Marist College GROUP HEALTH PLAN

SECURITY POLICIES AND PROCEDURES REGARDING
ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Effective April 20, 2006
Revised September 23, 2013
# Table of Contents

**INTRODUCTION**  

**IMPORTANT PRELIMINARY GUIDELINES**

A. Plan vs. Marist College  
B. ePHI  
C. Required Plan Amendments  
D. Implementation Specifications

**DOCUMENTATION REQUIREMENTS**

**ADMINISTRATIVE SAFEGUARDS**

   RISK ANALYSIS  
   RISK MANAGEMENT  
   SANCTION POLICY  
   INFORMATION SYSTEM ACTIVITY REVIEW  
B. STANDARD: Assigned Security Responsibility.  
D. STANDARD: Information Access Management.  
E. STANDARD: Security Awareness and Training.  
F. STANDARD: Security Incident Procedures.  
G. STANDARD: Contingency Plan.  
H. STANDARD: Evaluation.

1. STANDARD: Business Associate Contracts and Other Arrangements.

**PHYSICAL SAFEGUARDS**

A. STANDARD: Facility Access Controls.  
B. STANDARD: Workstation Use.  
D. STANDARD: Device and Media Controls.

**TECHNICAL SAFEGUARDS**

A. STANDARD: Access Control.  
B. STANDARD: Audit Controls.  
C. STANDARD: Integrity.  
D. STANDARD: Person or Entity Authentication.

**APPROVALS**
Marist College provides the Marist College Group Health Plan (the "Plan") for certain employees, retirees and other beneficiaries. This document and the attached Exhibits describe the policies and procedures that are intended to comply with certain security requirements that apply to the Plan and relevant portions of Marist College pursuant to the federal Health Insurance Portability and Accountability Act ("HIPAA") and related regulations by the Department of Health and Human Services (together, the "HIPAA Security Requirements").

The HIPAA Security Requirements require the review and implementation of appropriate administrative, physical and technical policies and procedures that are intended to safeguard the confidentiality, availability, and integrity of "protected health information" that is in an electronic format ("ePHI"). As the sponsor of the Plan, Marist College is fully committed to the security of protected health information that may be created, received, maintained or transmitted by or on behalf of the Plan.

Jennie Owen is the Interim HIPAA Security Officer, as well as the HIPAA Privacy Officer.

The Plan is administered by AETNA. For the purpose of this document, they will be referred to as the "Provider".

The policies and procedures described in this document and the attached Exhibits will be interpreted, administered, amended, modified and/or terminated at the sole discretion of the Plan's HIPAA Security Officer and/or other appropriate personnel to the extent deemed necessary or proper to comply with the HIPAA Security Requirements.

Finally, this document and the attached Exhibits are not intended to create or acknowledge any right or entitlement of any third party (including, but not limited to, Plan participants, beneficiaries, and business associates) with regard to the adoption, design, administration, modification or termination of the Plan.
IMPORTANT PRELIMINARY GUIDELINES

A. Plan vs. Marist College

The HIPAA Security Requirements and the policies and procedures in this document (including Exhibits) do not necessarily apply to all of Marist College and its employees. Rather, they apply to:

- Marist College Group Health Plan (the "Elrul"); and
- Marist College, but only to the extent electronic protected health information ("ePHI") is created, received, maintained, or transmitted to or by Marist College on behalf of the Plan; and
- Any subcontractors (of the Plan or Marist College) that create, receive, maintain, or transmit ePHI on behalf of the Plan.

B. ePHI

Generally, ePHI is any and all individually identifiable health information that is transmitted by or maintained in electronic media. The definition of “individually identifiable health information” is the same as used for purposes of HIPAA privacy requirements. ePHI includes Address, Date of Birth, Social Security Number and Name when in combination with any of the previous three as intended for health information. For further information on that definition, you should consult the Plan’s HIPAA Privacy Officer.

C. Required Plan Amendments

In order to appropriately adopt and implement the policies and procedures in this document (including Exhibits), the Plan must be amended in accordance with the HIPAA Security Requirements as well as the HIPAA privacy regulations. Among others, such amendments must:

1. Establish Permitted Uses and Disclosures. Establish the permitted and required uses and disclosures of protected health information (which includes ePHI) by Marist College consistent with the privacy requirements of HIPAA;

2. Provide "Firewall" between Plan and Marist College with regard to PHI. Describe those Marist College employees or classes of Marist College employees to be given access to the protected health information to be disclosed by the Plan (or its agents or subcontractors). Any employee or person who receives protected health information relating to payments under, health care operations of, or other matters pertaining to the plan in the ordinary course of business must be included in such description. Access to and use of protected health information by such employees and other persons must be restricted to the plan administration functions that Marist College performs for the Plan. The Plan amendment must also provide an effective mechanism for resolving any issues of noncompliance by any such employees or other persons with the Plan document provisions intended to comply with the privacy requirements of HIPAA;

3. Security Measures for the "Firewall". Require Marist College to ensure that the adequate separation as described in Paragraph 2 above is supported by reasonable and appropriate security measures;

4. Security Safeguards for ePHI. Require Marist College to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the Plan;

5. Requirements for Agents and Subcontractors. Require Marist College to ensure that any agent, including a subcontractor, to whom it provides ePHI agrees to implement reasonable and appropriate security measures to protect the information; and

6. Reporting Security Incidents. Require Marist College to report to the Plan any security incident of which it becomes aware.

For purposes of the privacy requirements of HIPAA, there are additional Plan amendments that may be required. For information regarding such additional amendments, you should consult the Plan’s HIPAA Privacy Officer.
D. Implementation Specifications

The framework of policies and procedures in this document closely track the requirements as laid out in the HIPAA Security Requirements, and consist of three main types of "safeguards" – Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Each set of safeguards is comprised of a number of standards, which, in turn, are generally comprised of a number of implementation specifications that are, under the HIPAA Security Requirements, either "required" (noted with "(R)") or "addressable" (noted with "(A)").

If an implementation specification is required, policies and/or procedures must be implemented to meet what that implementation specification requires.

If an implementation specification is addressable, then there must be an assessment of whether it is a reasonable and appropriate safeguard for the particular environment in question. This involves analyzing the specification in reference to the likelihood of protecting the Plan's ePHI from reasonably anticipated threats and hazards. If it is decided, based on such an assessment, that an addressable specification is not to be implemented, then the HIPAA Security Requirement requires documentation of the reason and, if reasonable and appropriate, implementation of an equivalent alternative measure.
Pursuant to the HIPAA Security Requirements, the following documentation requirements apply:

A. **Policies and Procedures.** All policies and procedures implemented to comply with the HIPAA Security Requirements must be documented in writing. The documentations may be in electronic format;

B. **Actions, Activities and Assessments.** If an action, activity or assessment is required to be documented, a record of the action, activity or assessment must be maintained in writing. The written record may be in electronic format;

C. **Six-Year Retention.** The documentations and records described above must be retained for at least six years from the date of its creation or the date when it last was in effect, whichever is later;

D. **Availability.** The documentations and records described above must be made available to those persons responsible for implementing the procedures to which the document pertains;

E. **Review and Update.** The documentations and records described above must be reviewed periodically, and updated as needed, in response to environmental or operational changes affecting the security of ePHI.

The foregoing documentation requirements also apply to all attachments to this booklet, which further describe the policies and procedures relating to the security of ePHI in connection with the Plan.
ADMINISTRATIVE SAFEGUARDS


RISK ANALYSIS

The HIPAA Security Officer, together with appropriate Information Technology personnel, completed a thorough risk analysis and assessment that evaluated the potential risks and vulnerability to the confidentiality, integrity, and availability of ePHI held by the Plan and by Marist College in connection with the Plan.

Marist College will evaluate the technical and non-technical implementation of its Security Policies and procedures on an "as needed basis". The purpose of the evaluation will be to determine the effectiveness of the Policies as well as to ensure compliance with new and/or revised state and federal regulations. Tills evaluation will occur with any of the following events:

- A change in any state or federal regulation that may affect the Security Policies.
- A new state or federal regulation that may affect the Security Policies.
- A breach of security within Marist College.
- Any other time the HIPAA Security Officer believes there is a need to evaluate the Security Policies.

The evaluation of the Security Policies will be done by the HIPAA Security Officer in consultation and/or conjunction with the Chief Technology Officer. All findings shall be documented and shall be maintained in a HIPAA Security Evaluations File. Any resultant changes to the Security Policies shall be included as Security Policy Amendments.

RISK MANAGEMENT

- All enrollment information entered into the Provider's secure website (must utilize confidential username and password for both employee and employer [Plan Manager]).
- Information stored on the Provider's data systems at their physical site as well as on their secure website.
- Stored at Marist either in locked office or in supervised area at all times.
- Also refer to the Marist College Security Policy Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer.

SANCTION POLICY

Marist College employees who violate the College's privacy policy and 1) knowingly release ePHI without written authorization from a Plan participant or their designated representative or 2) knowingly release or store ePHI without safeguards, may be subject to discipline up to and including termination of employment. Employees who expose or release ePHI inadvertently by not complying with safeguards, may also be subject to discipline, up to and including termination of employment.

The security of ePHI requires constant attention from the College employees who handle this personal information. Accidental violations, while not acceptable, may not lead to severe discipline unless the offense is repeated.

All employees who are likely to handle ePHI will be identified by the HIPAA Security Officer and must sign a confidentiality statement indicating they are aware of their responsibilities and will adhere to ePHI safeguards.

Examples of potential violations include but are not limited to:

1. Emailing personal, identifiable health information of a Plan participant without seeking written permission from that participant.

2. Emailing personal identifiable health information of a Plan participant without coding/encrypting it as specified by the Security Policies and Procedures.
3. Taking a paper copy of ePHI and providing it to any unauthorized person or leaving that information available for an unauthorized person to read or take.

4. Neglecting to log-off a computer which contains ePHI.

5. Allowing an unauthorized person to use your computer which contains ePHI without first ensuring the inaccessibility of that ePHI.

INFORMATION SYSTEM ACTIVITY REVIEW

Refer to Marist College's Security Policies, Procedures, Standards and Guidelines Manual for Information Technology; the Information Security Policy; External Audit Reports.

B. STANDARD: Assigned Security Responsibility.

The HIPAA Security Officer is responsible for the development and implementation of the policies and procedures in compliance with the HIPAA Security Requirements. The HIPAA Security Officer position will be reviewed on an annual basis by the Associate Vice President for Human Resources and a replacement will be designated should the HIPAA Security Officer terminate employment or become unable to fulfill the requirements of the position.


AUTHORIZATION AND/OR SUPERVISION

The HIPAA Security Officer will recommend to the Department Administrator(as defined in the Marist College's Security Policies, Procedures, Standards and Guidelines Manual for Information Technology) who will be authorized to access ePHI and the levels of supervision necessary based on the level of the employee's access to ePHI and the sensitivity of that information.

The HIPAA Security Officer will determine if access to ePHI is necessary for Marist employees.

The Chief Technology Officer will have authorization plus those employees already provided access to PHI in the Marist HIPAA Privacy Policies and Procedures document.

Physical supervision of any of these employees is not required when they are viewing ePHI.

Physical supervision of Marist Information Technology staff performing IT system maintenance or repair is not required.

Physical supervision of non-Marist individuals performing IT system maintenance or repair is required.

D. STANDARD: Information Access Management.

ISOLATING HEALTH CARE CLEARINGHOUSE FUNCTIONS

As the Plan does not perform health care clearinghouse functions, this specification has not been implemented.

E. STANDARD: Security Awareness and Training.

SECURITY REMINDERS

A Security Reminder process is currently under development.
PROTECTION FROM MALICIOUS SOFTWARE

All information regarding the HIPAA Security Policy and Procedures is provided to all new hires upon enrollment.

Security awareness training for all members of the College will be an on-going process and is currently under development.

LOG-IN MONITORING

PASSWORD MANAGEMENT

F. STANDARD: Security Incident Procedures.

RESPONSE AND REPORTING

An Incident Report Process will be developed.

IDENTIFICATION
Any employee who believes that a violation of the Security Policy has occurred is required to notify the Chief Technology Officer in writing immediately to report the incident in question. The Chief Technology Officer will investigate the facts and circumstances of the alleged violation and determine an appropriate course of action.

RESPONSE & MITIGATION
The Chief Technology Officer will notify all involved parties in a timely manner once it has been determined that a security incident has occurred. The response to each reported security incident will seek to restore the level of security that is required under the Security Policy. The Chief Technology Officer will coordinate to correct any deficiency in the Security Policy or related procedures under the policy, and formulate and execute steps necessary to mitigate, to the extent practicable, the harmful effects of known security incidents.

DOCUMENTATION
All known incidents, responses, and outcomes are reported and documented by the Chief Technology Officer. The Chief Technology Officer will also document relevant information on all reported incidents of potential violation under this policy whether or not a reported incident is ultimately found to be an actual violation.

G. STANDARD: Contingency Plan.

DATA BACKUP PLAN

Human Resources:
- All data regarding employee's medical, dental and life insurance enrollment and payment history.
- Backup schedule is done daily.
- Backup storage in onsite and on the hard drive. Also stored on discs (CD, flash drive).
- All referenced materials are saved/stored with the Provider.

Information Technology:
• HIPPA data is contained in the following directories/systems: LDAP, Active Directory, HRS, ADS, SIS, FRS, Banner, Voyager, Content Manager.
• Backups are performed on a daily basis. They are incremental until a full backup is performed. The application department schedules a full backup.
• All backups are currently stored onsite. They are in different buildings, but all onsite.

DISASTER RECOVERY PLAN
• The current Information Technology Disaster Recovery Plan is being reviewed and updated. Much of this is due to changes in hardware, software, and network systems as well as building location and utilization. Definition of how systems can be affected will be part of that new definition.
• Damage is determined by the Business Continuance / Recovery Team.
• Restoration of systems is controlled by the Chief Technology Officer and the appropriate software group responsible.
  The Technical Services department will restore to the system and middleware level.
  The Administrative Computing department will restore the applications and the data.
  The Network department will restore network capability
  Hardware replacement will be the responsibility of the Computer Operations Department.
• The Disaster Recovery plan is accessible, with authorization, through the Marist iLearn site. It is maintained by the Chief Technology Officer.

EMERGENCY MODE OPERATION PLAN
The current Information Technology Disaster Recovery Plan is being reviewed and updated. A new emergency mode of operation plan will be defined as part of that process.

TESTING AND REVISION PROCEDURES
• Testing of Disaster Recovery procedures are to be conducted once a year.
• Testing will be comprised of both live tests as well as scenario walk thurs.
• The Chief Technology Officer is responsible for reviewing all test results and any appropriate changes.

APPLICATIONS AND DATA CRITICALITY ANALYSIS
The critical business systems and operations at Marist are listed below along with the recovery time goal. Business owners of each process still need to be identified, which will require some processes to be broken down into individual component parts, especially the Banner administrative systems. User functions not directly tied to computer and telephone support by Information Technology are not addressed.

Initially, all web addresses will point to the same minimal web server to be used for communication. As their services are recovered, those web addresses will point back to their recovered system. All methods of communication have a goal of 7-day recovery.

Different times of the year may require adjustments to the recovery goals below. No attempt has been made to identify those adjustments at this time.

Level A. Systems to be recovered within: (Currently 2 hours, Goal 4 hours)
  1. Minimal College web servers to be used for communications

Level B. Systems to be recovered within: (Currently 2 hours –*, Goal 12 hours)
  1. Central Directory/Authentication server (LDAP & CAS)
  2. Network Infrastructure
  3. Telephone (CBX) services
  4. Network Support Systems (DNS, DHCP, VPN, Proxy Servers, licensing, encryption, etc)
Levels A and B have been achievable goals since June 30, 2007.

* - Not including CBX

Level C. Systems to be recovered within: (Currently 14 days, Goal 7 days)- Key items are multiple methods of communications to community and items for basic IT functions

1. Communications Methods
   a. Telephone - PhoneMail (VoiceRite)
   b. IT internal support databases (Helpdesk, inventory, network, C\IP)
   c. E-mail
      i. Notes
      ii. Foxmail
   d. Cable TV

2. Sakai (iLearn, iCollaborate, iPortfolio)

3. Academic Web Servers

4. Centralized Backup Manager – Tivoli Storage Manager (ISM)

5. Centralized File Server

6. IT Support Systems (DeepFreeze, Lab metering, Maintenance, AntiVirus)

7. Lenel- Card Swipe access system

Level D. Systems to be recovered within: (Currently 14 days, Goal 7 days)- Key items are multiple methods of communications to community, and items for basic IT functions

1. Academic Applications

2. Academic Web Servers

3. Banner Administrative System
   a. Banner Human Resources – includes Payroll

4. IA Plus administrative system
   a. Human Resource System (HRS) – Includes Payroll
   b. Financial Records System (FRS) – Required for Payroll

Level E. Systems to be recovered within: (Currently 14 days, Goal 10 days)

1. Academic Applications
   a. Linux Virtual Servers
   b. zSeries Knowledge Center

2. Main College Web Servers
Level F. Systems to be recovered within: (Currently 14 days, Goal 14 days)

1. IA Plus Administrative System
   a. Student Information System (SIS)
   b. Admissions
2. Banner administrative systems
   a. Banner Finance
   b. Banner Student
   c. Banner Financial Aid
3. Jobs.Marist
4. Library Online Catalog (Voyager)
5. Student Services Web Servers

Level G. Systems to be recovered within: (Currently 21 days, Goal 21 days)

1. IA Plus Administrative System
   a. Alumni Development System (ADS)
2. Banner administrative systems
   a. Banner Alumni/Development
3. Content Manager (iDocs and others)
4. Web Content Managers
5. Marist Money
6. Security Camera system
7. MIPO web server
8. Online Calendar-Scheduler Plus

Level H. Systems to be recovered within: (Currently 21 days, Goal 21 days)

1. FDR Library System
2. Other Servers and Web Servers- (HRVI, ECC, IDCP, OSDL, etc.)
3. Hosted Sakai/ERP
4. Academic Applications
   a. Oracle Server
5. Video Streaming-Darwin, IVI'
6. Hour Track-Biometric Hand Scanner
H. STANDARD: Evaluation.
   - HIPAA Security Officer will perform a check list on an annual basis.
   - HIPAA Security Officer will document any potential security breaches and implement corrective action.

I. STANDARD: Business Associate Contracts and Other Arrangements.

The Plan, in accordance with the general rules of the HIPAA Security Requirements (45 CFR 164.306), may permit a business associate to create, receive, maintain, or transmit ePHI on the Plan's behalf only if the Plan obtains satisfactory assurances, in accordance with the business associate agreement requirement under the HIPAA Security Requirements, that the business associate will appropriately safeguard the information. This Standard does not apply to:

   - The transmission by the Plan of ePHI to a health care provider concerning the treatment of an individual; and
   - The transmission of ePHI by the Plan (or an HMO or health insurance issuer on behalf of the Plan) to the Plan sponsor, to the extent that the plan amendment requirements of the HIPAA Security Requirements and the HIPAA privacy rules are met.

The HIPAA Security Officer identifies each business associate and ensures that business associate agreements are executed with each business associate before the business associate is permitted to create, receive, maintain or transmit ePHI on behalf of the Plan. The business associate agreement will contain satisfactory assurance that the business associate will implement the required administrative, physical and technical safeguards as required under HIPAA. Executed business associate agreements are retained by the HIPAA Security Officer.

PHYSICAL SAFEGUARDS

A. STANDARD: Facility Access Controls.

CONTINGENCY OPERATIONS
   - Information Technology personnel assigned to assist with computer related issues will be allowed to enter the office of HIPAA Security/Privacy Officer by appointment and announcement only.
   - Information Technology personnel must have approval by the HIPAA Security/Privacy Officer to perform retrieval of lost data from their computer.
   - Information Technology personnel must be identified and verified before admitted in HIPAA Security/Privacy Officer's office.
   - HIPAA Security/Privacy Officer's desk must be cleared of all other important information.
   - Refer to the Marist College Information Technology Disaster Recovery Site

FACILITY SECURITY PLAN

The facility security plan includes controls which are intended to ensure that only authorized individuals have access to facilities and equipment that contain ePHI.

   - Outside door locked and access not permitted without HR staff member present except Security Officer if emergency is present.
   - Computers shut down at night.
   - Computers logged off or locked while unattended
• Both outer and inner doors locked with key and windows safely secured with locking mechanism.
• Each computer is tagged for each particular/individual user.
• No access during non-working hours.
• File cabinets are locked.
• Inner office of HIPAA Security Officer is locked when not present.
• All ePHI is securely filed and not left unattended during non-business hours.
• Prescreening of all customers/visitors and prevented from walking toward the back offices without announcement and permission.
• Refer to the Marist College Security Policies, Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer

ACCESS CONTROL AND VALIDATION PROCEDURES

• Certain work areas require the use of key cards for entrance to certain offices.
• Certain work areas require the use of electronic control for entrance to certain offices.
• The Payroll Office has access to information such as ID#, SS#, and salary information which are shared.
• All students who work in offices with access to information related to security/privacy must sign a Confidential Statement.
• Refer to the Marist College Security Policies, Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer

N.UNTENANCERECORDS

The Director of Safety and Security is responsible for tracking and maintaining records of facility security repairs and modifications to the extent they relate to facilities that house ePHI or related software or equipment.

• Keys/ID swipe access changes are recorded on ID system. When a verbal, e-mail or hard copy request is received for repairs, the completed documentation is filed in the Office of the Access Control Specialist. If key(s)/swipe card(s) are lost, locks/swipe systems are changed depending on the circumstances (e.g. if a key/ID swipe card has fallen in a drain, locks/swipe system is not replaced). Each building has a Master Key in the possession of a high ranking Administrator that opens all doors in his/her area. All "Master Keys" are in the possession of the Access Control Specialist whose office is locked when vacant.
• All Keys and lock core information are kept on file in the Office of the Access Control Specialist.
• Electronic swipe access for each individual's ID is "shut off" so he/she cannot swipe and/or the physical locks are changed. This can also be adjusted or canceled based on need (e.g. high level access [employee in Information Technology] changed jobs and only needed access to McCann Center can be adjusted). Locks also changed as needed. No daily log of repairs.
• Employee information is housed on a password protected computer accessed by the Access Control Specialist and the Assistant Locksmith/Security Guard.
• ID cards generated and modified by the Card Office through password protected computer.
• ID cards have "key swipe" capability.
• Replacement ID card generates new number which in turn terminates old number automatically.
• Terminated employee's card reverts to '0' which cancels activation.
• Master keys are maintained in a locked office during shift changes. Security personnel responsible for master keys on duty at all times (two shift changes).
• Keys (master) to all offices maintained in Security Office must have access in times of emergency.

B. STANDARD: Workstation Use.

HR Workstation Use

• Computer not visible from outside office.
• Workstation is in a secure office.
• Office/workstation reconfigured for security and privacy.
- Computer is locked out of all programs when unattended for extended periods of time. An automatic screensaver locks the computer after an assigned number of unattended minutes and requires password authentication to access the computer again.
- Office securely closed when unattended
- Close screen when unauthorized employees enter work area.
- Office always locked after business hours.
- All computers in the Human Resources Office are encrypted.

Payroll Workstation Use
- Computers visible from outside office are equipped with a privacy filter which allows the employee to view data on a monitor head-on. The computer visible from outside the office is a student payroll computer which does not contain HIPAA related data.
- Workstations are in a secure office which is locked at all times. An access card reader is being installed to electronically track access.
- Computer is locked out of all programs when unattended for extended periods of time. An automatic screensaver locks the computer after an assigned number of unattended minutes and requires password authentication to access the computer again.
- All computers in the Business Office (includes the Payroll Office) are encrypted.
- Office always locked after business hours.
- Payroll sensitive documents are locked in secure file drawers/cabinets after business hours.

I.T. Workstation Use
- Workstation location (e.g., centrally located or segregated) is very important so that monitors are strategically placed to avoid others from seeing EIP information on their screens. Facing monitors towards the wall and not towards a walkway is critical and must be enforced by the department's manager. There are special screen protectors that will only allow employees to look at a monitor head-on. This can minimize the possibility of unauthorized view that the employee may not be aware is happening.
- Computer is locked out of all programs when unattended for extended periods of time. An automatic screensaver locks the computer after an assigned number of unattended minutes and requires password authentication to access the computer again.
- Procedures when leaving a workstation or when unauthorized individuals enter the area (e.g., employees will log off before leaving a workstation unattended or close screen displaying ePHI if unauthorized employees enter the work area.) Routine internal audits should be performed to insure the monitoring and supervision of the workstation is being conformed to.
- All offices must be locked after business hours and only those with pre-approved access should be allowed to enter. If I.T. needs to update machines they will notify the department head and staff with enough notice to allow important information to be removed from their desks.
- There should not be any ePHI stored on the hard drives of the laptop or other portable devices in case of theft or unauthorized use of the Marist equipment. Procedures for employees who telecommute should be put into place to include use of firewalls, virus protection and limited access to ePHI information to home offices. All information should be encrypted when backing up to a portable device.
- All computers in Human Resources, Payroll and Business Office are encrypted.
- All laptops across campus are fully encrypted.


All workstations with access to ePHI will be locked during non-working hours. During working hours computers may remain on but all employees with access to ePHI are responsible for logging out of programs that contain ePHI if they leave their station for any period of time.

Employees should have the latest security patches installed on their workstations.
Use of separate machines for work and home are recommended to reduce the possibility of compromising data. The use of strong passwords, a combination of lower case, caps, numbers, and symbols are encouraged. Employees should never share their password with anyone, and they should change their passwords frequently (i.e. every 180 days).

Employees should ensure that the Antivirus software and Spyware removal tools have the latest definitions and real time monitoring.

Only software from trusted sources should be installed, this includes any ActiveX/Java applets.

Employees should contact Marist Network Security immediately if anything appears suspicious on a workstation.

These physical security measures will be deemed effective unless any release of ePHI occurs at which time the security measures will be reevaluated.

D. STANDARD: Device and Media Controls.

DISPOSAL

Marist College uses a third party vendor to recycle old computer equipment including computer hard drives. Before computers are turned over to the recycler, the hard drives are wiped cleaned using a hard drive duplicator that erases the hard drive to meet U.S. Department of Defense specification DoD 5220-22M.

MEDIA RE-USE

Before reusing a hard drive, the hard drive is erased using the hard drive duplicator that meets U.S. Department of Defense specification DoD 5220-22M. This ensures the hard drive is wiped clean of any data and is ready for computer reimaging.

Backups and other information kept on portable media should be securely located in a locked area by the employee. COs and DVDs containing data are not reused and are shredded before disposal.

Media tapes are handled by the Operations Department and documentation is contained in the Information Technology Operations Manual.

ACCOUNTABILITY

Refer to Marist College Inventory System/Procedures which can be provided by the Chief Technology Officer.

DATABACKUPANDSTORAGE

When computers are replaced due to age or transfer in location, the data is transferred from the old hard drive to the new hard drive by the Desktop Administrator or Technician. The old hard drive is then tested for errors and will be cleaned using the hard drive duplicator that erases the hard drive to meet U.S. Department of Defense specification DoD 5220-22M.

If computers are being moved from one location to another, no copying of data will be performed.

TECHNICAL SAFEGUARDS

A. STANDARD: Access Control.

UNIQUE USER IDENTIFICATION

Refer to Marist College's Security Policies, Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer.
EMERGENCY ACCESS PROCEDURE
Refer to Marist College's Disaster Recovery Manual which can be provided by the Chief Technology Officer.

AUTOMATIC LOGOFF

Via Active Directory, a Group Policy will be set for those with access to ePHI to automatically lockout the computer after 15 minutes of inactivity.

B. STANDARD: Audit Controls.

Refer to Marist College's Security Policies, Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer.

C. STANDARD: Integrity.

MECHANISM TO AUTHENTICATE ePHI

A mechanism to authenticate ePHI is not implemented at this time.

D. STANDARD: Person or Entity Authentication.

Refer to Marist College's Security Policies, Procedures, Standards and Guidelines Manual for Information Technology which can be provided by the Chief Technology Officer.


INTEGRITY CONTROLS

There is an IT Data Security Task Force that is currently performing an overall risk analysis, which includes vulnerability of ePHI. This Task Force is working on identifying appropriate means to protect data that is transmitted and the necessary security measures.

ENCRYPTION

A policy for encryption is being developed. ePHI will be included in that plan.

All computers in Human Resources, Payroll and Business Office are encrypted.

TLS encryption is turned on in our Barracuda Spam appliances through which all e-mail passes while entering/leaving Marist.
APPROVALS

Jennie Owen, Intcom, HIPAA Security Officer

Han§

Deborah Raikes-Colbert, Associate Vice President for Human Resources