**Encryption Policy**

**Purpose:**

[Insert Covered Entity or Business Associate name] is committed to conducting business in compliance with all applicable laws, regulations and policies. [Insert Covered Entity or Business Associate name] has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

The goal of these policies is to protect patient health information and other protected information such as individually identifying information by enhancing the security of our electronic information systems. [Insert Covered Entity or Business Associate name] requires securing Protected Health Information (PHI) contained on all mobile media, laptops, workstations, servers and external hosted sites that are not located in Approved Secure Data Centers. Approved Secure Data Centers are defined as data centers that have had a formal risk assessment on the physical and logical controls completed by the Information Security Office and the Internal Audit Office with no findings that would render the data center unsecured.

**Scope:**

These policies and guidelines apply to all workforce members who use, collect and/or access PHI. These policies and guidelines apply to all [Insert Covered Entity or Business Associate name] owned and personal electronic devices that are connected to [Insert Covered Entity or Business Associate name] networks and receive, store or transmit PHI. This policy does not cover text pagers or basic voice / SMS text cell phones.

**DEFINITIONS:**

1. Encryption: the process of converting data to an unrecognizable or "encrypted" form.
2. Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form.
3. Electronic Protected Health Information (ePHI): Individually identifiable health information transmitted or maintained in electronic form.
4. Workforce Member: Employees, volunteers (board members, community representatives), trainees (students), contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

**Policy:**

1. The Security Officer will provide appropriate workforce members with training and awareness regarding encryption methods implemented to protect ePHI from unauthorized alteration or destruction during transmission over electronic communications networks.
2. All ePHI will be encrypted, whether at rest or in transmission, where a risk analysis indicates that such encryption is necessary to protect the security of PHI.
	1. Such risk analysis shall consider the probability and criticality of risks to security.
3. All electronic devices that receive, store and/or transmit PHI and are not located in [an Approved Secure Data Center] must use approved encryption methods to secure the information stored on or transmitted outside the secure clinical network.
4. Servers that are not located in [an Approved Secure Data Center] are required to have all information stores of PHI encrypted.
5. PHI contained on laptops or workstations are required to be either File, Folder or Full Disk Encrypted.
6. Any and all mobile devices (smart phones and tablets) that connect to the secure clinical network that may contain or transmit PHI (through e-mail) are required to accept Information Security Standards to encrypt and protect the devices.
	1. External storage media (backup tapes, removable drives, etc) will need to have the PHI encrypted.
7. Files that contain PHI transmitted across the Internet (e-mail attachments sent outside network, or file transfers to other entities) will need to have the attachments encrypted or use an approved secure encryption method to deliver the information.

**Exceptions:**

Existing systems and applications containing Protected Information which cannot use encryption because of a technological limitation, but have compensating controls, may be granted a special exception by the Security Officer. However, these systems and applications will be required to have a formal risk assessment performed by the Security Officer to ensure that major risks are addressed via compensating controls to protect the data in lieu of encryption. Exceptions will be reviewed periodically and removed when a suitable solution is available.

**Violations:**

Any known violations of this policy should be reported to the Security Officer.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with [Insert Covered Entity or Business Associate name] procedures.

[Insert Covered Entity or Business Associate name] may advise law enforcement agencies when a criminal offense may have been committed.