Technical Safeguards

Date: 5/1/2018

Author: Aaron Picton

164.312(a)(1)

Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).

Noble has technical policies and procedures that only allow access to information to individuals that have been granted such access.

164.312(a)(2)(i)

Have you assigned a unique name and/or number for identifying and tracking user identity? (R)

Yes, all users have a unique user name for tracking and identifying user identity.

164.312(a)(2)(ii)

Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during and emergency? (R)

We have a security incident policy, but don't have any information for obtaining necessary EPHU during an emergency, as we have no need to access EPHI in an emergency.

164.312(a)(2)(iii)

Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)

By default, the system will attempt to keep sessions alive for users, however we also expect that local workstation policy will control access as well. In onsite configurations, the system can be controlled for session time.

164.312(a)(2)(iv)

Have you implemented a mechanism to encrypt and decrypt EPHI? (A)

Not for data at rest, but for information that is in transit, yes (SSL with 2048-bit certificates).

164.312(b)

Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)

The system implements audit controls at the database level to examine activity with all data in the system, not just identified EPHI.

164.312(c)(1)

Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.

Noble has policies and procedures to protect all data from improper alteration or destruction. Principally this is done by limiting access to only those individuals with a job-duty need to access customer data, ensuring that those individuals are suitably trained, and ensuring the application and database employ suitable safeguards to ensure data cannot be improperly accessed, altered, or destroyed. Furthermore, the system employs auditing to ensure that any additions, alterations, or destruction of data can be cross-checked for authorization should the need arise.

164.312(c)(2)

Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)

Noble uses audit tables within the database to determine if changes to data, including EPHI data has been altered or destroyed. This information can be corroborated with other data within the organization to determine if such changes were authorized.

164.312(d)

Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed? (R)

Noble takes steps to ensure that anyone accessing data is the person claimed. Access to the application itself, however, is handled by the customer agency, and such measures would be handled by the client.

164.312(e)(1)

Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

Noble uses 2048-bit SLL certificates to encrypt all data being transmitted to guard against interception and manipulation of data.

164.312(e)(2)(i)

Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)

Noble uses 2048-bit SLL certificates to encrypt all data being transmitted to guard against interception and manipulation of data.

164.312(e)(2)(ii)

Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)

Noble uses 2048-bit SLL certificates to encrypt all data being transmitted to guard against interception and manipulation of data. This does not apply to data at rest, which is not encrypted currently, as it would have a negative impact on reporting in the system.