

HIPAA Technical Safeguards

January 1

2007

This document includes reference material and information extracted for publicly available information related to HIPAA compliance and associated guideline materials. This information is subject to change and may not be 100% accurate. This information is provided for information purposes only and does not constitute a legal contract between the Level 4 and any person or entity unless otherwise specified.

Self
Assessment
Questions

Contents

Technical Safeguards	3
Access Control - 164.304.....	3
Emergency Access - 164.312(a)(2)(ii).....	3
Automatic Logoff - 164.312(a)(2)(iii)	3
Encryption and Decryption - 164.312(a)(2)(iv)	4
Integrity - 164.312(c)(1)	4
Person or Entity Authentication - 164.312(d).....	5
Transmission Security – 164.312(e)(1).....	6
Integrity Controls (A) -	6
Encryption (A) -	6

Technical Safeguards

The Security Rule defines technical safeguards in 164.304 as *“the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”*

Access Control - 164.304

1. Does each workforce member have a unique user identifier?
2. What is the current format used for unique user identification?
3. Can the unique user identifier be used to track user activity within information systems that contain EPHI?

Emergency Access - 164.312(a)(2)(ii)

1. Who needs access to the EPHI in the event of an emergency?
2. Are there policies and procedures in place to provide appropriate access to EPHI in emergency situations?

Automatic Logoff - 164.312(a)(2)(iii)

1. Do current information systems have an automatic logoff capability?
2. Is the automatic logoff feature activated on all workstations with access to EPHI?

Encryption and Decryption - 164.312(a)(2)(iv)

1. Which EPHI should be encrypted and decrypted to prevent access by persons or software programs that have not been granted access rights?
2. What encryption and decryption mechanisms are reasonable and appropriate implement to prevent access to EPHI by the persons or software programs at have not been granted access rights?

Audit Controls - 164.312(b)

1. What audit control mechanisms are reasonable and appropriate to implement as to record and examine activity in information systems that contain or use EPHI?
2. What are the audit control capabilities of information systems with EPHI?
3. Do the audit controls implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specifications at 164.308 (a) (1) (ii) (D) for information System Activity Review?

Integrity - 164.312(c)(1)

1. Do existing information systems have the availability functions or processes that automatically check for data integrity such as check sum verification or digital signatures?
2. Are electronic mechanisms to protect the integrity of EPHI currently used?

Person or Entity Authentication - 164.312(d)

1. What types of authentication mechanisms are currently used?
2. What level or type of authentication is reasonable and appropriate for each information system with EPHI?
3. Are other authentication methods available that may be reasonable and appropriate?

Transmission Security – 164.312(e)(1)

Integrity Controls (A) - 164.312(e)(2)(i)

1. What security measures are currently used to protect EPHI during transmission?
2. Has the risk analysis identified scenarios that may result in modifications to EPHI by unauthorized sources during transmission?

Encryption (A) - 164.312(e)(2)(ii)

1. How does the organization transmit EPHI?
2. How often does the organization transmit EPHI?
3. Based on the risk analysis, is encryption needed to protect EPHI during transmission?
4. What methods of encryption will be used to protect the transmission of EPHI?