126076 Security Requirements - Technical Controls

(a)

Email & Messaging Security. A Demonstration Project Participant shall safeguard electronic mail and other messaging transmissions containing IHI through the use of encryption or an equivalent mechanism.

(b)

Audit Controls. A Demonstration Project Participant shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use IHI. The audit log parameters listed below are required for Demonstration Project Participants: * Login ID (successful and unsuccessful attempts) * Events (create, read, update, delete) * Timestamp (date, time) * Role (e.g. doctor, nurse, admin, billing, IT) * Unauthorized accesses

(c)

Consistent Time. A Demonstration Project Participant shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).

(d)

Data Assurance. A Demonstration Project Participant shall protect IHI from unauthorized alteration or destruction. A Demonstration Project Participant shall implement technical security measures to guard against unauthorized access to, or

modification of, IHI that is being transmitted over an electronic communications network. (1) Encryption & Cryptographic Controls. A Demonstration Project Participant shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect IHI. Demonstration Project Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each Demonstration Project Participant's internal best practices.

(1)

Encryption & Cryptographic Controls. A Demonstration Project Participant shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect IHI. Demonstration Project Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each Demonstration Project Participant's internal best practices.