INBRIEF®

CNA
We can show you more.®

IB 2017 ISSUE 1

Record Retention Policies: Evaluating Compliance, Mitigating Risk

Formal record retention policies and procedures demonstrate a systematic and organized approach to information storage. In addition, they can help enhance compliance with legal and regulatory requirements and evince good faith in the event of an allegation that records relevant to a malpractice claim were deliberately and maliciously destroyed.

Organizational record retention programs should encompass every aspect of healthcare delivery and administrative functioning, including the following:

- *Clinical care*, e.g., provider and nurses' notes, patient assessments, medication profiles, diagnostic testing, care plans, consultation reports.
- *Quality improvement,* e.g., quality assurance and peer review documents, incident reports, performance improvement projects, risk management investigations and findings.
- *Employment*, e.g., original applications, background check and drug screen results, provider and staff licensure and certification, OSHA training and immunization verification, personnel performance reviews, disciplinary action reports, employment contracts, payroll records.
- *Operations*, e.g., appointment schedules, laboratory specimen tracking logs, staff time sheets, patient billing statements.
- *Legal/governance*, e.g., governing charter and bylaws, executive board meeting minutes, partnership agreements, vendor contracts, annual reports.
- *Regulatory*, e.g., cost reports, state surveys, accreditation documents, year-end management summaries.
- *Financial,* e.g., bank deposits, monthly statements, tax returns, accounting audits, insurance policies.
- *Retired health data,* e.g., electronic healthcare records, hard-copy patient files, medical images, voice recordings.

To access *inBrief*® online, visit **www.cna.com/healthcare**, click on "Search CNA" in the top right-hand corner of the screen, type the article's full title in the search box and then click on the magnifying glass icon.

Healthcare organizations and providers must maintain records in accordance with various federal regulations. Although there is no single record retention schedule that every healthcare professional must follow, healthcare leaders should be aware of rules and recommendations from the following agencies and professional associations, among others:

- American Health Information Management Association (AHIMA) (especially Appendix A).
- Centers for Medicare & Medicaid Services (CMS).
- Health Information & the Law (an online resource supported by the George Washington University's Hirsh Health Law and Policy Program and the Robert Wood Johnson Foundation).
- U.S. Department of Health & Human Services (HHS), on the HIPAA Privacy Rule.

In addition, organizations must observe individual state record retention requirements, which may vary for different types of providers and/or patients. For a listing and comparison of state-specific regulations, respectively, consult the websites of HealthIT.gov and Heath Information & the Law.

In the absence of a specified time frame, organizations should retain health information for at least the period of the state's statute of limitations for malpractice lawsuits. For minors, health information should be archived until the patient reaches majority as defined by state law, plus the period of the statute of limitations. It is prudent to err on the side of longer retention, as the statute may not be triggered until the potential plaintiff learns of a possible connection between an injury and care received.

Sound documentation is fundamental to risk management. By implementing legally compliant record retention and maintenance policies, as outlined on the following pages, organizations can help ensure that vital documents are accessible when needed for clinical and legal purposes.

Document Management and Retention Questionnaire

This checklist can help healthcare entities and professionals evaluate their risk management efforts in regard to maintenance, security, retention and destruction of records. This resource is intended to serve as a summary of basic considerations, rather than a comprehensive list of requirements and good practices.

RISK CONTROL MEASURES	STATUS	COMMENTS
HEALTH INFORMATION MANAGEMENT (HIM) ESSENTIALS		
Is there an HIM policy and procedure manual, which addresses document retention and other compliance issues?		
Are patient healthcare information records treated as the property of the healthcare entity, and is this fact affirmed in written policy?		
Does the organization maintain an accurate inventory of patient healthcare information and specify which personnel have access to it?		
Is the path of protected health information (PHI) from admission to discharge tightly controlled, and is it depicted in an explanatory flowchart?		
Do all business associates who handle PHI meet HIPAA requirements in regard to privacy and security?		
Where shared-care arrangements exist, are each party's information-management responsibilities clearly delineated in contracts, including access to patient healthcare records in the event of litigation?		
Is there a designated depository for employment-related records, including drug-screening results and proof of immunizations?		
EMPLOYEE/VENDOR ACCOUNTABILITY		
Are staff trained in documentation requirements, and is this training based on written organizational protocols?		
Are records maintained of staff training, ongoing communication and enforcement efforts related to compliance with documentation, retention and privacy requirements?		
Are employees trained to properly handle PHI pursuant to HIPAA privacy requirements?		
Are background checks conducted for new hires, and do these checks include cyber-crime and data breach incidents?		
Are all hired and contracted staff and vendors informed of the rules governing patient healthcare information records, and is this issue covered in the terms and conditions of employment?		
Are staff documentation practices closely monitored, and is improper maintenance of patient records considered grounds for disciplinary action?		

In the absence of a specified time frame, organizations should retain health information for at least the period of the state's statute of limitations for malpractice lawsuits.

RISK CONTROL MEASURES	STATUS	COMMENTS
HEALTHCARE INFORMATION RECORD COMPOSITION		
Are the elements of a patient healthcare information record defined in written policy?		
Are unique identifiers used for all patient healthcare information records?		
If multiple patient identifiers exist for different forms of health data, is there a process for reconciling and linking separate records, and is this process regularly audited?		
Do patient healthcare information records identify other documents that relate to patient care and thus may be subject to retention requirements, such as laboratory specimen logs or diagnostic reports?		
Is there an index system designed to track "satellite" records distinct from the principal patient healthcare information record?		
ELECTRONIC HEALTH RECORD (EHR) SAFEGUARDS		
Is there an up-to-date list of the electronic portion of patient records in "hybrid" computerized/paper record systems?		
Are past portions of EHRs accessible regardless of more recent software or hardware changes, and are these records capable of being reproduced on paper when needed?		
Does written protocol designate the EHR format as a legal record, and are staff reminded of this policy?		
Is there a written policy for scanning paper documents into EHRs, and is this protocol regularly reviewed and updated?		
Are all diagnostic and laboratory order forms bar-coded for quality and record-keeping purposes?		
Do all staff members understand their responsibility for securing and retaining EHRs, including providers, clinical staff, IT administrators and technical support personnel?		
Are prior versions of software and retired servers retained by EHR vendors, in order to facilitate access to old or archived records?		
PAPER RECORD SAFEGUARDS		
Is there a centralized storage place for paper records?		
Does the organization have an effective tracking system permitting prompt retrieval of paper records?		
Are controls in place to prevent removal of paper records from the site of care without prior authorization?		
Are there formal policies governing conversion of paper records into electronic ones, and is this responsibility assigned to just one vendor?		

RISK CONTROL MEASURES	STATUS	COMMENTS
RECORD SECURITY AND ACCESS CONTROLS		
Are appropriate security measures in place to protect electronic data, including use of encryption, user authentication and strong passwords?		
Are paper and digital patient healthcare information records and PHI fully secured during the retention period by a range of administrative, technical and physical safeguards?		
Are newly hired staff informed during orientation about privacy and retention practices, and do they have ready access to relevant written policies?		
Are data integrity checks conducted on an ongoing basis to detect possible corruption of electronic files?		
Are patient records readily accessible to staff at the point of patient care or service delivery?		
Are employees granted full, partial or no access to PHI based upon their specific job or task?		
Do passwords contain upper- and lowercase letters, as well as special characters and numbers, as an anti-hacking measure?		
Are clinical and business data security measures continually reviewed and updated, and has a formal risk analysis been performed in this area?		
Does written policy dictate when passwords must be changed (e.g., every 90 days), and does one person assign and track staff passwords?		
Are environmental access controls in place where paper records are stored, such as visual monitoring, locked doors, and intruder detection and alarm systems?		
Are login timeouts utilized to prevent unattended "live" screens?		
Are user accounts locked after a specified number of failed login attempts to prevent unauthorized access?		
Are login credentials deactivated for terminated employees as soon as they leave the organization?		
Are patients informed of the organization's record retention policy, especially with regard to accessing records from patient portals and/or locating past records for issues that may arise after treatment has ended?		

For minors, health information should be archived until the patient reaches majority as defined by state law, plus the period of the statute of limitations.

RISK CONTROL MEASURES	STATUS	COMMENTS
RETENTION, STORAGE AND DISPOSAL		
Do written retention schedules reflect state and federal requirements for patient healthcare information records, as well as for documents pertaining to quality of care, employment, finances, legal matters and other regulated areas?		
Are electronic records stored securely, and do data storage systems feature built-in redundancy?		
Are paper records containing PHI filed securely in a locked storage unit that complies with HIPAA requirements?		
Do written policies and procedures address the destruction or disposal of paper and electronic records, and are these policies consistent throughout the facility or health system?		
Are electronic records disposed of in a manner that renders them permanently unreadable and unable to be reconstructed, and is there a secure system to shred, pulp or burn paper records?		
Does the organization contract with a vendor specializing in proper storage and disposal of records, and is the vendor carefully selected and monitored?		
Does a formal protocol govern the safe disposal of all electronic equipment with a memory, including laptops, work stations, copiers, smartphones, etc.?		
CHAIN OF CUSTODY		
Is there a written protocol regarding the movement of paper records from site to site, especially in terms of chain of custody?		
Does the protocol address specific handling activities and responsibilities, including who is authorized to transport records, and when?		
Does the protocol require transporters to check and document the condition of records both at departure and upon arrival at the designated site?		
Is an audit trail maintained for record transport, and is it available for review?		
Is the chain of custody maintained at all times, including when PHI and other protected data are being transported for destruction?		
CONTINGENCY PLANNING		
Is there a written disaster recovery plan, and does it include the possibility of damage to electronic and paper records?		
Is the recovery plan tested at least once a year through a mock disaster drill?		
Are EHRs and electronic business records backed up on a daily basis and stored at a separate site?		
Are servers and file storage areas protected by fire detection and suppression systems, as well as other environmental controls?		
Are duplicate hard-copy and electronic files of vital patient and business information readily available for recovery purposes following a disaster?		
Is one individual in charge of managing archived data during the disaster recovery process?		
Is there a list of vendors specializing in post-disaster data recovery who can be contacted in an emergency?		

RISK CONTROL MEASURES	STATUS	COMMENTS
QUALITY ASSURANCE/MANAGEMENT		
Is there a designated director of patient healthcare information records who oversees record retention and management?		
Are record retention issues addressed by relevant internal committees, such as those responsible for overseeing forms, EHR and quality assurance/ performance improvement?		
Is there a written protocol for developing, revising and approving forms for the patient healthcare information record?		
Is there an established audit mechanism to monitor incomplete or inadequate patient healthcare information records?		
Are patient record maintenance and retention concerns addressed by the quality assurance committee, including issues involving medical and clinical staff?		
Are quality audits of scanned records performed regularly to ensure that the EHR is complete and scanned contents are accurate?		
LEGAL CONSIDERATIONS		
Does the record retention policy reflect all legal and regulatory requirements, including applicable state and federal rules and the state statute of limitations?		
Is a policy in place addressing retention of and access to minors' healthcare records, as well as other special cases?		
Is there a formal records release policy, which is aligned with the organization's patient privacy and document retention protocols?		

This tool serves as a reference for organizations seeking to evaluate risk exposures in regard to maintenance, retention and destruction of 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 clinical procedures and risks may be different from those addressed herein, and you may wish to modify the tool to suit your individual practice and patient needs. The information contained herein is not intended to establish any standard of care, serve as professional advice or address the circumstances of any specific entity. 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.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.

Published by CNA. For additional information, please contact CNA at 1-866-262-0540. The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA 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 situation. Please note that Internet links cited herein are active as of the date of publication, but may be subject to change or discontinuation. 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. "CNA" is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.
Published 2/17. CNA IB17-1.