

PIEDMONT HOSPITAL & the First HIPAA audit:

The 42 questions HHS might ask

June 19, 2007 (Computerworld) In March, Atlanta's Piedmont Hospital became the first institution in the country **to be audited for compliance with the HIPAA security rules.**

The audit was conducted by the office of the inspector general at the U.S. Department of Health and Human Service (HHS) and is being seen by some in the health care industry as a precursor of similar audits to come at other institutions.



Neither Piedmont nor HHS officials have publicly confirmed the audit or spoken about it. That silence has sparked considerable curiosity about why Piedmont was targeted as well as the scope of the audit and the kind of information HHS was seeking.

A document obtained by *Computerworld* from a reliable source indicates that Piedmont was presented with a list of 42 items that HHS officials wanted information on within 10 days. Specifically, Piedmont was asked to provide policies and procedures for:

1. Establishing and terminating users' access to systems housing electronic patient health information (ePHI).
2. Emergency access to electronic information systems.
3. Inactive computer sessions (periods of inactivity).
4. Recording and examining activity in information systems that contain or use ePHI.
5. Risk assessments and analyses of relevant information systems that house or process ePHI data.
6. Employee violations (sanctions).
7. Electronically transmitting ePHI.
8. Preventing, detecting, containing and correcting security violations (incident reports).
9. Regularly reviewing records of information system activity, such as audit logs, access reports and security incident tracking reports.
10. Creating, documenting and reviewing exception reports or logs. Please provide a list of examples of security violation logging and monitoring.
11. Monitoring systems and the network, including a listing of all network perimeter devices, i.e. firewalls and routers.
12. Physical access to electronic information systems and the facility in which they are housed.
13. Establishing security access controls; (what types of security access controls are currently implemented or installed in hospitals' databases that house ePHI data?).
14. Remote access activity i.e. network infrastructure, platform, access servers, authentication, and encryption software.
15. Internet usage.

16. Wireless security (transmission and usage).
17. Firewalls, routers and switches.
18. Maintenance and repairs of hardware, walls, doors, and locks in sensitive areas.
19. Terminating an electronic session and encrypting and decrypting ePHI.
20. Transmitting ePHI.
21. Password and server configurations.
22. Antivirus software.
23. Network remote access.
24. Computer patch management.

HHS also had a slew of other requests:

1. 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.
2. Please provide a list of terminated employees.
3. Please provide a list of all new hires.
4. Please provide a list of encryption mechanisms use for ePHI.
5. Please provide a list of authentication methods used to identify users authorized to access ePHI.
6. 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.
7. Please provide a list of transmission methods used to transmit ePHI over an electronic communications network.
8. Please provide organizational charts that include names and titles for the management information system and information system security departments.
9. Please provide entity wide security program plans (e.g System Security Plan).
10. Please provide a list of all users with access to ePHI data. Please identify each user's access rights and privileges.
11. Please provide a list of systems administrators, backup operators and users.
12. Please include a list of antivirus servers, installed, including their versions.
13. Please provide a list of software used to manage and control access to the Internet.
14. Please provide the antivirus software used for desktop and other devices, including their versions.
15. Please provide a list of users with remote access capabilities.
16. Please provide a list of database security requirements and settings.
17. 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.
18. Please provide a list of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

Reprinted from COMPUTERWORLD, June 2007