POLICY

Information Security is a responsibility of every member of the Munson Healthcare/Mercy North workforce and every other individual who has access to Munson/Mercy information systems and/or confidential information. Workforce members are required to receive education regarding their expectations towards information security.

PROCEDURE

Information maintained by Munson Healthcare and Mercy North Hospitals is a vital company asset. The preservation of its confidentiality, integrity, and availability is essential to our success. In pursuit of that goal, Information Systems has established policies and procedures to protect this information from, but not limited to, unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use, whether accidental or intentional.

The provisions of this policy apply to all users of Munson Healthcare/Mercy Hospital information systems; all users have a responsibility to assure security, confidentiality and use in an authorized manner. Every user of information -- no matter what their status (employee, volunteer, intern, contractor, consultant, medical staff, temporary, etc.) -- must comply with the information security policies found in this and related information security documents. Any unauthorized utilization of Munson Healthcare/Mercy Hospital information is grounds for disciplinary action and/or referral to law enforcement agencies for civil and/or criminal action, when appropriate.

The provisions of this policy apply to all computer, mobile devices and network systems, etc. owned by and/or managed by Munson Healthcare and Mercy North Hospitals. Similarly, this policy applies to all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house, purchased from third parties or used in an Application Server Provider setting) providing heightened wireless security and for extending the physical range of services.

ACCESS MANAGEMENT

Procedures for configuring access controls (e.g., password strength; user obligations with respect to passwords and other access-enabling mechanisms and information, etc.) on information systems and Users’ obligations for use
and protection of their User IDs and passwords are defined in the Access Management policy.

**ANTI-VIRUS MANAGEMENT**

Munson Healthcare’s information resources shall remain current on available anti-virus software updates to ensure effective virus detection and prevention. The following are guidelines that must be followed:

1. All Munson Healthcare computers and servers must have Munson Healthcare’s standard anti-virus software installed and set to scan all files on access and all files inbound.
2. Virus infected computers must be removed from the network until they are verified as virus-free.
3. Any activities with the intention to create and/or distribute malicious programs are prohibited.
4. The Anti-virus System Administrator will be responsible for anti-virus management technology and the use of anti-virus management software at Munson that minimizes the need for Munson user intervention as new viruses, worms, and trojan horses are created and disseminated. The Anti-virus System Administrator will monitor the implemented solution to ensure the product is functioning properly and updates are being distributed as scheduled and to initiate scanning if an immediate threat is detected.
5. All removable media, regardless of where they come from, must be scanned for viruses before they can be used.
6. IS will keep current on the anti-virus software as new viruses are created and/or discovered regularly.

**ELECTRONIC MAIL**

Use of an e-mail account administered by Munson Healthcare/Mercy North is defined in the Use of Internet and Electronic Communication System Policy. Special rules apply to the transmission of confidential information via e-mail and they are referred to in this policy.

**INFORMATION SYSTEMS SELECTION/IMPLEMENTATION AND INFORMATION SECURITY**

Munson Healthcare uses Implementation Methodology for implementing new systems. The following guidelines apply:
1. Information security is integrated into systems life cycle planning through use of methodologies developed and maintained by Information Systems.

2. Information security analysis must be made during the selection of new applications/information systems to ensure a given solution meets or exceeds appropriate information security standards.

3. During a system implementation, various information security needs must be considered, implemented, and tested through various phases of the project, including, for example, remote user and vendor access; configuration of the system and user access in accordance with the Access Management policy; HIPAA-mandated or other types of contracts with vendors and other recipients of confidential data; and, physical security.

4. Complete IS Methodology Application Security Checklist when implementing systems to ensure that information security is addressed appropriately.

INTERNET USE

Access to the Internet is granted to Munson/Mercy Users as defined in the Use of Internet and Electronic Communication Systems Policy. The policy describes the many ways of protecting our network and the data on it.

NETWORK COMMUNICATIONS SECURITY

Munson Healthcare/Mercy North Hospitals must ensure the security of the networks and must be protected from any action that could jeopardize the integrity or security of our information. The following outlines the steps that have been and must be taken on a continual basis.

1. Network connections will be defined as Secure and Unsecure. Under no circumstance may an Unsecured Network terminate directly into a Secure Network perimeter. Connections that are classified as Unsecure must connect into a firewall, DMZ, packet filtering router or extranet. These network isolation devices create a security perimeter that acts as a wall between a secure and unsecure (i.e. external network) network.

2. The network will be segmented to provide a level of isolation between devices, services, and organization for security reasons.

PHYSICAL SECURITY AND WORKSTATION USE
Workstation Use: The following guidelines outline the workstation use within the health system:

1. To prevent unauthorized access to information on the Munson/Mercy network, Users must log out or appropriately secure (i.e. lock office, lock workstation) their PC when away from the PC. Workstations can be locked by using the Ctrl, Alt and Del keys simultaneously. Your Novell password is needed to unlock the PC.
2. Users should situate the computer monitor in such a way as to minimize or eliminate unauthorized viewing of confidential information (i.e., by visitors and others who have no need to know).
3. Confidential and business critical information must never be saved on the c: drive of any computer.
   a. Theft may result in an inappropriate disclosure of confidential information;
   b. Data stored on the PC is not backed up by network utilities;
   c. Theft and/or damage may result in the inability to recover the information.
4. Workstations must be properly disposed of by the IS Department, taking into consideration cleaning of the media and disposing in a way that is environmentally safe.
5. The Use of Internet and Electronic Communication Systems Policy outlines the appropriate use of computers, Internet and other electronic communication systems.
6. The computer user is responsible for any locally stored data (such as those files stored on the C: drive). This should include ensuring backup and disaster recovery plans are in place.
7. The use of workstations not managed by Munson should not be used on Munson/Mercy North premises without prior IS management approval. This approval should only be given in extenuating circumstances where the Munson workstation cannot be provided in a timely fashion or meet the requirements for the job at hand. These workstations should follow the same policies, standards, and guidelines set forth for Munson owned equipment.

Laptops and Other Portable Devices

The following guidelines must be followed when using laptops, notebooks or other electronic portable devices. These guidelines are above and beyond the guidelines listed above for the workstation use:
1. Laptops and other portable devices, such as Personal Digital Assistants (PDAs/Palm Pilots) are prone to theft and/or loss. It is a good practice to never save confidential (Munson/Mercy) data on the c: drive of a laptop or on PDAs and other portable devices.

2. If confidential information must be maintained/used through use of a laptop, save the confidential data to a biometric thumb drive (also called jump drives, memory devices, USB devices, etc.). Use of a biometric thumb drive ensures security of data from unauthorized access.

3. Because laptops are prone to theft, it’s a good practice to physically secure your laptop, particularly those that are stationed on carts throughout the facility in somewhat public areas (such as patient floors). Cables that lock a laptop to a cart, desk, or other device are a cost-effective means to take a small measure to protect your laptop from theft.

4. Refer to the Personal Digital Assistants policy if you intend to use a PDA to support your Munson/Mercy work.

**Wireless Security**

All wireless access points shall be implemented by or approved by IS. Only hardware and software consistent with wireless standards approved by IS shall be used for wireless access points. The following guidelines must be followed:

2. The wireless infrastructure needs to provide user and/or device authentication services and ensure data privacy. Applications using the wireless infrastructure may require their own authentication, authorization and encryption mechanisms to be used by the wireless user at the sole discretion of IS.

4. IS approved encryption standards must be used.

5. Deployment and management of wireless access points is the responsibility of IS.

6. Interference and distribution of services between wireless networks will be resolved by IS and BioMed. IS is authorized to restrict the user of wireless devices when the interference cannot be resolved.

7. New and remodeling plans for buildings should consider the need for and use of wireless networking.
8. Periodic scans for rogue Wireless Access Points will be conducted by IS.

5. **Remote Access Controls:**
6. All remote access to the systems will be controlled and monitored by IS to prevent unauthorized access. IS has the authority to grant, revoke and monitor remote access. The following guidelines must be followed:
   1. Authentication and encryption methods will be implemented for all remote connections to the network.
   2. Unauthorized connections will be strictly prohibited to any part of the network. This includes modems to desktop systems, phone lines, VPNs, etc.
   3. All customers, vendors and business associates will be required to accept security and other applicable legal/contractual agreements prior to the issuance of user accounts and passwords.
   4. Only dial-out modems authorized by IS will be permitted to connect to the network. A risk analysis will be conducted by IS and approvals made based on the outcome.
   5. Only dial-out connections that require authentication at the remote end will be permitted.
   6. All dial-out only modems and phone lines will be configured to reject incoming calls.
   7. Where technically feasible, the dial up connection will be configured to disconnect after 15 minutes of inactivity.
   8. A list of dial out modem phone numbers will be maintained by IS.
   9. Where ever possible, applications should be internet accessible rather than dial up access via a modem. Proper security is required.

7. **Telecommunication Security:**
8. The following guidelines govern the use of telecommunication services:

   1. Land lines are considered secure. The cellular spectrum is considered public domain
and hence is considered insecure. Employees are expected to exercise good judgment when discussing company or patient confidential information over the cellular network and defer the conversation to a secure land based line if necessary.

2. Caution should be used when sending PHI or company confidential information over an alphanumeric pager or text messages on a pager. Make sure the appropriate pager number is entered before sending the page.

3. System administration access to the telephone system (PBX) will only be granted to IS telecommunication personnel. Passwords will change on a regular basis and when a telecommunication analyst leaves the organization.

4. Our maintenance provider monitors the telecommunication switches remotely. Other than technician remote access to the phone switch, no other remote access to any PBX system will be allowed.

5. Voice mail messages may contain PHI and other company information but great care should be given to leaving messages. We encourage/expect a bare minimum amount of information to be left on an answering machine when calling a patient’s household.

6. Voice mail user passwords are required.

7. Out Calling from voice mail, trunk-to-trunk transfers, or any other off-net transfers will not be permitted.

8. Caution should be exercised when sending any PHI via facsimile (FAX) machine. The correct number should be verified and the recipient should be expecting the information.

**Physical Security**

The physical security of the computer room is governed by the Information Systems Department Policy Regarding Access to the Data Center. The following additional environmental and other guidelines apply:
1. All employees are required to have a photo identification badge on at all times to gain access to the facility.
2. Vendors are required to have appropriate hospital ID’s and vendor personnel must be in the presence of an IS member at all time while in the Data Center and/or any wiring closets.
3. Access to the IS Computer Room is logged. Some areas, such as network closets are not logged, however they are locked with limited keys being issued.
4. All major computer equipment is inventoried and tracked by the IS department. Unauthorized removal of any equipment is prohibited.
5. Proper HVAC is provided for all secure areas including the computer room and the telephone rooms. Alarms are activated if critical points are reached.
6. Fire suppression serves the computer room and switch room.
7. Electrical power for critical equipment will be conditioned in accordance with the manufactures specifications. Periodic testing of the electrical, UPS and generators are conducted by facilities/plant engineering.
8. UPS’s are required to prevent critical devices from dropping power in the event of utility power outages. The UPS must be able to sustain operations of critical devices until load is transferred to the generators or a controlled shutdown of critical devices is permitted.
9. All major capital equipment will have a property tag or capital asset tag affixed to it when received from the vendor.

**Monitoring and Auditing:**

Munson IS will perform periodic evaluations of compliance with its security policies and procedures and with HIPAA security regulations. These evaluations include vulnerability tests, access logging and review, identification of security incidents, audits by Trinity Organizational Integrity and Audit Services and identification and management of security incidents and those privacy incidents, which also involve security violations. The following guidelines deal with monitoring and auditing as it relates to security:

1. New informations systems must be installed using the Implementation Methodology maintained by Munson IS. Included in the methodology is a security section. This section helps identify areas of concern from a security perspective.
2. The IS Security Engineer will do vulnerability testing of the mission critical systems as defined in the IS Unplanned Downtime Policy. The vulnerability test must include scans of servers, applications and
networks to determine whether internal or external users could gain unauthorized access to the network, its components and data.

3. Munson will periodically request Trinity Organizational Integrity and Audit Services to perform an evaluation.

4. Munson conducts Quarterly Security Assessments, which consists of “mini” self audits. These results are reported to the audit department.

5. Independent technical audits will be done as time and money permits by an outside firm such as D&T, Unisys, etc. These audits will focus on the security of data and systems.

6. All security incidences will be logged in the Heat, Peers or the HIPAA Incident database. Violations may include, but are not limited to, the following:

   a. Password guessing attempts.
   b. Sharing of passwords/accounts.
   c. Violation of vendor remote access login or logouts
   d. Unsecurely downloading or transmitting PHI.

7. Human Resources is to notify IS on a weekly (daily is preferred if available) of any terminations or changes in employment. Audits are conducted on the mission critical systems at least every 6 months to ensure each user ID is active/being used. If an ID has not been used within 90 days, the ID/Password will be removed with notification sent to the employee via GroupWise To re-enable, a call must be placed to the IS Help Desk at 56053. At the managers request, certain accounts may be left active for 30 days (such as Groupwise which may be needed to obtain needed access to data).

8. IS routinely audits systems containing PHI to identify potentially inappropriate access to PHI. This may include viewing records of a family member, viewing other appealing records an employee does not need to do his/her job. Any violations are referred to the Security Review Board for recommended disciplinary action. The Security Review Board has representatives from all the hospitals in the Munson Healthcare and Mercy North system.

9. Systems that contain PHI and are not considered mission critical are monitored as time permits, based on the level of risk associated with the PHI and the availability of such audit reports. Reasonable monitoring or alternative approaches will be used as appropriate.

10. If an employee is terminated for severe privacy or security breach, their record is flagged in Heat to prevent their access to Munson/Mercy systems through any other area employer.

11. If technical security breaches are detected, they are logged in the databases described above and presented to the IS management team by
the security engineer for discussion. This may include issues with firewalls, proxies, VPNs, virus attaches, denial of service, intrusions, etc.

12. All systems are monitored for downtime and recorded in the downtime log maintained by the IS Operations department. Downtime statistics are presented to Executive Advisory Panel (EAP) and the Mercy North Steering committee (ISSC) on a monthly basis for HBOC Star, Cerner and the Network. Other downtime statistics can be presented as needed. The IS Security Engineer and IS management will review trends and take appropriate actions if the metrics are exceeded.

13. Inappropriate activity will be investigated and corrective action will be carried out in accordance with existing disciplinary action policies. Further, if such monitoring reveals possible criminal activity, Munson Healthcare/Mercy North will provide such evidence to law enforcement officials.

14. Monitoring of systems occurs in many other ways. The following table gives a general overview of the system monitoring that is conducted by the IS department:

**Munson Network Monitoring**

**Applications**

<table>
<thead>
<tr>
<th>Product Used By Platforms Supported</th>
<th>Product Used By Platforms Supported</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ipswitch Whatsup Professional Infra</td>
<td>Infrastructure (other teams as de</td>
<td>SNMP enabled devices, syslog/event log generating devices</td>
</tr>
<tr>
<td>Networks</td>
<td>sired)</td>
<td></td>
</tr>
<tr>
<td>Cacti</td>
<td>Infrastructure (other teams as de</td>
<td>All</td>
</tr>
<tr>
<td>Bindview</td>
<td>Servers and desktops Windows, AD,</td>
<td>Directory admin, Migration, Reporting/Auditing, Compliance monitoring, Identity Admin, Config mgmt, Inventory mgmt</td>
</tr>
<tr>
<td>BMC Patrol</td>
<td>Operations IBM AIX, Sun Solaris,</td>
<td>Monitors server/application</td>
</tr>
<tr>
<td></td>
<td>Win NT</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Domain</td>
<td>OS</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>----</td>
</tr>
<tr>
<td>Big Brother</td>
<td>Operations</td>
<td>Linux, Sun Solaris, HP-UX, IBM AIX, Win NT, Win 2000/2003 server</td>
</tr>
<tr>
<td>Visibility (Pending)</td>
<td>Telecomm / Infrastructure</td>
<td>IP enabled devices</td>
</tr>
<tr>
<td>Softek Panther (Proposed)</td>
<td>Cerner</td>
<td>Millenium</td>
</tr>
<tr>
<td>HP Openview (Sunsetting)</td>
<td>Infrastructure</td>
<td>SNMP enabled devices</td>
</tr>
<tr>
<td>RRDTool</td>
<td>Operations</td>
<td>All</td>
</tr>
<tr>
<td>Custom Scripts</td>
<td>Operations</td>
<td>All</td>
</tr>
</tbody>
</table>

**Backup and Storage of Backups**

All Munson and Mercy North servers (operating systems, applications programs, master data files, transaction files, etc.) are backed up on a regular basis as determined by the Data Owner and the IS department. Individual PC’s are not backed up by the IS department. The schedule of backups is available in the operations department and daily run sheets are filled out or logged to the system in the case of automated backups. The following guidelines are followed:

1. All backups are stored in an environmentally protected and access-controlled facility.
2. The data backup plan is documented in the IS operations
department. Included in this plan is the schedule date and
time, method, type of backup (full or partial) and offsite
storage requirements.
3. Automated backups are done on TSM.
4. Selected backup media is stored off-site.
5. When a new application is put into production, the
Implementation Methodology mandates a review of the
backup requirements including frequency.
6. The data backup plan is reviewed annually by the IS
management.
7. Backup frequencies are consistent with the ability to
recover cost-effectively from a loss or corruption. Because
Munson has an EMR, read-only databases, stand alone
databases and databases stored on the units for inpatients
are maintained.
8. Disaster Recovery plans mandate we test system
recovery at least yearly for all mission critical systems if
not more often.
9. The backup plan and the associated test plans must be
modified whenever there is a significant change to the
application as outlined in Implementation Methodology.
10. RAID, Disk Mirroring or server fail overs are
considered for mission critical systems.
11. The IS Security Engineer and Data Owner must
approve significant changes in established backup plans
and new plans for systems being installed.

**Software Licensing and Media Management**

All computer software owned and installed by Munson or Mercy North will
comply with software copyright laws and appropriately licensed in accordance
with the manufacturer’s requirements. The following are general guidelines
adhered to:

1. Licensing comes in many forms including site license, server based
licenses, individual workstation licenses, concurrent licenses, etc. IS
must understand how each software package is licensed and must abide
by the licensing of each package.
2. Making unauthorized copies of licensed or copyrighted software, even
if only for evaluation copy, is prohibited. The Standards/Purchase for
Desktop Hardware and Software Policy provides more information
regarding purchasing of IS equipment and software.
3. The reproduction of copyrighted software is prohibited unless authorized within the terms of the licensing agreement.
4. Demo software obtained for a trial basis must be removed after evaluation unless properly licensed.
5. All software developed by employees or contractors on behalf of Munson is Munson’s property and protected by copyright law from unauthorized use and duplication.
6. All software purchases must be made through the IS department, which is responsible for software installation and tracking of all software installed.
7. Original software, diskettes, license agreements and other agreements must be maintained by the IS department. This software and documentation may be needed for technical support and to verify valid licenses.
8. Software inventories are conducted annually by IS. Any unauthorized software will be removed.
9. Software media is stored in the IS department under lock and key. Limited personnel in IS have a key and logging of any software removed is required.
10. Software is periodically disposed of by IS only. All media must be erased using magnetic means before disposal.
11. When disposing of hard drives, the drives must be wiped clean of all software and data before disposal by the IS department.

WORK FROM HOME/ OFF-SITE LOCATIONS

Work from home and off-site locations is governed by the Telecommuting Policy Agreement. The policy describes ways to secure the work environment and confidential information.

INCIDENT REPORTING

A Security Incident is any incident that is an attempted or actual compromise to the confidentiality, integrity, and/or availability of electronic information. Workforce members (including volunteers, physicians, employees, students, interns, etc.) are required to report all Security Incidents. Security breaches can be reported to the Risk Management department (via Peers), the Privacy Official at your hospital or for more urgent matters, the Help Desk may be called at x56053; the Help Desk will direct the call for troubleshooting and resolution.
Munson/Mercy’s non-retaliation policy ensures that no one will be punished for reporting an incident.

**INFORMATION SECURITY AWARENESS EDUCATION**

In order to help minimize information security risks, Munson Healthcare and Mercy North Hospitals ensures all members of the workforce have adequate Information Security Education. This education is provided at the start of employment/volunteer services and annually on mandatory day. The education departments and the HIPAA Coordinator review the Information Security Education material annually. The employee’s manager is responsible for all education that needs to happen before the formal education is provided.

**Business Continuity Planning**

Munson maintains and regularly tests business continuity plans to ensure the timely recovery of their critical business process and information resources in the event of a disaster. Munson Healthcare Disaster Preparedness does an annual vulnerability assessment, which includes any threats, including IS type threats to the healthcare system. Based on the vulnerability assessment, Munson Healthcare developed and maintains a Disaster Recovery Plan. The following general guidelines are applicable:

1. All documentation regarding the disaster plan can be found on “the G drive” under Downtime Procedures. The IS Unplanned Downtime Policy outlines all steps necessary in the case of a minor or major unplanned downtime. The concepts found within this policy also apply to the planned downtimes.
2. The Disaster Plan includes policies, job sheets, test plans, organization charts, forms, etc.
3. The Disaster Plan is tested yearly if an actual occurrence has not utilized the plan. The mission critical systems are tested for recovery every year in accordance with the disaster plan. The IS department tries to consider minimal impact to the operations of the hospitals and the cost of running these tests.
4. Paper copies of the disaster plan are located in IS conference room #1 in the South Tower at Munson Medical Center. This location serves as the Incident Command for IS incidents.
5. The IS Incident Command works very closely with Hospital Incident Command and the two plans were developed using the HEICS model.
6. The IS Disaster Recovery team is responsible to make sure the Disaster Plan is updated on a regular basis. After each disaster (planned or unplanned implementation of Incident Command), the Disaster Plan is updated based on the recommendations of the team involved in the disaster.
7. After each disaster requiring IS incident Command, a folder for that
event should be developed with all pertinent documentation.
8. Refer to the IS Unplanned Downtime policy for more information.

**Security Roles and Responsibilities**

Certain roles and responsibilities were established/modified to ensure initial preparation for and ongoing compliance with the HIPAA regulations and other federal and state laws addressing confidentiality and information security.

1. The HIPAA Compliance Officer oversees all HIPAA related activity both from the security and privacy standpoint for all Munson and Mercy North hospitals.
2. The Information Security Officer oversees the information security aspects of the HIPAA regulations for all Munson and Mercy North hospitals. The IS Security Officer reports to the HIPAA Compliance Officer. The Security Officer provides day-to-day direction to the implementation and operations of the HIPAA Security regulations, and the local information security program to ensure that Munson and Mercy information is properly protected. This includes consideration of the confidentiality, integrity and availability of both information and the systems that handle it. The duties include the following:
   a. Performing information security risk assessment.
   b. Preparing action plans in response to the risk assessment.
   c. Ensuring information security is considered in vendor product selections and in-house system development projects.
   d. Assisting monitoring activities.
   e. Overseeing the investigation of information security breaches, and performing other activities necessary to ensure a secure information-handling environment.
   f. Integrating security in Implementation Methodology and Change Control.
3. Each hospital has a Privacy Official that oversees the privacy aspects of that individual hospital.
4. The HIPAA Compliance Officer, the IS Security Officer and the Privacy Officials participate with Trinity Health Services on aspects of the HIPAA activities.
5. The HIPAA Oversight Committee, along with EAP (Executive Advisory Panel at Munson) and ISSC (Information Systems Steering Committee at Mercy North) oversee all activities related to HIPAA.
6. The IS Security Engineer, Security Analyst and Login ID Coordinator both reports to the Security Officer. They oversee all technical aspects of the security regulations as well as log in activity. The Security Engineer’s responsibilities include the following:
a. Design network security solutions.
b. Design and manage the vulnerability scanning and intrusion detection program.
c. Define content filtering and monitoring services such as virus detection.
d. Define security standards such as acceptable encryption technology.
e. All other technical responsibilities as it relates to security of data and systems.

7. The Security Review Board is responsible for making recommendations related to violations of the HIPAA regulations, including employee sanctions and measures that may be taken to prevent such violations in the future.