Security Audit Survivor – How to Remain "On the Island" in the Wake of the Piedmont Audit

Marc D. Goldstone
Vice President and Associate General Counsel
Community Health Systems

Gerald "Jud" E. DeLoss
Gray Plant Mooty

HHS has a Challenge for you

- Please produce the following policies and procedures….NOW!

How to Survive

- Produce policies and procedures:
  - Establishing and terminating users' access to systems housing electronic protected health information (“ePHI”).
  - Emergency access to electronic information systems.
  - Inactive computer sessions (periods of inactivity).
  - Recording and examining activity in information systems that contain or use ePHI.

HHS Challenge

- Do you have these policies and procedures?

How to Survive

- Produce these policies and procedures:
  - Risk assessments and analyses of relevant information systems that house or process ePHI data.
  - Employee violations (sanctions).
  - Electronically transmitting ePHI.
  - Preventing, detecting, containing and correcting security violations (incident reports).

HHS Challenge

- Have you got these policies and procedures?
  - Regularly reviewing records of information system activity, such as audit logs, access reports and security incident tracking reports.
  - Creating, documenting and reviewing exception reports or logs. Please provide a list of examples of security violation logging and monitoring.
  - Monitoring systems and the network, including a listing of all network perimeter devices, i.e. firewalls and routers.
  - Physical access to electronic information systems and the facility in which they are housed.

HHS Challenge

- How about these?
  - Establishing security access controls; (what types of security access controls are currently implemented or installed in hospitals' databases that house ePHI data?).
  - Remote access activity i.e. network infrastructure, platform, access servers, authentication, and encryption software.
  - Internet usage.
  - Wireless security (transmission and usage).

HHS Challenge

- More policies and procedures that you better have in place.
  - Firewalls, routers and switches.
  - Maintenance and repairs of hardware, walls, doors, and locks in sensitive areas.
  - Terminating an electronic session and encrypting and decrypting ePHI.
  - Transmitting ePHI.

HHS Challenge

- Finally (?)
  - Password and server configurations.
  - Antivirus software.
  - Network remote access.
  - Computer patch management.

Other HHS Demands

- In addition, make sure you have this information readily available.
  - Please provide a list of all information systems that house ePHI data, as well as network diagrams, including all hardware and software that are used to collect, store, process or transmit ePHI.
  - Please provide a list of terminated employees.
  - Please provide a list of all new hires.

More HHS Demands

- Please provide a list of encryption mechanisms use for ePHI.
- Please provide a list of authentication methods used to identify users authorized to access ePHI.
- Please provide a list of outsourced individuals and contractors with access to ePHI data, if applicable. Please include a copy of the contract for these individuals.

HHS Demands

- Please provide a list of transmission methods used to transmit ePHI over an electronic communications network.
- Please provide organizational charts that include names and titles for the management information system and information system security departments.
- Please provide entity wide security program plans (e.g System Security Plan).

HHS – Asking for More!

- Please provide a list of all users with access to ePHI data. Please identify each user's access rights and privileges.
- Please provide a list of systems administrators, backup operators and users.
- Please include a list of antivirus servers, installed, including their versions.

HHS Isn't Finished Yet

- Please provide a list of software used to manage and control access to the Internet.
- Please provide the antivirus software used for desktop and other devices, including their versions.
- Please provide a list of users with remote access capabilities.

Is This All HHS Needs?

- Please provide a list of database security requirements and settings.
- Please provide a list of all Primary Domain Controllers (PDC) and servers (including Unix, Apple, Linux and Windows). Please identify whether these servers are used for processing, maintaining, updating, and sorting ePHI.
- Please provide a list of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

FINISHED!

- Do you survive? It's more than a game.
- Be prepared for your organization's audit with Security Rule compliance.
- It is only going to get tougher!
  - CMS hires Price Waterhouse Coopers consulting firm to provide technical assistance with investigations
  - Who is on your side?

Questions?

- Relax, we have got your answers!
  - Marc Goldstone
    - Marc_Goldstone@chs.net
  - Gerald “Jud” DeLoss
    - Jud.DeLoss@gpmlaw.com