AHIMA Distance Education
Career-building Resources

Record Retention and Destruction

AHIMA FASTfacts audio seminars

Practical Tools for Seminar Learning

Disclaimer

The American Health Information Management Association makes no representation or guarantee with respect to the contents herein and specifically disclaims any implied guarantee of suitability for any specific purpose. AHIMA has no liability or responsibility to any person or entity with respect to any loss or damage caused by the use of this audio seminar, including but not limited to any loss of revenue, interruption of service, loss of business, or indirect damages resulting from the use of this program. AHIMA makes no guarantee that the use of this program will prevent differences of opinion or disputes with Medicare or other third party payers as to the amount that will be paid to providers of service.

How to earn one (1) CEU for participation

To earn one (1) continuing education unit, each participant must do the following:

Step 1: **Listen** to the seminar, via Webcast link, audio CD, or MP3.

Step 2: Complete the **assessment quiz** contained in this resource book. Use the included answer key. ***Do not return*** the quiz to AHIMA. Save it for your records.

Step 3: EACH LISTENER must visit **http://campus.ahima.org/audio/fastfactsresources.html** and complete the sign-in form and the seminar evaluation.

Step 4: After you complete the evaluation, you will receive your **CE certificate which you should print for your records**. The certificate must be retained by each participant as a record of their participation, along with a copy of their completed quiz.

Faculty

Nanette B. Sayles, EdD, RHIA, CCS, CHP, FAHIMA

Nanette Sayles has extensive health information management in hospitals, a computer vendor and a consulting company. She was the 2005 Triumph Educator award winner. She has held numerous offices and other volunteer roles for the American Health Information Management Association, the Georgia Health Information Management Association, the Alabama Association of Health Information Management, Middle Georgia Health Information Management Association and Birmingham Regional Health Information Management Association.

Dr. Sayles has published two books: *Professional Review Guide for the CHP, CHS, and CHPS Examinations* and *Case Studies in Health Information Management*. She is currently the Program Director of the Health Information Management and Technology Programs/Associate Professor at Macon State College in Macon, Georgia.

Dr. Sayles has a BS in Medical Record Administration, a MS in Health Information Management, a Masters in Public Administration, and a doctorate in Adult Education.

Table of Contents

Notes/Comments

Discussion Topics

- Discuss the important points for consideration when a physician office practice develops a retention schedule for patient health information (clinical and business) based on federal, state and accreditation retention standards
- Identify the legal record for retention purposes
- Provide best practices for when and how to destroy health and business records

1

Introduction to Retention of Medical Records

- **Retention addresses:**
  - How long?
  - What format?
  - Where?

2

Notes/Comments

Medical Records vs. Business Records

- **Medical records / Clinical records:**
  - Progress notes
  - Test results
  - Problem list
- **Business records / Non-clinical records:**
  - Bill
  - HIPAA Notice of Privacy Practices acknowledgement
  - Copy of insurance card

3

Retention is Influenced by:

- **State / federal statutes**
  - Medicare: 5 years
  - Other federal laws (see Practice Brief – Retention of Health Information)
  - State laws vary
  - Statute of limitations

4

Notes/Comments

Retention is Influenced by:

- **Provider needs**
  - Research
  - Education
  - Patient care
  - Pending litigation
- **Age of patient**

5

Retention is Influenced by:

- **Facility Resources**
  - Staff
  - Funds
  - Space
- **Professional standards**
  - American Health Information Management Association
- **Accreditation**

6

Notes/Comments

Ancillary Materials that Must be Retained

- **Email Communications**
- **Fax Communications**
- **Images/Tracings**
  - Radiology
  - EEGs
  - EMGs
  - EKGs

7

Retention Rule

Always follow strictest regulation!

8

Notes/Comments

Minors

- **Maintained to the age of majority PLUS the state law defined time period (typically the statute of limitations)**

9

Legal Medical Record

"The LHR is the documentation of the healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization. The LHR is individually identifiable data, in any medium, collected and directly used in and/or documenting healthcare or health status."

- Amatayakul, Margret et al. "Definition of the Health Record for Legal Purposes (AHIMA Practice Brief)." *Journal of AHIMA* 72, no.9 (2001): 88A-H.

10

Notes/Comments

Legal Health Record

- **Traditionally**
  - Paper medical record
  - Radiology
  - Other imaging
- **Currently more complex**
- **Each organization must define**

11

Legal Health Record

- **New Electronic Discovery Civil Rule**
  - Electronic documentation is discoverable
  - Records not destroyed according to retention schedule are discoverable

12

Notes/Comments

Components of Legal Health Record

Includes:

- Advanced directives
- Traditional medical record examples
  - Discharge summaries
  - Test results
  - Orders
  - Progress notes
  - Care plans
  - Medication records
- Emails between patient and provider or provider to provider
- Patient submitted documents
- Video of patient
- Diagnostic tracings
- Alerts

Excludes:

- Authorizations for release of information
- Birth/death certificates
- Audit trails
- Quality improvement
- Utilization review
- Clinical pathways
- Accreditation reports
- Best practices
- De-identified information used in research
- Personal health records

13

Retention Schedules

Should have policy and procedure on:

- What format medical records are stored in:
  - Paper
  - Electronic
  - Microfilm
  - Imaging
- Onsite vs. off-site storage
- Destroy everything vs. selected documents

14

Notes/Comments

Off-site Storage Considerations

- Costs
- Security of storage area
- Contract
- How records will be transported
- Employee training
- Accessibility of record

15

Destruction of Records

- "Normal course of business"
- In-house vs. vendor destruction
- Vendor must protect protected health information (PHI)
- Contract with destruction vendor
- Business associate agreement with vendor

16

Notes/Comments

Typical Methods of Destruction

- **Paper**
  - Burning
  - Shredding
- **Microfilm**
  - Pulverizing
  - Recycling
- **Electronic**
  - Degaussing
  - Overwriting

17

Certificate of Destruction

- Date of destruction
- Method of destruction
- What was destroyed
- Inclusive dates
- Statement that destruction was in normal course of business
- Signature of individuals performing/witnessing destruction

18

Notes/Comments

Summary of Required Documents/Documentation

- **Policies and Procedures**
  - Destruction schedule
  - Retention schedule
- **Business Associate Agreements**
- **Vendor Contracts**
- **Certificate of Destruction**

19

Other issues to consider

- **Privacy and security**
  - Access
- **Disaster planning**
  - Risk
  - Recovery

20

Notes/Comments

AHIMA References

- **Practice Brief: Retention of Health Information (2002)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_012545.hcsp?dDocName=bok1_012545
- **Practice Brief: Destruction of Patient Health Information (Updated 2002)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_016468.hcsp?dDocName=bok1_016468
- **Practice Brief: Definition of the Health Record for Legal Purposes (2001)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_009223.hcsp?dDocName=bok1_009223
- **Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes (2005)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_027921.hcsp?dDocName=bok1_027921
- **Sample Certificate of Destruction**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_016179.hcsp?dDocName=bok1_016179

21

AHIMA References

- **Update: Maintaining a Legally sound Health Record – Paper and Electronic (2006)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028509.hcsp?dDocName=bok1_028509
- **The New Electronic Discovery Civil Rule**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031860.hcsp?dDocName=bok1_031860
- **Mobile Device Use, Reuse and Disposal (2007)**
  http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_034415.hcsp?dDocName=bok1_034415 (*Note: this article is available to AHIMA members only, through the FORE Library Body of Knowledge.*)
- **Practice Brief: E-mail as a Provider-Patient Electronic Communication Medium and its Impact on the Electronic Health Record (2003)**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021588.hcsp?dDocName=bok1_021588

22

Notes/Comments

AHIMA References

- **Health Information Management: Concepts, Principles, and Practice by LaTour and Eichenwald-Maki (2006)**
  https://imis.ahima.org//orders/productDetail.cfm?pc=AB103306&bURL=%2Forders%2FSearchAction%2Ecfm%3F

23

Other References

- **Green, M.A. & Bowie, M.J. (2005). *Essentials of Health Information Management: Principles and Practices*. Thomson Delmar Learning: Clifton Park, NY.**

24

Notes/Comments

AHIMA Audio Seminars

Visit our Web site
http://campus.AHIMA.org
for updated information on the current seminar schedule.
While online, you can also register for live seminars or order CDs and Webcasts of past seminars.

AHIMA Distance Education
Career-building Resources

Assessment

To access the assessment quiz that follows this seminar, download the seminar's resource book at

http://campus.ahima.org/audio/fastfactsresources.html

Your sign-in form and certificate of completion are also found in the resource book.

AHIMA Distance Education
Career-building Resources

Notes/Comments

Thank you for attending!

Please visit the AHIMA Audio Seminars Web site to complete your evaluation form online at:

http://campus.ahima.org/audio/fastfactsresources.html

Appendix

Article: Southerton, Laurie. "Mobile Device Use, Reuse, and Disposal." *Journal of AHIMA* 78, no.6 (June 2007): 68-70.

http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_034415.hcsp

Assessment Quiz

CE Certificate and Sign-in Instructions

Quiz Answer Key

Mobile Device Use, Reuse, and Disposal

by Laurie Southerton, CHP, CHSS

The healthcare industry increasingly communicates via technology. Mobile devices are becoming prevalent in many organizations to the point where many staff find it difficult to work without them.

The HIPAA privacy and security rules require the private and secure handling of patient information that increasingly resides on mobile devices. As such, organizations are responsible for the secure use, reuse, and disposal of mobile devices such as notebooks, tablet PCs, PDAs, and smartphones.

HIPAA Privacy and Security Rules

The HIPAA privacy rule mandates that healthcare organizations keep protected health information (PHI) private. This pertains to all transmitted and maintained health information that identifies an individual or that could reasonably be used to identify an individual, including name, address, phone number, Social Security number, e-mail address, license plate number, prescription numbers, and medical record numbers.

The HIPAA security rule protects all forms of electronic PHI through controls maintained as administrative, physical, and technical safeguards. Mobile device security is primarily addressed under technical safeguards such as access control, person or entity authorization, audit control, and transmission security or encryption.

Designed to Preserve Data

To address the use, reuse, and disposal of mobile devices, one must first understand what is stored in the various components of a typical mobile device.

A mobile device is a computer with an operating system, applications, and storage areas. Just as with all complex modern computing systems, mobile devices are designed to preserve, rather than shed, data. For instance, in nearly all mobile computing devices the subscriber identity module (SIM), a smart card, securely stores the mobile phone unique subscriber information or the international mobile subscriber identity.

This information includes subscription information, all saved and dialed telephone numbers, phone preferences, text messages (including deleted messages), the network state information including the current location area identity, and information concerning countries visited by the user.

The phone has internal memory in the form of an onboard flash memory from which deleted items can be retrieved. Almost all data written to a computing hard drive or other type of digital storage remain there until overwritten. Deleted items are not erased from the device; deletion merely removes the pointer to the data. As such, a typical hard drive is littered with remnants of information that can be retrieved with widely available tools and techniques.

Information stored on a mobile phone can include the phone identity, some text messages and multimedia messages, location information, wordlist database, audio recordings, phone settings (language, date, time, tone, volume), camera images, computer files, logged incoming calls and dialed numbers, executable programs, calendar

events and tasks, general packet radio services, Wireless application protocol, and Internet settings and the cache from these activities. As new calls and messages are stored in phone memory and on the SIM, new calls and messages overwrite deleted material that may have been stored but not yet overwritten.

Many times the phone has a flash memory card used to extend storage capacity. This is considered a file system and can be used to store multimedia messaging service messages that may include images, audio, video, and rich text. However, phone system items are not stored on flash memory.

Privacy issues surface when the potential exists for renovating all the information amassed in the various components of a typical mobile device and using it with malicious intent.

Mobile Device Technical Controls

All healthcare organizations that authorize the use of mobile devices should have sound security policies in place that restrict personnel from using personal mobile devices. Ideally, each issued or authorized mobile device has a standard image installed that cannot be altered by the individual user.

The image must:

- Support applications that allow only properly authenticated individuals to access the device and its information
- Allow for audit control through logging activities
- Encrypt the data and information transmitted

Change management policies and procedures are IT safeguards that limit error and prevent unauthorized changes to computer systems and disruptions to the organization's IT assets. Change management policy and the resulting change management control system contain specific procedures that define analysis, application, and review of changes to the IT infrastructure.

These policies should maintain current standards for mobile devices. If the security policy is implemented and enforced, device reuse and disposal become a natural extension. Privacy for the information stored in the various components of a typical mobile device must be considered per the required and addressable HIPAA technical controls.

Access Control and Authentication

Access control addresses the levels of privileges granted to system resources. Authentication is based upon verifying the unique identity of a user through something the user knows, has, or is (such as a password, token, or retinal scan).

HIPAA requires that controls restrict PHI access to properly authenticated, authorized individuals only and only when required by a business need. The determination of who has access to what information is a function of organizational policy, and the organization's rules of access should be tailored to fit its particular situation.

The requirement supports emergency access control. As such, the security policy must support a solution for authorized users who have forgotten or lost an authentication mechanism such as a password or keycard. One consideration is implementing a secure form of two-factor authentication, which requires at least two authentication forms, such as a password and a keycard.

This differs from traditional password authentication, which requires only one authentication factor in order to gain

access to a system. Auditing and logging software used in conjunction with devices such as token authenticators provides this type of automatic logging.

Audit Control

A mechanism must exist to record and review mobile device activity so that individuals can be held accountable for their actions. The logging activity must be such that activities can be traced to the device and the user.

Transmission Control

Technical security measures must protect against intrusion or unauthorized access when data and information are being transmitted. Data and information transmitted and stored in an encrypted form are much less likely to be exploited. To comply with HIPAA, strong encryption such as 256-bit symmetric encryption must be implemented.

Use, Reuse, and Disposal

With implemented change management policies and procedures in place, the IT department should maintain a current standard image for each issued mobile device, know to whom each device has been issued, and regularly review audit logs and report anomalies.

If the device is to be reissued to an individual with identical access rights, the current SIM card can be removed from the device and destroyed and a new SIM card issued. There may be no reason to reimage the device. If flash cards are authorized, the contents of the flash drive should reflect the access parameters and may not need to be erased.

Still, the HIPAA privacy rule provides that the organization must reasonably safeguard PHI to prevent intentional or unintentional use or disclosure that is in violation of the privacy rule. With the amount of inadvertent PHI that may be viewed, the organization is best served by removing, destroying, and reissuing a new SIM card and erasing and reimaging the device as well as the flash drive when applicable.

If the device is to be reissued to an individual with different access rights, the SIM card must be removed and destroyed, and the device must be erased and reimaged with the current standard image. A flash card must be erased, overwritten, or totally destroyed.

If the device is to be disposed, the SIM card and flash memory (if applicable) must be removed from the device and destroyed. In order to positively ensure destruction of the mobile device, the device must be dissembled. The memory chip(s) or the hard drive must then be desoldered or physically removed, smashed, or otherwise destroyed.

Threats against the security and privacy of PHI are real. Personal information is a commodity that is readily bought and sold. Unfortunately, criminals go so far as to hack into hospital databases in order to obtain the Social Security numbers of newborns.

The development of forms, policies, and procedures is required to establish the compliance framework for the HIPAA privacy and security rules and provide a baseline for security. Although this article provides an overview, it is recommended that healthcare organizations consult with HIPAA professionals and legal counsel on the development of policies and agreements required by HIPAA.

References

Ali Pabrai, Uday O. *HIPAA Certification: Professional 2nd Edition*. Boston: Thomson Learning, 2003.

Ali Pabrai, Uday O. *HIPAA Certification Security Specialist 2nd Edition*. Boston: Thomson Learning, 2003.

Chadwick, David W. "An X.509 Role-based Privilege Management Infrastructure." Available online at www.permis.org/files/article1_chadwick.pdf.

IAnywhere Solutions. "Best Practices for Mobile Application Architectures." May 2006. Available online at www.ianywheresolutions.com.

Le Bodic, Gwenael. *Mobile Messaging Technologies and Services: SMS, EMS and MMS*. West Sussex, England: John Wiley & Sons, 2003.

"RSA ACE/Server." Available online at www.securehq.com/images/rsa/AS51_DS_1103.pdf.

Willassen, Svein Y. "Evidence in Mobile Phone Systems." (Synthesized version of the paper "Forensic Analysis of Mobile Phone Internal Memory," presented at the Conference of Digital Forensics in Orlando, FL, 2005.)

Wilson, Tim. "Stolen Data's Black Market." September 7, 2006. Available online at www.darkreading.com/document.asp?doc_id=103198.

***Laurie Southerton** (laurie.southerton@gmail.com) is a private consultant for security analysis.*

Article citation:
Southerton, Laurie. "Mobile Device Use, Reuse, and Disposal." *Journal of AHIMA* 78, no.6 (June 2007): 68-70.

Assessment Quiz – *Record Retention and Destruction*

To earn continuing education credit of one (1) AHIMA CEU, Fast Facts Audio Seminar listeners must also complete this 10-question quiz. This CE credit is for attending the audio seminar AND completing this quiz. Please **keep a copy** of the completed quiz with your certificate of attendance. **Do not send a copy to AHIMA.**

1. Which of the following is not a consideration when planning length of time medical records are retained?
   a. Accreditation requirements b. State laws
   c. Resources d. HIPAA

2. The information systems department has asked you how long they need to retain the Master Patient Index. What will you tell them?
   a. 10 years b. 5 years
   c. 25 years d. Permanently

3. Degaussing is the destruction method most commonly used for:
   a. paper records b. electronic data
   c. microfilm d. hybrid records

4. You are explaining to a student what the legal medical record is. Which of the following statements would you use in your explanation?
   a. the legal medical record is the documents stored in the medical record folder
   b. the legal medical record includes clinical pathways
   c. the legal medical record includes all documentation specific to an individual and may be stored in any media
   d. the legal medical record is equivalent to the personal health record

5. I am purging records for destruction. The record that I am evaluating has records from 15 years ago, 10 years ago, and 1 year ago. Which of the following statements is true?
   a. destroy the records from 15 years ago
   b. destroy the records from 10 years ago
   c. destroy the records from 10 and 15 years ago
   d. do not destroy any records since the patient is still active

6. We are experiencing a shortage of space to file medical records. As a result, we have decided to hire a company to store the records off-site. Which of the following statement(s) is(are) true?
   a. we need to have a signed business associate agreement
   b. the vendor must protect the privacy and security of the records [continued →]
   c. the vendor must hire a credentialed health information manager
   d. both a and b

7. Bob has filed a law suit against the facility because his records were destroyed. He wants to know what you were covering up. Which concept will protect the facility?
   a. The destruction was made in the normal course of business.
   b. Bob's records were only a few days from our 10 year retention so we decided to go ahead and shred it while we were purging records.
   c. The destruction vendor should have caught the error.
   d. We do not know what happened to the records.

8. I have developed the policy and procedure related to retention of Acknowledgement of Notice of Privacy Practices. In the policy, I stated that the acknowledge statement should be retained for 5 years. Which of the following statements is true?
   a. This statement is accurate based on HIPAA.
   b. The statement is inaccurate since they should be retained 10 years according to HIPAA.
   c. The statement is inaccurate since they should be retained 6 years according to HIPAA.
   d. It does not matter how long I keep it since it is a facility decision.

9. Pediatric records should be retained:
   a. For the same period as adult patients
   b. Until the age of majority plus state statute of limitations
   c. Until the age of majority
   d. Permanently

10. I have been asked to write a policy and procedure regarding what belongs and what does not belong in the legal medical record. In my list of what belongs in the medical record, I would include all of the following except:
    a. birth certificate
    b. email between patient and provider
    c. discharge summary
    d. video of surgery performed on patient

Do not send a copy of completed quizzes to AHIMA. Please keep them with your certificate of attendance, for your records. Be sure to sign-in and complete your evaluation form, to receive your certificate, at **http://campus.ahima.org/audio/fastfactsresources.html**.

AHIMA FASTfacts audio seminars

ANSWERS to this quiz are found on the last page of the seminar resource book, *Practical Tools for Seminar Learning*.

AHIMA Distance Education
Career-building Resources

To receive your

CE Certificate

visit
http://campus.ahima.org/audio/fastfactsresources.html

click on the link to
"**Sign In and Complete Online Evaluation**"
listed for this seminar.

You will be automatically linked to the
CE certificate for this seminar after completing the evaluation.

Each participant expecting to receive continuing education credit must complete the online evaluation and sign-in information, in order to view and print the CE certificate.

Quiz Answer Key

Fast Facts Audio Seminar: ***Record Retention and Destruction***

1: d; 2: d; 3: b; 4: c; 5: d; 6: d; 7: b; 8: c; 9: b; 10: a

Do not send a copy of your completed Fast Facts Audio Seminar quiz to AHIMA.
Please keep it with your certificate of attendance, for your records.