GREATER HUDSON VALLEY HEALTH CARE SYSTEM
Policy/Procedure

Manual: Hospital-Wide
Section: Information Technology

Policy #: 210004		The Joint Commission Chapter:
SUBJECT: GHVHS Encryption Policy		
Effective Date: 2005	Review Date: 2006,07,08,09	Concurrences: Compliance Office
Revision Date: 2009, 4/14, 6/16		
Process Owner: IT Security Officer		
Approver: CIO		
Attachment(s):		

PURPOSE*:*
The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout Greater Hudson Valley Health System (GHVHS). Where necessary, appropriate encryption must be used to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) contained on GHVHS information systems.

Definitions:
GHVHS "Staff"- herein meaning ORMC, ORMC Foundation, CRMC, CRMC Foundation, GHVHSMG, ORMG, CRMG, employees, physicians, volunteers, contractors, vendors, students, residents, DSRIP Affiliates, Board Members, or other persons having PHI or patient contact or doing business with GHVHS.

GHVHS "locations"- hereinafter meaning Orange Regional Medical Center, Catskill Regional Medical Center, Grover M. Herman Hospital, Catskill Regional Skilled Nursing Unit, Catskill Regional Adult Daycare, Livingston Manor, Greater Hudson Valley Medical Group, Orange Regional Medical Group, Orange Regional Medical Pavilion, Catskill Regional Medical Group, Monroe Primary & Urgent Care, Goshen Patient Service Center, Orange Regional Medical Center Family Program for Alcoholism/Chemical Dependency, Outpatient Rehabilitation Center, Ambulatory Surgery Centers, DSRIP related functions, Arden LDC and all locations where GHVHS conducts business.

ePHI- Electronic Protected Health Information

PHI – Protected Health Information

BSI- Business Sensitive Information

PROTOCOL:

GHVHS will identify systems that require PHI to be encrypted.

Proven standard algorithms such as 3DES, AES, Blowfish, RSA, and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption.

Symmetric cryptosystem key lengths must be at least 1048 bits.

Asymmetric cryptosystem keys must be of a length that yields equivalent strength.

Procedure:

Boot Disk/ Full Disk Encryption:

The preferred method of encryption for laptop computers and smart devices is full disk encryption in conjunction with boot disk encryption. Laptop computers and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential and restricted information stored on the device.

E-mail Encryption:

All confidential or restricted information transmitted through email to an email address outside of the GHVHS domain (i.e. one that does not end in “@ormc.org” or “crmcny.org”) must be encrypted.
If Staff must send confidential information outside of the GHVHS domain, the user must type the word **encrypt** in the subject line.

Removable Storage Devices:

All confidential and restricted information (such as PHI or BSI) stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removable storage device. Removable storage devices must not be used for long term storage of confidential or restricted information.

Refer to the GHVHS Mobile Device Policy for further information.

Transmission Security:

Sensitive data transmitted in or out of the GHVHS network, via the public Internet, must be encrypted. Encryption may be accomplished through VPN, TLS, SSL, SSH, IPSec, S/MIME, SFTP or other secure methods approved by the IT Department.

All confidential and restricted information transmitted around existing wireless networks must be encrypted using WPA (Wi-Fi Protected Access) or better. All new wireless network installations must be encrypted using WPA or WPA2 128-bit or better.

REFERENCES WITH LEVELS OF EVIDENCE:

1. CMS, “CMS Information Security Policy, Standards and Guidelines Handbook”
2. SANS, “Acceptable Encryption Policy”
3. HIPAA Security Standard: Technical Safeguard “Encryption and Decryption” 45 CFR§ 164.312(a)(2)(iv)
4. International Standards Organization (ISO/IEC 17799:20000E))
5. GHVHS Mobile Device Policy