[redacted]

Policy

Encryption

Department
IT
Date
05-05-2009
Policy Number
IT.022

Replaces
Policy Number
IT.002.005
Date
05-05-2009

Review Frequency
Annual

Next Scheduled Review
05-2010

Scope:

This policy applies to all computing devices and users which may store or access confidential information.

Subject:

Data Encryption Policy

Purpose:

To provide security for confidential and restricted GHS information.

Authoritative Reference:

HIPAA Security Implementation 164.312(e) and (a)
CMS Security Standards – Access Control (AC), Media Protection (MP)
NIST guidelines SP800-111, SP800-63, SP800-53, SP800-113.

Related Policies and Procedures:

IT.001S Encryption Standards
IT.026 Systems and Network Security Policy
IT.025 Data Sanitization and Equipment Disposal Policy
IT.027 Off-site Use of GHS Information Systems

Policy:

Confidential and restricted information must be encrypted when stored on mobile devices, such as laptops or USB drives, or when being transmitted over any communications network, such as the Internet, using valid cryptographic algorithms. FIPS approved cryptographic standards are employed by GHS and are documented in *Encryption Standards*. The use of proprietary or non-approved encryption algorithms is prohibited.

All devices that cannot be physically secured and may store or access confidential or restricted information must be encrypted, including all portable and mobile storage devices, and removable media, even when physically secured. This includes but is not limited to: hard disks of laptops, CD-ROMs, USB/thumb drives, and floppy discs. Exceptions:

- A mobile/portable device, such as a laptop, that is made immobile via physical restraints (e.g., bolted down to an immobile object) *and* is located in a physically secured, limited access environment, *and* has the approval of the Systems Security Officer, may not use storage encryption.
- Backup tapes are not encrypted due to potential errors and delays involved with the restoration of data from the backup. However, these are kept physically secured.
- Off-site/remote access to GHS information systems employ SSL certificate, VPN, or other types of transmission encryption, and/or require user authentication in order to access. (see policy on *Off-site Use of GHS Information Systems*).

[redacted]

Information used for authentication purposes (e.g., to verify the identification of users or objects on GHS networks and systems), such as passwords, shall be stored in an encrypted format.

Non-reusable authentication data (e.g., digital certificates) shall be based upon industry encryption standards. Digital Secure Sockets Layer (SSL) Certificates shall be used to protect sensitive Internet based transactions. SSL Certificates shall be issued by the IT Department based on business need and type of transaction or data asset to be protected.

Decryption keys are held solely by the IT Department and access to those keys is on a limited, restricted, need-to-know basis. Encryption keys must always be encrypted when sent over the Internet. Wherever possible, GHS shall employ automated encryption key management processes.

GHS upholds the U.S. government's restrictions on export of encryption technologies.

Definitions:
Confidential information = any data whose loss, misuse, or unauthorized access or modification could have adverse affects. This includes personal health information, and communications with clients, members and business partners that may contain this type of data.

Restricted information = any data whose access is restricted to employees who need it to perform their assigned duties for the company. This includes but is not limited to internal company communications and operations data, including human resources or payroll information, company financial, proprietary or strategic planning information, internal reporting data, software source code, and contact lists.

Department
IT
Date
05-05-2009
Policy Number
IT.022

Replaces
Policy Number
IT.002.005
Date
05-05-2009

Review Frequency
Annual

Next Scheduled Review
05-2010

Page Number
Page 2 of 2