

EHR: Authentication of Entries

Audio Seminar/Webinar
May 15, 2007

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.

As a provider of continuing education the American Health Information Management Association (AHIMA) must assure balance, independence, objectivity and scientific rigor in all of its endeavors. AHIMA is solely responsible for control of program objectives and content and the selection of presenters. All speakers and planning committee members are expected to disclose to the audience: (1) any significant financial interest or other relationships with the manufacturer(s) or provider(s) of any commercial product(s) or services(s) discussed in an educational presentation; (2) any significant financial interest or other relationship with any companies providing commercial support for the activity; and (3) if the presentation will include discussion of investigational or unlabeled uses of a product. The intent of this requirement is not to prevent a speaker with commercial affiliations from presenting, but rather to provide the participants with information from which they may make their own judgments.

Faculty

Deborah Kohn, MPH, RHIA, CHE, CPHIMS

Deborah Kohn is the principal of Dak Systems Consulting, a national healthcare information technology advisory consultancy. Deborah has over twenty-five years of healthcare provider organization management and information technology experience.

Since founding Dak in 1985, Deborah has earned a national reputation for her expertise in strategically architecting component technologies of Electronic Health Record systems. She has published numerous articles on healthcare delivery and information systems. Also, she is a sought-after speaker on EHR systems as they relate to health information exchange initiatives, document management technology, diagnostic image management technology, Internet technologies, and other healthcare information technology applications.

Deborah is a Registered Health Information Administrator (RHIA) with undergraduate degrees from The Ohio State University and a graduate degree from UCLA in Health Services and Hospital Administration.

Deborah is board certified in healthcare management (a Certified Healthcare Executive - CHE) and a Diplomate of the American College of Healthcare Executives (ACHE). She is certified in healthcare information systems (a Certified Professional in Healthcare Information and Management Systems - CPHIMS) and a Fellow of the Healthcare Information and Management Systems Society (HIMSS). She is an active member of the American Health Information Management Association (AHIMA) and the Association for Information and Image Management International (AIIM).

Deborah has served on several AHIMA and HIMSS committees, such as AHIMA's EHR Practice Council, and she is a current member of AIIM / ASTM's PDF for Healthcare Working Group. In addition, Deborah serves as a "resource" to CalRHIO, an umbrella organization that brings together common governance, operational process, technology, and financing elements required for forming and sustaining RHIOs in California. From 1998-2001, Deborah served on the state of California's Committee to Advance Patient Safety, Privacy and Care.

Cheryl E. Servais, MPH, RHIA

Ms. Servais is VP, Compliance and Privacy Officer at Precyse Solutions. She has more than 20 years of experience in Health Information Management. At Precyse, Servais' responsibilities include planning, designing, implementing and maintaining corporate-wide compliance programs, policies and procedures, and updating them to accommodate changes in federal and other regulations; overseeing training and development programs related to ethics, compliance and patient privacy; developing and chairing compliance and privacy advisory committees at the Executive and Board levels; and taking an active role in professional organizations.

Ms. Servais has proven expertise in a wide range of HIM-related areas, including product development and marketing strategies, system analysis and installation,

Faculty

operations improvement and re-engineering, electronic medical record project management, DRG and data quality analysis and education, compliance strategies, and clinical database management. Servais most recently established HIM Consulting Services, which provided a variety of services to various HIM consulting companies and was also associated with Atlanta-based eWebCoding/InterTech as a consultant and Domain Expert. Prior to that Servais held increasingly responsible positions with Tenet Healthcare, ultimately serving as the company's manager of Health Information Services. She also established a successful HIM consulting business, Servais Holloway & Associates, and served as one of its principals. Other past experience includes medical records management at three California hospitals and research at UCLA's School of Public Health.

Ms. Servais holds a B.S. in Health Records, and an M.P.H. in Health Information Systems from UCLA. Her many professional accomplishments include authoring several published columns, manuals and papers, and developing and teaching courses for both colleges and professional associations.

Table of Contents

Disclaimer	i
Faculty	ii
Learning Objectives.....	1
Definitions	
Authorship.....	2
Authentication.....	2
Non-repudiation	3
Signatures	3-4
Analog vs. Digital Signatures	4
Handwritten vs. Stamped Signatures.....	5
Polling Question #1.....	5
Definitions (cont'd)	
Different Forms of Digital Signatures.....	6
eSignature.....	6-7
Digital Signature.....	7
There Are Many Digital Signature Standards	8
Public Key Infrastructure (PKI)	8
Digitized Signature	9
Polling Question #2.....	9
eSignatures – Pros and Cons.....	10
Digital Signatures – Pros and Cons	10
Digitized Signatures – Pros and Cons	11
Issues Legal, Regulatory, Standards	
Federal Laws: Conditions of Participation.....	11-12
Federal Laws: HIPAA	13
Federal Laws: Electronic Signatures in Global and Nat'l Commerce Act.....	13
State Laws.....	14
Joint Commission	14
ASTM	15
Tips and Cautions	
Document Lockdown	15
Document Lockdown: Pros and Cons	16
Auto-authentication	17
Usage Controls/Audit Trails	17-18
Date/Time	18-19
Multiple eSignature Applications.....	19-21
Polling Question #3.....	21

(CONTINUED)

Table of Contents

Implementation Tips	
Implementation is its own project	22
Get a champion.....	22
Phase in the implementation	23
Select a pilot area that sees the advantage.....	23
Documentation editing plus eSignature	24
Train in small groups	24
Have standard configuration/set-up template.....	25
Be sure to have extra Help Desk support	25
Plan for retraining and ongoing training.....	26
Resource/Reference List	26-27
Audience Questions.....	28
Audio Seminar Discussion and Audio Seminar Information Online.....	28
Upcoming Audio Seminars	29
AHIMA Distance Education online courses	30
Thank You/Evaluation Form and CE Certificate (Web Address)	30
Appendix	31
Resource/Reference List	32
CE Certificate Instructions	

Learning Objectives

- ♦ **Define and describe what is meant by authentication of medical record entries**
- ♦ **Review how one can be sure that Electronic Health Record (EHR) entries are authenticated**
- ♦ **Review the legal aspects related to the authentication of EHR entries**

1

Learning Objectives

- ♦ **Provide awareness of issues related to authentication of electronic documents**
- ♦ **Obtain tips for a successful implementation of an eSignature system**

2

Definitions



♦ What is meant by Authorship?

“The origin of recorded information that is attributed to a specific individual or entity.”

AHIMA eHIM® Workgroup: Guidelines for EHR Documentation Practice. “Guidelines for EHR Documentation to Prevent Fraud” *Journal of AHIMA* 78, no 1 (Jan 2007): 65-68

3

Definitions



♦ What is meant by Authentication?

“The process that ensures that users are who they say they are. The aim is to prevent unauthorized people from accessing data or using another person’s identity to sign documents.”

AHIMA Practice Brief: Implementing Electronic Signatures

4

Definitions



♦ What is meant by **Non-repudiation**?

“The ability to ensure that a party to a communication cannot deny the authenticity of his or her signature on a document or the sending of a message that he or she originated.”

AHIMA Practice Brief: Implementing Electronic Signatures

5

Definitions



♦ What is meant by a **Signature**?

A **signature** identifies the author or the responsible party who takes ownership of and attests to the information contained in a record entry or document.

6

Definitions

- ♦ **Signatures** are the usual method for authenticating most medical record entries/documents.
 - Signatures address legal and regulatory requirements.
 - Signatures affirm the truth of the information in the entry/document.

7

Definitions

- ♦ What are some acceptable types of signatures for authenticating most medical record entries/documents?
 - **Analog** name/initials applied to paper or stone storage media
 - **Digital** name/initials applied to electronic storage media, such as magnetic disk

8

Definitions

- ♦ What are some acceptable types of **analog signatures** for authenticating most medical record entries/ documents?



- Handwritten signatures
- Stamped signatures

9

Polling Question #1

For **analog signatures**:

- *1 Only handwritten signatures are allowed for authenticating our paper medical record entries/documents.
- *2 Both handwritten and stamped signatures are allowed for authenticating our paper medical record entries/documents.
- *3 Not applicable



10

Definitions

- ♦ The terminology regarding **digital signatures** has been used rather loosely.
- ♦ The following terms distinguish various forms of **digital signatures**.
 - eSignatures
 - Digital signatures
 - Digitized signatures



11

Definitions

- ♦ What is meant by an **eSignature**?
 - Narrowly defined, an **eSignature** is the application of a password or other form of electronic authentication to an electronic document.
 - The term **eSignature** is often used to describe the signing of
 - transcribed dictation
 - orders in a computerized provider order entry (CPOE) system

12

Definitions

- ♦ An **eSignature** can be strengthened from only using a password or other form of electronic authentication to an electronic document by adding a token (such as an ID card) or a biometric device to the authentication process.
 - This is called two-tiered eSignature authentication.

13

Definitions

- ♦ What is meant by a **Digital Signature**?
 - A **digital signature** is a cryptographic signature (a digital key) that authenticates the user, provides non-repudiation, and ensures message integrity.
 - This is the strongest form of a digital signature because it protects the signature by a type of “tamper-proof seal” that breaks if the content were to be altered.

14

Definitions

- ♦ There are many **digital signature** standards.
 - The federal government uses the Digital Signature Standard (DSS), which enables the use of the Rivest-Shamir-Adleman (RSA) digital signature algorithm to digitally sign a message.
 - The RSA algorithm is the most popular.
 - It is used in most web browsers with the Secure Sockets Layer (SSL) protocol, the standard security protocol for establishing an encrypted link between a web server and a web browser.

15

Definitions

- ♦ Public Key Infrastructure (PKI) is neither a **digital signature** nor a **standard**.
 - It is an entire infrastructure of computer programs, procedures, data formats, communication protocols, security policies and public key cryptography.

16

Definitions

- ♦ What is meant by a **Digitized Signature**?
 - A **digitized signature** is an applied image of a handwritten signature
 - This is the weakest form of a digital signature because someone could acquire a copy of the image of a handwritten signature and forge an electronic document.

17

Polling Question #2



For **digital signatures**:

- *1 **eSignatures** are used for authenticating most of our electronic medical record entries /documents
- *2 **Digital signatures** are used for authenticating most of our electronic medical record entries/documents
- *3 **Digitized signatures** are used for authenticating most of our electronic medical record entries/documents
- *4 Not applicable

18

eSignatures – Pros and Cons

♦ eSignatures

• Pros

- Easy to use
- Only need password



• Cons

- Passwords can be shared
- Some systems do not require authors to review all documentation prior to eSigning (i.e., allowing for blanket signatures)

19

Digital Signatures – Pros and Cons

♦ Digital Signatures

• Pros

- Most secure option

• Cons

- Most difficult to implement
- Most costly



20

Digitized Signatures – Pros and Cons

♦ **Digitized Signatures**

- **Pros**
 - Looks like a real, handwritten signature
 - Easy to implement
- **Cons**
 - Least secure option



21

Issues: Legal, Regulatory, Standards

♦ **Federal Laws**

- **Conditions of Participation**
 - **New Rules (Nov/Dec 2006)**

“All medical record entries must be legible, dated, timed, and authenticated in written or electronic form by the person responsible for providing or evaluating a service provided.”

22

Issues:

Legal, Regulatory, Standards

♦ **Federal Laws**

• **Conditions of Participation**

• **Authentication of orders**

- "...all orders, including verbal orders, must be dated, timed and authenticated by the ordering practitioner or another practitioner who is responsible for the care of the patient...."
- "All verbal orders must be authenticated based upon federal and state law. If there is no state law that designates a specific timeframe for authentication of verbal orders, verbal orders must be authenticated within 48 hours."

23

Issues:

Legal, Regulatory, Standards

♦ **Federal Laws**

• **Conditions of Participation (Response)**

"Authentication of a verbal order may occur in writing or electronically. The hospital must have a method to establish the identity of the practitioner who has authenticated a verbal order. Hospital policies should address author verification process for both written and electronic signatures."

24

Issues:
Legal, Regulatory, Standards

- ♦ **Federal Laws**
 - **HIPAA (PL 104-191)**
 - **Originally had standards for electronic signatures**
 - **No standards in final Rule**

25

Issues:
Legal, Regulatory, Standards

- ♦ **Federal Laws**
 - **Electronic Signatures in Global and National Commerce Act**
 - **Enacted to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.**
 - **Pub. L. No. 106-229, 114 Stat. 464 (2000)**
(codified at 15 U.S.C. § 7001 *et seq.*)

26

Issues:
Legal, Regulatory, Standards

♦ **State Laws**

- **Vary widely**
 - **AHIMA Practice Brief: Implementing Electronic Signatures contains an Appendix with a State-by-State Review of Regulations Pertaining to Electronic Signature**
 - **In some states, providers may be able to obtain a variance from licensing authorities.**

27

Issues:
Legal, Regulatory, Standards

♦ **Joint Commission**

- **IM 6.10 of CAMH**
 - **Entries may be authenticated "by written signatures or initials, by rubber-stamp, or computer key."**
 - **"The practitioner must sign a statement that he or she alone will use it."**
 - **eSignatures are OK for ambulatory care, home care, long term care, and mental health care**

28

Issues:

Legal, Regulatory, Standards

- ◆ **ASTM**
 - The ASTM "STANDARDS FOR SECURITY AND ELECTRONIC SIGNATURES IN HEALTHCARE " contain standards for electronic signatures.

29

Tips and Cautions



- ◆ **Document Lockdown**
 - Some EHR or eSignature systems do not allow authors to make changes to a text document or data entry screen once an eSignature has been affixed to or embedded into a document.

30

Tips and Cautions



◆ Document Lockdown – Pros

- Ensures that the data/documentation are not altered after authentication
- Preserves integrity of signed document or data
- Might require author to have the ability to edit as well as sign documents

31

Tips and Cautions



◆ Document Lockdown – Cons

- Difficult to correct errors:
 - Must use an addendumOR
 - “Unsign” the document (requires the author to remove the eSignature, make the correction, and then “resign” the document)
- Author might not bother to correct errors

32

Tips and Cautions

- ◆ **Auto-authentication**
 - Must require an author to review the entry before authenticating
 - Failure to do so may place the organization at legal risk due to failure to meet federal or state requirements for each entry to be authenticated

33

Tips and Cautions

- ◆ **Usage Controls/Audit Trails**
 - If digital signatures are used in the EHR, the software program or technology should provide
 - *the message integrity*
(i.e., the assurance that the message sent or entry made by a user is the same as the one received or maintained by the system)
 - *the non-repudiation*
(i.e., the assurance that the entry or message came from a particular user)

34

Tips and Cautions

◆ Usage Controls / Audit Trails

- Audit trails may include one or more of the following:
 - An electronic file or hardcopy report (real time or batch processed) of
 - Transactions and activities (e.g., data creation /access/revision, with date and time)
 - Data transmissions or interfaces
 - Exceptions of unauthorized access attempts

35

Tips and Cautions

◆ Date/Time

- In association with the signature, every entry in the EHR must include a complete date (month, day, year [xxxx]) and a time (e.g., military hour, minute, time zone if necessary)



36

Tips and Cautions

◆ Date/Time

- EHR systems must have the ability to generate a date and time as the entry is made.
- EHR systems must have the ability for the author to generate a date and time of occurrence for late entries.



37

Tips and Cautions

◆ Multiple eSignature Applications

- Multiple text (transcription) systems with eSignature capabilities
- Multiple speech systems with eSignature capabilities
- CPOE systems with eSignature capabilities
- Clinical documentation systems with eSignature capabilities

38

Tips and Cautions

- ◆ **Multiple eSignature Applications**
 - With IT, try to consolidate these multiple eSignature applications, similar to trying to consolidate multiple voice/text systems
 - Depending on the number and type of users, some of these multiple systems can be eliminated/phased out over time.
 - This process requires extensive systems analysis and change management/planning.

39

Tips and Cautions

- ◆ **Multiple eSignature Applications**
 - This might require the development of a “single eSignature capability” similar to the development of a “single sign-on capability”.
 - Might be similar to an “umbrella-type” application that “masks” some of the existing capabilities

40

Tips and Cautions

♦ Multiple eSignature Applications

- If a “single eSignature capability” is not practical:
 - Keep the individual eSig applications in the source systems (e.g., eSigning radiology result reports in the RIS)
 - Upload the various signed reports to the EHR
 - Maintain the integrity of the eSig process!

41

Polling Question #3

Have you implemented an eSignature application?

- *1 Yes**
- *2 No**
- *3 Not applicable**



42

Implementation Tips

- ◆ **Implementing eSignature software is its own project**
 - Not part of new transcription system training
 - Not part of CPOE training
- ◆ **Requires specific templates, training, login and password setup**

43

Implementation Tips

- ◆ **Get a Champion (MD)**
 - Not a TechnoGeek
 - Someone willing to use the system
 - Someone willing to communicate and encourage other practitioners



44

Implementation Tips

- ♦ **Phase in the Implementation**
 - **Better than doing it all at once**
 - **Phase in by**
 - **Specific area (Diagnostic Service or ED)**

OR

- **Certain reports**

OR

- **Certain MDs (e.g., volunteers)**

45

Implementation Tips

- ♦ **Select a pilot area that sees the advantage to eSignature**
 - **Rehab might not have enough volume or intensity to see eSignature as an advantage.**
 - **ED is good because of volume and intensity.**

46

Implementation Tips

◆ Documentation Editing plus eSignature

- Allowing end-users to be able to edit as well as sign documents requires more training and technical sophistication on the part of the end-users.
- Must be able to edit accurately

47

Implementation Tips

◆ Train in small groups



- One-on-one is best
- Train trainers so that many people are available to assist MDs
- If possible, provide hands-on training

48

Implementation Tips

- ◆ **Have standard configuration/set-up template for all PCs and laptops**
 - Reduces issues related to incorrect set-up
 - Makes it easier for training and technical support group

49

Implementation Tips

- ◆ **Be sure to have extra Help Desk support for the first few weeks**
 - Drill down to actual reason for complaint
 - “System doesn’t work”
 - isn’t enough information
 - Might be simple a solution
 - e.g., “caps lock on” when doing login

50

Implementation Tips

- ◆ **Plan for retraining**
- ◆ **Plan for ongoing training for new staff**
 - **Ideal is web demo and training so new users can train themselves**
- ◆ **Plan for retraining for system enhancements**

51

Resource/Reference List

- **AHIMA Practice Brief: Authentication of Health Record Entries (2000)**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_000040.hcsp

- **AHIMA Practice Brief: Verbal/Telephone Order Authentication and Time Frames (2001)**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_000032.hcsp

52

Resource/Reference List

- **AHIMA Practice Brief: Implementing Electronic Signatures (2003)**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021585.hcsp

- **AHIMA Practice Brief: Maintaining a Legally Sound Health Record—Paper and Electronic (2005)**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028509.hcsp

53

Resource/Reference List

- **Article e-HIM[®] Work Group: Guidelines for EHR Documentation Practice. "Guidelines for EHR Documentation to Prevent Fraud." *Journal of AHIMA* 78, no.1 (January 2007): 65-68.**

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033097.hcsp

54

Audience Questions



Audio Seminar Discussion



***Following today's live seminar
Available to AHIMA members at
www.AHIMA.org***

*"Members Only" Communities of Practice (CoP)
AHIMA Member ID number and password required*

Join the [e-HIM Community](#) from your Personal Page. Look under Community Discussions for the ***Audio Seminar Forum***

You will be able to:

- discuss seminar topics
- network with other AHIMA members
- enhance your learning experience

AHIMA Audio Seminars

Visit our Web site

<http://campus.AHIMA.org>

for information on the
2007 seminar schedule.

While online, you can also register
for seminars or order CDs and
Webcasts of past seminars.



Upcoming Audio Seminars

- ♦ **Benchmarking:
HIM Processes**
May 22, 2007
- ♦ **Pay for Performance**
July 12, 2007
- ♦ **Amending Closed
Health Records**
August 9, 2007

AHIMA Distance Education

Anyone interested in learning more about e-HIM[®] should consider one of AHIMA's **web-based training courses**.

For more information visit
<http://campus.ahima.org>

Thank you for joining us today!

Remember – visit the AHIMA Audio Seminars Web site to complete your evaluation form and receive your CE Certificate online at:

<http://campus.ahima.org/audio/2007seminars.html>

Each person seeking CE credit must complete the **sign-in form** and **evaluation** in order to view and print their CE certificate.

Certificates will be awarded for AHIMA CEUs and ANCC Contact Hours.



Appendix

Resource/Reference List	32
CE Certificate Instructions	

Resource/Reference List

AHIMA Practice Briefs

Authentication of Health Record Entries (2000)

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_000040.hcsp

Verbal/Telephone Order Authentication and Time Frames (2001)

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_000032.hcsp

Implementing Electronic Signatures (2003)

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021585.hcsp

Maintaining a Legally Sound Health Record—Paper and Electronic (2005)

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028509.hcsp

AHIMA Journal Article

"Guidelines for EHR Documentation to Prevent Fraud." *Journal of AHIMA* 78, no.1 (January 2007): 65-68.

e-HIM[®] Work Group: Guidelines for EHR Documentation Practice.

http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033097.hcsp



To receive your

CE Certificate

Please go to the AHIMA Web site

<http://campus.ahima.org/audio/2007seminars.html>

click on

"Complete Online Evaluation"

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 after the seminar, in order to view and print the CE certificate.