

Items to discuss with your EPHI systems data manager or provider

Administrative Safeguards:

Information Systems Activity Review: **R** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Is this type of information available from your system?

_____ If so, what information can be provided and what reports can you receive to review? Examples of adequate reports will contain information that will allow you to understand who is accessing data when, who is attempting to access data that they are not authorized to access, changes that are made to the system and who made changes. Collect sample reports.

_____ If not, can the system be modified to provide this type of information?

_____ If so, how long will it take and at what cost?

_____ If not, reconsider the use of the system, it is not HIPAA compliant.

Technical Safeguards:

Unique User ID: **R** Your system must include the assignment of a unique name and/or number for identifying and tracking user identity.

_____ If so, ensure each user is provided with a unique ID and that they use only that ID when accessing the system. IDs can not be shared.

_____ If not, can the system be modified to provide allow for assigned unique ID's?

_____ If so, how long will it take and at what cost?

_____ If not, reconsider the use of the system, it is not HIPAA compliant.

Audit Controls: **R** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. What is available in your system?

_____ If controls are available in your system, implement procedures for review.

_____ If nothing is build-in, are their third party tools that can extract the information and provide reports?

_____ If so, what do they cost, what is required for implementation, how long will it take and at what cost?

_____ If not, reconsider the use of the system, it is not HIPAA compliant.

Person or Entity Authentication: **R** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. Must be a) something a person knows such as a password, b) something a person is in possession of such as a token (smart card, ATM card etc.) c) some type of biometric device, 4) a combination of two or more of the above. How will you do this in your system?

_____ If controls are authentication procedures are available in your system, ensure they are implemented.

_____ If nothing is build-in, are their third party authentication mechanisms available that can be used for authentication?

_____ If so, what do they cost, what is required for implementation, how long will it take and at what cost?

_____ If not, reconsider the use of the system, it is not HIPAA compliant.

Login Monitoring: **A** Does your system allow for monitoring of log-in attempts and reporting of discrepancies.

_____ If so, identify procedures for monitoring records and reporting of discrepancies.

_____ If not, can the system be modified to allow for monitoring?

_____ If so, how long will it take and at what cost?

_____ If not, reconsider the use of the system

or

_____ Mark as an addressable item and be prepared to document and implement a reasonable alternative.

Password Management: A Does your system allow for creating, changing and safeguarding passwords?

_____ If so, ensure that all users are managing passwords and that they are refreshed at least every 60 days.

_____ If not, can the system be modified to allow for passwords?

_____ If so, how long will it take and at what cost?

_____ If not, reconsider the use of the system

or

_____ Mark as an addressable item and be prepared to document and implement a reasonable alternative.