

LISTING OF QUESTIONS/REQUESTED ITEMS – OIG HIPAA SECURITY RULE AUDIT

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.
Other Requested Items	
25	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.
26	List of terminated employees.
27	List of all new hires.
28	List of encryption mechanisms use for ePHI.
29	List of authentication methods used to identify users authorized to access ePHI.
30	List of outsourced individuals and contractors with access to ePHI data, if applicable. Please include a copy of the contract for these individuals.
31	List of transmission methods used to transmit ePHI over an electronic communications network.
32	Organizational charts that include names and titles for the management information system and information system security departments.
33	Entity wide security program plans (e.g., System Security Plan).
34	List of all users with access to ePHI data. Please identify each user's access rights and privileges.
35	List of systems administrators, backup operators and users.
36	List of antivirus servers, installed, including their versions.
37	List of software used to manage and control access to the Internet.

38	Antivirus software used for desktop and other devices, including their versions.
39	List of users with remote access capabilities.
40	List of database security requirements and settings.
41	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.
42	List of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

Sources: Multiple, Unofficial Listing of Audit Questions/Requests

Davis/HCCA/OIG Audit Questions