that the patient's erroneous anticoagulation dose was the root cause of the stroke. A lawsuit filed by the patient's family asserted improper treatment, leading to permanent neurological injury. The case was settled due to an inability to defend the copy-paste documentation error and subsequent medication miscalculation.

Risk reduction measures:

- **Educate staff members and providers on the proper use of copy-paste** and other related EHR functionalities, and document attendance.
- **Prohibit copying and pasting of high-risk items**, such as laboratory results, radiology reports and drug formulations.
- **Audit staff and provider compliance with copy-paste protocols**, and institute a corrective action plan if irregularities are detected.
- **Consider disabling the EHR system's copy-paste function** if misuse becomes a chronic problem.

For more information, please call us at 888-288-3534 or visit www.nso.com or www.hpso.com.



888-288-3534

www.nso.comwww.hpso.com

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable as of the date they are cited, but they should not be construed as legal or other professional advice. CNA, Aon, Affinity Insurance Services, Inc., NSO, or HPSO accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Certain coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds. The claims examples are hypothetical situations based on actual matters. Settlement amounts are approximations. Certain facts and identifying characteristics were changed to protect confidentiality and privacy. Any references to non-CNA, non-Aon, AIS, NSO, and HPSO websites are provided solely for convenience, and CNA, Aon, AIS, NSO and HPSO disclaim any responsibility with respect to such websites. "CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities. This material is not for further distribution without the express consent of CNA. Copyright © 2026 CNA. All rights reserved. Published 3/26. CNA AB26-1.

Healthcare Providers Service Organization is a registered trade name of Affinity Insurance Services, Inc., a licensed producer in all states (TX 13695); (AR 100106022); in CA, MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services, Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.

Nurses Service Organization is a registered trade name of Affinity Insurance Services, Inc., a licensed producer in all states (TX 13695); (AR 100106022); in CA, MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services, Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.