HIPAA Security Regulations: Audit Trails

One Look at What The Rule Expects

Second National HIPAA Summit

March 1, 2001

Concurrent Session # 203

Climate of Confidentiality

- Unwritten cornerstone of the proposed Security rule
  - And its “companion” Privacy final rule
- Audit trails have a technology and a human component
- Technology may prove easier to implement
- But people make it all work

Guidance from the Security NPRM

- Proposed rule does not provide an exact definition for either ‘audit trail’ or ‘audit control’
- Focus is on the expected outcome, the “what”
  - “How” is the covered entity’s responsibility
- Covered entities must put in place whatever mechanisms are deemed necessary

Expected outcomes

- Enable the organization to record and examine system activity
- So that an organization can identify suspect data activity
- See if high-risk patterns are present
- Assess its security program
- Respond to potential weaknesses

Implementation considerations and issues

- Each health care entity is required to establish its own process to ensure compliance with the HIPAA Security standard
- Individual circumstances (e.g., “size”) will influence each process, of which the BIA (Business Impact Analysis) is an integral part and early step

Security and Privacy work together

- Both rules anticipate audit trails as one of the safeguards to be HIPAA compliant
- Security addresses the '**how**'; Privacy also wants to know the '**why**'
  - Audit logs will have to go beyond the simple capture of login name, date/timestamp, and action taken associated with the data that was accessed

What an audit trail should do

- Provide the ability to determine
  - Who accessed what information
  - When the information was accessed
  - What was changed
- A manual capture of audit trails would be necessary for non-electronic environments

When considering the technology component --

- Does the vendor know what HIPAA is and can it demonstrate an understanding of the rules?
- Will the vendor provide enhanced security features to meet HIPAA?
- How do the enhanced features impact the existing security foundations and applications?

Question the technology

- What types of access controls are enabled -- user, role or context-based access?
- If the Internet is used, does it have encryption and does it meet at minimum HCFA's Internet Policy?
- Can the application or system support digital certificates?

Consider the human side --

- Each covered entity is required to establish its own process to ensure compliance
  - Are the right people on the decision-making team?
- How well does management make use of audit trail information, and always act when necessary?
  - Staff must be trained, monitored and retrained as necessary

Surveillance

- Part of the “culture of confidentiality”
- Staff will be under physical and software “watch”
- Software provides the information for the auditors
- The old banking model is gone
  - No need to take 2-week vacation at one time, to give auditors time to find out if you’ve done something wrong

Closing thought

- Every organization should conduct an initial risk and exposure evaluation and baseline planning
- Focus on determining how much of the two year HIPAA implementation timeframe will be needed

Information Resources

- WEDI SNIP Security and Privacy White Paper, Version 2.0
  - www.wedi.org/snip
- Listserves
  - e.g., www.hipaalive.com
- HIPAA Summit
  - www.hipaasummit.com
- AFEHCT security self-evaluation
  - www.afehct.org/security eval.html
- CPRI Security Guidelines (“Toolkit”)
  - www.cpri.org
- NCHICA Security Questionnaire
  - www.nchica.org

Caveat emptor

Nothing included in this paper is "official." If you want or need the final word, please read the applicable laws and regulations and seek appropriate legal counsel for interpretation. This presentation is intended only as a summary of the concepts involved and as an aid in beginning to understand the material.

Enquiries?

Frank Pokorny

Co-chair (retired) WEDI SNIP Security and Privacy Work Group

Manager, Code and Third-Party Issues
American Dental Association
pokornyf@ada.org
312-440-2752