HIPAA Security Policy

1.0 Overview

Marquette University is committed to compliance with the Health Insurance Portability and Accountability Act (HIPAA). This policy establishes guidance for compliance with HIPAA standards for security management that will prevent, detect, contain, and correct security violations.

2.0 Purpose

This policy establishes requirements for technical security safeguards that will be used to store, process, and transmit electronic Protected Health Information (ePHI) at the University.

3.0 Scope

This policy covers all units and persons at the University that have access to ePHI. Each unit is responsible for compliance with and implementation of this policy. Individuals or departments who process, store or transmit electronic ePHI are required to obtain technical security support from Information Technology Services (ITS) at Marquette University.

4.0 Security Official

The Chief Information Officer of the University is the security official with regard to this policy.

5.0 Security Management

5.1 Identify relevant information systems. IT Services has primary responsibly for the security oversight of electronic health systems. Individual units that have access to ePHI will work with IT Services to identify, document, and protect information systems that house individually identifiable health information. This includes all hardware and software that are used to collect, store, process, or transmit health information. This inventory will include business function, ownership, and control of information system elements.

5.2 Conduct risk assessment. Based on the documentation provided in 5.1 (above), the following studies will be conducted:

5.2.1 Identify current controls in place.
5.2.2 Identify any vulnerability or weakness in security procedures or safeguards.
5.2.3 Identify events that can negatively impact security.
5.2.4 Identify the potential impact that a security breach could have on operations or assets, including loss of integrity, availability, or confidentiality.

5.3 Develop mitigation plan. In the event that a gap is determined where ePHI is at risk or the level of control in place falls short of recommended norms:

5.3.1 The gaps will be prioritized based on:
1) Applicability of the IT solution to the intended environment
2) The sensitivity of the data

3) Resources available for operation, maintenance, and training

5.3.2 A mitigation plan will be instituted to provide timely remediation of the liability.

5.4 Annual review. The process described in 5.1 through 5.3 (identify, assess, and mitigate) will be conducted on an annual basis.

6.0 Workforce Security

6.1 Job Description and Responsibility. Each unit, in conjunction with the Human Resources Department at Marquette University, will identify in writing who has the business need – and who has been granted permission - to view, alter, retrieve, and store electronic health information. Conditions under which access to ePHI is allowed will be documented in memo maintained by each area. Appropriate levels of security oversight, training, and access will be assigned to persons responsible for ePHI within the University.

6.2 Termination Procedure. A standard set of procedures will be maintained that will assure access control devices including access cards and keys will be recovered upon termination. Accordingly, access to computer accounts will be disabled, passwords will be changed, and cardholder records modified to disable access.

7.0 Security Awareness and Training

7.1 Timing. Security awareness and training may be included as part of an integrated training program. However, training related to HIPAA and ePHI must be segregated logically from a broader training program. Training will take place as part of new employee orientation as well as periodically as a part of unit training.

7.2 Content. While it is necessary to thoroughly cover the specific HIPAA policies that require awareness and training, it is also important to include any emerging trends, vulnerabilities, or advisories that are relevant at the time of training. Information security is a dynamic threat countermeasure requiring vigilance. Content will include:

7.2.1 Procedures for reporting incidents
7.2.2 How to protect and guard against malicious software
7.2.3 Password management and use
7.2.4 Procedures for monitoring log-in attempts and reporting discrepancies
7.2.5 Procedures for detecting and reporting malicious software
7.2.6 Security reminders

8.0 Security Incident Handling

IT Services will maintain a set of procedures documenting the protocol the University will use in the event of an incident involving ePHI. These procedures will:

8.0.1 Determine what activity/evidence constitutes a security breach/incident
8.0.2 Determine how the organization will respond
8.0.3 Establish a reporting mechanism and a process to coordinate responses

8.0.4 Allow for direct technical assistance, liaison to legal and criminal investigative groups, and interaction with vendors to address product related problems as needed
8.0.5 Identify appropriate individuals to be part of a formal incident response team when required
8.0.6 Document incident response procedures
8.0.7 Require regular review of the effectiveness of existing procedures and updates to those procedures to reflect lessons learned as well as make recommendations for improvements to security controls

9.0 Policies for Desktops, laptops, and PDAs

9.1 Disposal. This policy addresses the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

In the case of computers and laptops, IT Services will remove the hard drive from each computer or laptop that is scheduled for disposal. These hard drives will be physically secured until they are destroyed or until they are collected by a recycling company which will then destroy the hard drives. If a third party disposes of the media they must provide written documentation of that destruction.

When scheduled for disposal all other media must be rendered inoperative such that ePHI data cannot be retrieved.

9.2 Media Re-use. In the event that a computer is being transferred to a non-HIPAA protected environment, protected health information must be removed from electronic media before the media are made available for re-use. Transfer with the same department/clinic/school (Dental, Health Services, etc.) does not require any extraordinary measures.

9.3 Accountability. IT Services will maintain record of ownership of specific devices that has access to or contains ePHI (desktop, laptops, and PDAs). Users should request transfer of these devices through the IT Services Help Desk.

10.0 Access Authorization

Marquette University protects electronic patient health information via a login and password combination, user rights within a specific application, and application auto-log-out functionality, where possible. An end user needs to authenticate into an application containing ePHI information by using either their domain or Application login and password combination. Once logged into an application, User Rights may be used to restrict a user to the type and amount of detail that can be seen.

10.1 Domain Membership. Where feasible workstations that contain or has access to ePHI should be members of an IT Services administered domain providing for password management and user access control. As members of an IT Services administered domain users will have access automatically removed when they are classified as inactive in the HR/Payroll system.

10.2 Auto Logout. Where possible workstations and or applications that has access or contains ePHI should be configured for auto-logout after a period of no activity.

10.3 Password Management. Passwords will governed by IT Services password management policy. Where possible the application should authenticate against the University's enterprise LDAP (Active Directory). This will enable a more automated account management.

10.4 Workstation access. Workstations that contain or has access to ePHI should be locked so that a password must be entered to gain access when user is away from the workstation, and the workstation should be logged off or locked at the end of the day to prevent unauthorized use.

10.5 Workstation physical security. Workstations that contain or has access to ePHI information that are in highly vulnerable areas should be secured by locked cable where possible. Workstations with access to protected information that are located in office areas are secured within those office areas

10.6 e-Mail. ePHI should not be transmitted via e-mail off campus unless encrypted at 128 bits or better. ePHI information can be transmitted on campus if the user is using the Outlook client connected to the Exchange server using the MAPI format.

11.0 Authorized Users

11.1 Identify Authorized Users. Identify all approved users with ability to alter or destroy protected health information. Applications and/or workstations that contain or has access to ePHI must provide for unique user names and passwords for access. Users may not share usernames and passwords. If a password is suspected to be compromised a user must change that password immediately.

11.2 Identify Possible Unauthorized Altering or Destruction of Data. Identify scenarios that may result in unauthorized altering or destruction of protected health information. In addition critical infrastructure areas (Data Center, switch rooms, etc.) must have physical security (locked doors or card access).

12.0 Business Associates Contract and Other Agreements

Policies and procedures are designed for Covered Entity (CE) and Business Associate (BA) to protect electronic protected health information.

12.1 Nondisclosure. BA shall not use or disclose CE's ePHI otherwise than as permitted or required by this Policy

12.2 Minimum Necessary. BA shall use or further disclose ePHI only in the minimum amount and to the minimum number of individuals necessary to achieve the purpose of the services being rendered to or on behalf of CE.

12.3 Safeguards. BA shall use appropriate safeguards to prevent use or disclosure of CE’s ePHI.

12.4 Reporting of Unauthorized Disclosures. BA shall report to CE any use or disclosure of CE's ePHI of which BA becomes aware.

12.5 Mitigation. BA shall mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of ePHI by BA in violation of the requirements of this Policy.

12.6 BA's Agents. BA shall ensure that any agents, including subcontractors, to whom it provides ePHI received from, or created or received by BA on behalf of CE, agree to the same restrictions and conditions that, apply to BA through this Policy with respect to such ePHI.

12.7 Internal Practices. BA shall make its internal practices, books and records relating to the use and disclosure of ePHI received from CE, or created or received by BA on behalf of CE, available to the CE, for purposes of determining CE’s compliance with the Privacy Rule.

13.0 Data Center

The Data Center contains the server side architecture including the backup environment. Backups are performed on primary servers and computers located in the data center or other locations on campus. The data backed up relates to all files associated with Operating systems, installed applications and files pertaining to said applications. Tape backups are retained for 3 months and then recycled. Modification to the existing backup environment must be made through change management.

13.1 Backup Responsibly. It is the responsibility of the backup team at Marquette University to provide regular scheduled backups of critical university data. These backups serve as a disaster recovery resource in the event of hardware malfunction, natural disaster and user error.

13.2 Backup Schedule. The backups are controlled by an automated time schedule. The backup levels are skip, incremental and full. The backup level Full is generally run once a week. The exceptions being E-mail which is a full backup every other day. Backup schedules may be temporarily adjusted in order to facilitate maintenance windows or other maintenance situations.

13.3 Backup Retention. Backup sets other then those in the tape libraries will be stored off-site and retained 3 months.

13.4 Recovery. Recoveries are prioritized, with machine malfunction being ASAP, and user requests being 2 business days.

13.5 Special backups. Special request backups may be run with proper authorization.

13.6 Data Center Media. All Data Center media which contains ePHI (SAN disks, etc.) should be cleaned of data before disposal or returning to the vendor.

14.0 Physical Access

14.1 Location. All Enterprise Systems are located in Cudahy Hall Data Center and Core Data Closet, and Redundant Data Center. Each of these areas are equipped with ID card readers that control entrance into the data center.

14.2 Granting Access. All individuals requiring access to the Marquette University Data Center and/or Core Data Closet must get approval from the Senior Director, or CIO. Once proper approval is obtained the individual's ID card will be programmed for the approved access. For temporary access in addition to the above approval can be granted by the Systems or Networks Manager.

14.3 Access Cataloguing. All access to the Marquette University Data Center and Network Operations Center is catalogued in the ID card reader system stamped with date, time, ID card number, name, and door accessed. These system catalogues are retained for one year.

14.4 Access Review. Access to the Marquette University Data Center and Network Operations Center will be reviewed on a quarterly basis. Any individual who no longer requires access will be removed from the access list.

15.0 Enforcement

This policy is administered by Marquette University IT Services.

17.0 Sanctions

Any person found to be in violation of these policies may be subject to disciplinary action, up to and including dismissal.

18.0 Definitions

Term	**Definition**
ePHI	Electronic Protected Health Information
CE	Covered Entity (Marquette University)
BA	Business Associate (i.e. HP,)
Backup	Disk to tape data transfer
Full	Image backup of mount point(s)
Increment	Selective backup of mount point(s)
Recovery	Tape to disk data transfer
Skip	Backup for that time period is skipped.
Tape cartridge	DLT or SDLT tape cartridge 40GB to 160 GB in size
Tape library	Collection of tape cartridges and Tape Drives
Schedule	Automated time frame for backup processing