E-Mail and Internet Use, 100-006

Purpose

- Establish guidelines for the use of Marquette General Health System (MGHS) e-mail/Internet systems to protect the integrity and confidentiality of MGHS patient and business information.
- For the purpose of this policy "users" include employees, interns, volunteers, contracted personnel, students, residents and other personnel using the MGHS e-mail/Internet systems.
- Electronic mail ("e-mail") is defined as a communications tool whereby messages are prepared, sent and retrieved electronically.
- Internet is defined as a communications tool whereby business information, reference material and messages are sent and retrieved electronically. These technologies may also be applied to the internal MGHS "Intranet". These systems are typically Web browsers (http), e-mail (smtp), file transfer (ftp), and news groups (nntp).

Policy

MGHS e-mail/Internet systems are provided to support patient care, business communications, clinical research, education, and advanced computing for all institutions connected to the MGHS network; use for informal or personal purpose is prohibited.

MGHS owns the equipment and software making up the e-mail/Internet systems, and all messages and transactions generated by or handled by these systems, including back-up copies. Consequently, users do not have a right to privacy in their use of the e-mail/Internet systems. MGHS reserves the right to monitor, audit, delete, and read e-mail messages and monitor Internet activity. E-mail and Internet activity will be monitored routinely or as deemed necessary by management and Human Resources. Additionally, as corporate records, records of e-mail/Internet activity are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other process without notification to or permission from users. Consequently, users should always ensure that the business information contained in e-mail/Internet messages is accurate, appropriate and lawful.

Acceptable Use

MGHS e-mail/Internet systems are to be used for business purposes only such as:

1. Communications to support patient care, clinical research, education, business communications, and advanced computing
2. Communication and exchange of information for professional development and to exchange or debate in field of knowledge

3. Use for university-association, government-advisory or standards activities related to MGHS research education or business activities

4. Use for administrative business communications

Unacceptable Use

MGHS is committed to providing an environment that is free of discrimination, including sexual harassment. No information should be viewed, stored or accessed on the e-mail/Internet systems, MGHS computers OR the MGHS network which creates an offensive work or educational environment. To this end, harassing or obscene messages, pictures and/or materials must not be transmitted via the e-mail or Internet system on or off site. Inappropriate messages, pictures, access and/or materials include but are not limited to:

1. Fraudulent messages – Messages sent under an anonymous or assumed name with the intent to obscure the origin of the message

2. Messages or sites that harass an individual or group because of their race, sex, religious beliefs, national origin, physical attributes or sexual preference

3. Messages or sites that contain obscene or inflammatory remarks

4. Messages or sites that contain inappropriate adult content such as pictures, graphics, or stories

MGHS reserves the right to utilize software that will prohibit, filter or monitor access to sites and e-mail messages with questionable content. Users are advised that attempts to access or transmit inappropriate material may be monitored and documented in the Unusual Occurrence form.

Users must not use e-mail/Internet systems for personal or private business activities that may include but are not limited to:

1. Personal for-profit activities (e.g., consulting for pay, sale of MGHS assets).

2. Solicitation for outside business ventures, organizational campaigns, or political or religious causes

3. Electronic chain letters and other forms of non-business related mass mailing

User Responsibilities

All users must strictly observe the following rules when using the e-mail/Internet systems:

1. Users should regularly check and delete unneeded e-mail

2. Users are not to share their passwords with any third party, nor may they be shared with another user(s).

3. Users must honor rules of copyright and personal property, and refrain from duplicating copyrighted information, including software using Internet resources.

4. Users must not use an e-mail account assigned to another individual to either send or receive messages. If there is need to send or receive messages for other hospital users (e.g., while they are away on vacation, leave, or sick), message forwarding, mail delegation, or other authorized information-sharing mechanisms must be used instead.

5. Users must not transmit MGHS information, including patient information to unauthorized recipients.

6. Users must have up-to-date anti-virus running at all times.
Protected Health Information

- Protected health information (PHI) is not to be transmitted via the Internet or e-mailed outside of the MGHS Network without the use of encryption. The Information Technology department should be contacted in the event that encryption capabilities need to be setup or confirmed.
- Prior to transmitting PHI, the user will comply with Release of Information policy to ensure legal authority for the disclosure exists. PHI transmitted via the e-mail/Internet systems will be treated with the same degree of confidentiality as the medical record.
- All e-mail messages must include the following statement:
  - "This email and any files contained in it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. Any unintended review, use, distribution or disclosure is strictly prohibited."
- E-mail/Internet messages and activity by users may not necessarily reflect the views of MGHS, its Officers, Directors, or Management. Any inappropriate communication is contrary to MGHS policy and outside the scope of the intended use of the e-mail/Internet systems. MGHS will not accept any liability in respect of such communication, and the user responsible will be personally liable for any damages or other liability arising.

<table>
<thead>
<tr>
<th>Attachments:</th>
<th>No Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Committee</th>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edward Banos: Chief Executive Officer</td>
<td></td>
<td>03/2014</td>
</tr>
<tr>
<td>Linda St. Aubin: Secretary</td>
<td></td>
<td>04/2014</td>
</tr>
</tbody>
</table>
Access to Computers, Systems and Networks, 100-139

Purpose
For the purpose of this policy, "users" includes employees, interns, volunteers, contracted personnel, students, residents, and anyone using MGHS computers, systems, or network. "System Security Administrators" includes employees responsible for supporting and/or administering MGHS computers, systems, or network.

Remote access users are defined as anyone accessing hospital computers, systems or network remotely. Remote access implementations covered included but not limited to telephone modems, digital service lines, virtual private networks, cable modems and any and all mobile devices such as iPhone, iPad.

Policy
System Security Administration
Each system containing hospital-proprietary or patient-confidential information must have a System Security Administrator. Responsibilities include:

- Granting user access (user id, password) after receiving proper authorization via the Security Authorization Request (SAR) form.
- Monitoring, validating, and making recommendations for disciplinary action for breaches of security.
- Maintaining system and user passwords, and password security.
- System maintenance and support, including routine backups.

Information Technology (IT) will provide system Security Administration for those systems located in the Information Technology Department. The Director, Information Technology will provide authorization for computer systems to reside outside of the Information Technology Department, and will only be granted if the area where the system resides meets industry fire and disaster standards for computer equipment.

It is the Department responsibility if the computer system is located outside of Information Technology to provide for System Security Administration that includes:

- Granting user access (user id, password) after receiving proper authorization via the Security Authorization Request Form.
- Monitoring, validating, and making recommendations for disciplinary action for breaches of security.
- Physical security.
• System security and confidentiality
• System maintenance and support, including routine backups

System and Information Access

Only authorized users shall have access to MGHS computers, systems and network on a need to know basis for purposes authorized by management as necessary to carry out their job responsibilities. Authorization will be defined via the SAR and approved by the appropriate department manager or Senior Executive as outlined below.

Security and Access Procedures

The department manager or Senior Executive must submit a SAR for any individual that needs access and/or remote access to MGHS computers, systems, or network. Department managers will determine which individuals get access using the following guidelines:

• Users will not get access unless they have a need for access to perform duties.
• Users will have the minimum access necessary to perform duties.
• Health care providers will have access only to data of patients they have responsibility for, with emergency override to access other patients' data to respond to emergencies.
• Access is limited to necessary tasks, such as read-only, read and update.

Department managers and Senior Executives will ensure that users receive training as specified in policies "Employee Orientation" and "Training, Observation, Education of Persons not Employed by MGHS", prior to submitting a SAR.

Registration access requires additional approval. Registration access must be approved by Patient Access.

Access Establishment

Access establishment is the process of granting access to a user via the SAR. Upon receipt of the SAR, Information Technology will process the request as follows:

• Requests will be reviewed by the Help Desk for accuracy and routed to the appropriate System Security Administrator via the Security Access Management (SAM) system.
• The appropriate System Security Administrator will grant access as authorized by the SAR within 5 business days of receiving the request using the information in SAM.
• The Help Desk will route the password letter to the user in a sealed envelope. Passwords will not be disclosed via telephone without proper verification or unencrypted e-mail.
• IT will be responsible for installation and configuration of software at the user's workstation if necessary for access to the requested systems.

Access Modification

Access modification is the process of changing a user's access via the SAR. Department managers may determine that a user needs more, less, or changed access because of a change in duties, in which case a SAR must be submitted so that current level of access may be modified to reflect the new access requirements. Upon receipt of the SAR, IT will process the request as follows:

• Requests will be reviewed by the Help Desk to ensure accuracy and routed to the appropriate System Security Administrator via the SAM system.
- The System Security Administrator will modify or revoke access privileges according to the information provided in SAM.
- IT will be responsible for installation and configuration of software at the user's workstation if necessary for access to the requested systems.
- Department managers will be responsible for notifying the IT Help Desk of any information or software on the workstation that needs to be transferred, archived or disposed of.

**Access Termination**

Access termination is the process of revoking a user's access via the SAR. When a user no longer needs access, the department manager must submit a SAR to discontinue access. When a user terminates employment, Human Resources will update the Human Resource Information System (HRIS) or submit notification via e-mail by the user's last day of employment. Upon receipt of the SAR or HRIS notification, IT will process the request as follows:

- Requests will be reviewed by the Help Desk to ensure accuracy and routed to the appropriate System Security Administrator via the SAM system.
- The System Security Administrator will revoke access privileges according to the information in SAM.
- IT will be responsible for uninstalling Lotus Notes ID files, e-mail archives, and licensed software from the user's workstation if applicable.
- Department managers will be responsible for notifying the IT Service Center of any information or software on the workstation that needs to be transferred, archived or disposed of.

IT will keep records of the security and access procedures as outlined above for each such user for not less than six years from the date of access termination.

**Remote Access**

Remote access to the MGHS Network and Computer Systems is for the authorized user's exclusive and individual use on a secured computer. It is the responsibility of users with remote access privileges to the MGHS network to ensure that their remote access connection is given the same consideration as the user's on-site connection to MGHS.

Remote access is limited to select applications and application remote accessibility will be determined by need and compatibility with the remote access technology being used.

Users must abide by all remote security requirements outlined in this policy and must take reasonable precautions to protect any MGHS hardware, software, and information from theft, damage, and misuse. These include but are not limited to, compliance with software license agreements, proper safeguards and disposal of sensitive information and compliance with all hospital policies regarding computer and system access and patient confidentiality. Up-to-date anti-virus and desktop firewall configured to scan e-mails, downloads, and all file types must be running at all times.

**User Responsibilities**

Users have the responsibility to report breaches and policy violations via the "Unusual Occurrence Form," to preserve patient confidentiality, and protect MGHS proprietary information. In addition, users must comply with the security standards outlined below:

- Do not access data for which there is no need to know, even if security mechanisms fail or are absent. A lack of security mechanisms does not imply that the information is public.
• Do not access data outside that granted by the approval process. Remote users must use accounts only to access the applications listed on the SAR for remote access.
• Remote access users are to use remote access on an active basis, meaning only as needed and in no way on standby or inactive basis in order to maintain a connection.
• Remote access users are prohibited from accessing the MGHS network from computers that do not meet the security requirements and prohibited from establishing remove access connections via dial-up modems or other remote access software or hardware appliance without prior written approval via an SAR.
• Change passwords when prompted by electronic systems.
• Use passwords with a minimum of eight characters of which must contain three of the following four, upper case, lower case, numeric or special characters.
• Use computers, systems, and network for business related functions.
• Log off sensitive business or patient systems when leaving the computer unattended for any period of time.
• Use password-protected screensavers or privacy screens to prevent unauthorized view of patient information. If a password-protected screensaver is used, the password must be communicated to IT to allow for support of the workstation.
• Do not share passwords with anyone. Do not use someone else’s password, even with their permission. Exception for IT staff and System Security Administrators when needed for system or network support or troubleshooting.
• Do not keep passwords in an unsecured location, such as an unlocked desk or file cabinet, tacked to a bulletin board, or taped to the side of a monitor or keyboard.
• Only encrypted electronic media (e.g. CD’s, encrypted Jump Drives and disks), containing sensitive business or patient information and allow access only to authorized individuals are to be used.
• Properly dispose of electronic media or contact IT for appropriate disposal.
• Take preventative measures to protect data, systems, and network from viruses and other forms of malicious code. For example, do not open e-mails or files from unknown sources or download software from the Internet without approval from IT. Intentional or accidental introduction of a virus or other malicious code to MGHS systems or network may be subject to potential legal action.
• Contact the Help Desk if password(s) are forgotten, lost, or compromised.
• Do not leave printers unattended when printing sensitive business or patient information. This is especially important when multiple users share a printer or the printer is in an area where unauthorized personnel have access.
• Users are responsible for storing information that if lost or destroyed, would be difficult to recreate, on a network drive for backup purposes. Users are responsible for backup of information if stored locally onto their workstation.
• Remote access users are prohibited from savings any patient information on the local hard drive of non-MGHS owned computers and are responsible for providing adequate safeguards and disposal of patient information.
• Do not use MGHS systems and network resources to solicit for outside business ventures, organizational campaigns, political, or religious causes.
• Do not enter, transmit, or maintain communications of a discriminatory, harassing, derogatory or inflammatory nature about an individual’s race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition or materials that are obscene or X-rated.
• Do not enter, maintain, or transmit any abusive, profane, or offensive language.
All intellectual property developed or conceived of while users are working at home or alternative worksites are the exclusive property of MGHS. This includes but is not limited to memos, plans, documentation, programs, software and other materials.

Monitoring

Computers, systems, networks, and other computer equipment are the property of MGHS, wherever located, although patients and others may have rights of access to the data. MGHS is required to ensure the integrity of its data and user's activities comply with MGHS policies and procedures, laws, professional ethics, and accreditation requirements, and will monitor network and system activity routinely or as deemed necessary by management and Human Resources. Users have no expectation of privacy when using MGHS computer equipment, wherever located.

Audit logs of remote activity are to be maintained for all remote access connections that have the capability to track connectivity.

Software

Only authorized software may be utilized on MGHS computer equipment or on the MGHS network. Software must be examined and approved by IT prior to use. Software used to process patient information must be examined and approved by IT before purchase and implementation to ensure it meets MGHS and regulatory security requirements.

IT is responsible for protecting the MGHS network against malicious code whenever possible by ensuring that computer equipment connected to the MGHS network has updated anti-virus installed and running at all times whenever possible IT must provide for data and system backup to allow for data and system recovery with minimal disruption to business operations.

Hardware

Only authorized hardware may be utilized on the MGHS Network. Hardware must be examined and approved by IT prior to use. MGHS computer equipment may not be used outside of the facility without prior approval from the appropriate department manager. Conditions for offsite use of MGHS computer equipment include the following:

• Computer equipment must be under the control of the user authorized at all times.
• User is responsible for providing appropriate safeguards, such as locked storage compartments, to secure computer equipment and data from unauthorized users.
• Users must immediately report losses, damages, or security breaches regarding such equipment to their department manager.
• Computer equipment is not to be used for private purposes nor used by unauthorized individuals.
• Authorized offsite use of MGHS equipment must be documented and communicated to Human Resources to ensure collection of MGHS computer equipment during transfer or termination.

It is the responsibility of the Information Technology department to maintain an updated software and hardware inventory for computer equipment connected to the network.
Use of Wireless and Portable Devices for PHI

When using wireless or portable devices, including but not limited to personal handheld devices, CD's, high-capacity drives, memory sticks, tablets, laptops for PHI and/or business information, following security standards must be met:

- Password protection – for data synchronization, data access and wireless transmission - minimum 8 alpha-numeric characters
- Password protection – for device power-on
- Automatic log-off or shut-off
- Up-to-date Anti-Virus Protection
- Encryption – for PHI synchronization and wireless transmission - 128-bit

Approval for the use of personally-owned wireless or portable devices for PHI can only be obtained through the appropriate department head and/or Senior Executive via the Security Authorization Request (SAR) form and will only be granted if the security standards outlined above are met. Furthermore, such data must be returned and properly destroyed upon termination of employment or change in access requirements.

Use of personal computer equipment, including but not limited to wireless and portable devices, to use, record, or store information relating to MGHS, its patients, or business activities subjects the user to the terms of this policy.

<table>
<thead>
<tr>
<th>Attachments:</th>
<th>No Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee</td>
<td>Approver</td>
</tr>
<tr>
<td>Edward Banos: Chief Executive Officer</td>
<td>03/2014</td>
</tr>
<tr>
<td>Linda St.Aubin: Secretary</td>
<td>04/2014</td>
</tr>
</tbody>
</table>
MARQUETTE GENERAL HEALTH SYSTEM
MARQUETTE, MICHIGAN

SYSTEM HUMAN RESOURCES POLICY

SUBJECT: Dress Code and Personal Appearance

POLICY NO: 200-052
EFFECTIVE DATE: 12/6/1999
REVISION DATE: 2/4/02, 1/12/04, 7/15/07, 1/14/08; 6/1/10

DISTRIBUTION: All Departments

Authorized By
A. Gary Muller, FACHE
President & CEO

Our work environment is conservative in many respects, including the values of many of those within our communities to whom we strive to provide excellence in patient care and customer service. It is, therefore, essential that all employees project an image that is professional and will inspire our customers' confidence in both our services and providers. It is the personal responsibility of each employee to present a professional appearance of a conservative manner that is reflective of our patient care focus and exemplifies the image of the health care professions.

Each department is responsible for its own dress code special regulations based on appropriate criteria for the services it provides. Departmental uniform color requirements, if any, must be approved and included in departmental policy. All departmental dress codes are to be approved by, and kept on file with, the Sr. Director of Human Resources.

The following guidelines are to be enforced, in conjunction with individual departmental policy, by the employee's immediate supervisor, or other manager as appropriate:

Clothing
- Clothing will be clean, neat, and in good repair at all times. Clothing shall be coordinated and in good taste.
- Hosiery/socks to cover exposed leg, ankle, and foot, must be worn by all employees providing direct patient customer service or working in a patient care department. Shoes must be worn and should be appropriate to the System and to each employee's particular job and department. Shoes, like all other clothing, will be clean, neat, and in good repair at all times.

Hair
- All employees are to keep hair clean and neatly combed.
- For those employees in patient care areas, hair is to be off the shoulders. Hair longer than shoulder length MUST be worn in a fashion that is up and off the shoulders.
- To meet hygiene standards, some employees will be required to wear hair nets or caps. Hair and hand contact provide possibilities for contamination. Particular cautions should be observed whenever patient or food contact is made.

Beards and Moustaches
- Beards and moustaches may be worn, providing they are clean, neat, and well trimmed.
- The length of a beard will be kept off the clothing or uniforms.
A mask or hooded mask should be worn as appropriate whenever the possibility of contamination exists.

In incidents where beards or other hair will interfere with the safety of the work environment, it will be necessary for the hair to be removed or trimmed to such a degree that the hazardous situation it creates is eliminated, i.e. proper fit and seal of respirator. When an employee's job requires utilization of this equipment, they should remain prepared at all times for its use. This will ensure that the hair will not interfere with safe and effective use of personal protective equipment.

Cosmetics, if used, should be worn in moderation.

**Scented personal products**
- Perfumes, after-shave lotions, colognes and heavily scented personal products are not permitted in patient care areas, and are discouraged in non-patient care areas, due to sensitivity (allergies, illness) of patients and other employees. Complaints from others regarding scented products will result in the employee being required to refrain from wearing such products.

**Hygiene**
- Employees are to maintain proper hygiene, cleanliness, and appearance, and remain odor-free.

**Fingernails**
- Personnel coming into direct contact with patients may not wear artificial nails.
- Hands and fingernails are to be kept clean.
- Fingernails are to be clean and at a reasonable length.
- Employees having direct contact with patients may not have nails that extend beyond the fingertip.
- Fingernail polish may be prohibited in certain patient care areas. In patient care areas where polish is allowed, the polish shall be intact and of a soft hue.

**Jewelry**
- Jewelry should be worn in moderation unless departmental policy prohibits its use in its entirety.
- Jewelry should not interfere with the performance of your job.
- Employees are not permitted to wear any visible pierced jewelry, other than in the ears. Other visible pierced jewelry must be removed. Covering is not acceptable. Earrings shall be kept to a conservative size and number.

**Tattoos**
- Tattoos shall be covered to the best of one's ability.
- Any tattoos that cannot be covered shall be conservative and not offensive.

**Scrubs and Other Uniforms**
- Scrubs will be provided to only those departments as mandated by MDPH and OSHA requirements. MGHS will launder all furnished scrubs. Under no circumstances should any MGHS owned scrub uniforms be removed from the premises.
- Personnel working in semi-restricted or restricted OR/procedure areas are not permitted to wear their scrubs outside the building to minimize contamination (e.g. animal hair, cross contamination from uncontrolled environments).
- Scrubs may not be worn by employees of non-patient care providing departments.
- Departments may require employees to wear and provide their own scrubs. This will be directed by departmental policy.
Cover up Jackets
- Cover up jackets required in conjunction with required scrub uniforms will be provided.
- Disposable cover gowns will be provided for departments where certain tasks require this protection.
- Where required, coveralls will be furnished and laundered by the System. Coveralls will not be worn in patient care areas unless directed by a supervisor.

Students
- All students affiliating at MGHS are expected to wear either the uniform that is associated with their particular school or the specified dress code for the department with which they are affiliating.

Casual Days
- Certain days of the year may be designated as casual days. On any days designated as casual days, all policy requirements remain in effect, unless otherwise excepted in the casual day notification.
- Every Friday is designated as MGHS Attire Day. On Fridays, employees may wear MGHS shirts and denim pants (other than blue), if appropriate for their department. All other guidelines set forth by this policy apply.

The following list is not intended to be all-inclusive, but is intended as a guideline to attire.

Appropriate
- Dresses/Skirts/Skorts (length cannot be shorter than three inches above the knee)
- Suits with ties/Pant Suits/Tailored slacks with coordinating jacket
- Professional Blouses/Shirts/Sweaters with modest necklines
- Pants in business suitable fabrics or “docker” style
- Uniforms/Scrubs as described by policy

Inappropriate
- Denim, or any material resembling denim, of any color unless otherwise approved in departmental policy.
- Casual T-shirts (including MGHS logo t-shirts)
- Shorts
- Stretch pants/Stirrup leggings
- Any inappropriately revealing or tight-fitting clothes (e.g. bare stomachs, cleavage)
- Tank tops, halter tops, crop tops
- Thong type sandals, flip flops
- Sweats

Any violations of the dress code will result in the employee being sent home to change into acceptable attire. During this absence, vacation time will be utilized, if available. Violations may also result in corrective action, leading up to and including discharge from employment.

Direct any questions regarding the interpretation of this policy to the Sr. Director of Human Resources for clarification.

End of Policy
Marquette General Health System (MGHS) attempts to make parking available at no cost to patients, families, visitors and employees. Limited parking is available to those employees who elect to park on hospital property. In an effort to continue to provide the best possible customer service, including convenient parking for our guests, it is essential that employees cooperate in complying and enforcing this policy.

**Vehicle Identification**
Those employees who choose to use hospital-owned parking lots during work hours must display a valid employee parking tag on the mirror of the vehicle at all times when parked in a designated employee parking area. Human Resources will provide MGHS parking tags to all employees. Lost parking tags will be reissued at a cost of $20. Damaged tags may be exchanged at no cost.

Vehicles found parked in employee-designated parking areas not having a valid MGHS-issued parking tag will be ticketed, towed or may have a wheel-boot installed. Failure to display the MGHS parking tag while working will result in disciplinary action and all violations will be reported to Human Resources for inclusion in the Performance Evaluation Tool system.

Vehicles identified via license plate (confirmed through the Secretary of State/Department of Motor Vehicles) as being MGHS employees who are parked in patient/visitor parking during their working hours will be subject to corrective action, ticketing, or towing at the employee’s expense. Employees who are observed parking in these areas should be reported to Security for immediate removal. Employees are prohibited from utilizing non-employee parking areas while they are working.

When an employee or family member is a patient or visitor, the MGHS parking tag should be removed from the mirror of the vehicle. You may choose to contact MGHS Security at 361-3368 to have the vehicle recorded as approved for parking in “Patient Parking” for that occurrence.
MGHS Parking Availability

Street/Public Parking is available on all city-owned streets surrounding the facility including, but not limited to, Magnetic, College, Lee, Alger, Fourth, Fifth, Sixth, Crescent, Harrison, and parts of Kaye Avenue (which is owned by Northern Michigan University). Street/public parking is available at no cost. *(Note: Parking on the Northern Michigan University campus, St. Michael’s Church, Messiah Lutheran Church, or other neighboring properties is prohibited by these organizations and may result in towing or ticketing by those organizations at their discretion).*

All employee-parking areas that are gated are accessed utilizing employee magnetic cards. Human Resources will issue these magnetic cards to all employees. No more than one card will be issued per employee. Lost cards will be re-issued at the employee’s expense at a cost of $40.

Parking Lot A provides controlled parking to be used only by, and is reserved for, visitors and patients. The lot provides designated spaces for patients of Hemodialysis, Radiation Oncology, Valet Parking and others, as well as a maximum of five spots for Family Birthing Center on-call physicians. Employees may use this parking lot on weekends and after 2 p.m. on weekdays if they will be exiting the lot prior to 7 a.m.

Parking Lot B provides gated parking to be used only by, and is reserved for, employees who have elected to display an MGHS-issued parking tag and follow the parking directives identified in the policy.

Parking Lot C provides gated parking to be used only by, and is reserved for, employees who have elected to display an MGHS-issued parking tag and follow the parking directives identified in the policy. A separate section in the northwest portion of Lot C is designated for MGHS Visitors only.

Parking Lot D provides gated parking to be used only by, and is reserved for, employees who have elected to display an MGHS-issued parking tag and follow the parking directives identified in the policy.

Parking Lot E (across from the ’81 Building South Entrance) provides a minimum number of parking spaces available for patients, visitors and employees. Designated spots are restricted for On-Call OR, On-Call EMS, On-Call Imaging Staff and Trauma Surgeon parking.

Parking Lot F provides gated parking to be used only by, and is reserved for, employees who have elected to display an MGHS-issued parking tag and follow the parking directives identified in the policy.

Parking Lot G provides gated parking to be used only by, and is reserved for, employees who have elected to display an MGHS-issued parking tag and follow the parking directives identified in the policy.

Blood Donor Lot provides parking for Blood Donor visitors, designated spaces for Blood Donor Center employees and MGHS vehicles only.
Emergency Department Parking Lot provides parking for Emergency Department patients and includes designated spaces for physicians and Foundation guests on the North side. It is not to be used by employees. All physicians must display an MGHS-issued "Physician Parking" tag visibly in their vehicles, or may be subject to ticketing, towing, or wheel-booting as noted above.

Wallace Side Lot (Between Wallace Building and St. Luke's Building) provides parking for hospital vehicles, IT vehicles, and service-designated vehicles. It is not to be used for general employee parking. Certain employees who utilize MGHS vehicles in their work may replace the vacant spot with their personal vehicle during their work shift if displaying an appropriate MGHS Parking Permit on the dash.

Old Emergency Department Parking (Between the '81 Building and the '69 Building) provides parking for patients, visitors, and designated hospital employees — generally those who are on-call for EMS and the Operating Room. This area also includes designated parking spaces for Michigan Department of Corrections and Law Enforcement vehicles.

Parking Deck

Parking Deck Level 1 provides restricted physician parking. All physicians must display MGHS Medical Staff parking tags in their vehicles.

Parking Deck Levels 3 and 4 provides restricted patient and visitor parking. Parking on level 3 is not allowed by employees on any shift, at any time. Parking on Level 4 is permitted for employee overflow after 2 p.m. only.

Parking Deck Levels 2, 5 and 6 provide restricted employee parking. All employees must display MGHS employee parking tags in their vehicles. Non-tagged vehicles risk ticketing, wheel-booting, or towing at the owner's expense. Volunteer designated spaces are located on levels 2 and 4 of the Parking Deck. Vehicles must have volunteer parking tags displayed and visible to utilize these spaces. Other spots are identified for specific patient populations, such as Expectant Mothers.

All vehicles, on all levels, are prohibited from parking in the corners or on the abatements of the Parking deck. Motorcycle parking is allowed on the abatement of level 2 in the Parking Deck. For safety reasons, cameras monitor the deck. For safety reasons, the speed limit in the Parking Deck is 5 mph. All employees are to avoid parking vehicles with a plow in the Parking Deck.

Motorcycle parking is in designated automobile spots, or in the identified motorcycle areas. Motorcycles are not to park near the campus adjacent to doors in non-parking areas.

Afternoon or night shift employees may park on Level 4 beginning at 2:00 p.m. If there are no available spots in designated employee levels of the Parking Deck. Parking in valet spaces or reserved spaces is prohibited.

On-call employees may park on an employee level in the Parking Deck and access the Skywalk using the Skywalk entrance to the Neldberg Building by using their ID badge or "buzzing" the Hospital Contact Center for access. Delays may occur during certain times with the Contact Center not able to release the doors immediately. Please be courteous while awaiting their response. On-call employees may also park in designated spaces identified for their specific
department/responsibilities, but display an On-Call Employee permit in their front windshield. Employees using an On-Call Employee permit when not responding "on-call" will be subject to disciplinary action.

Specific Patient Parking

Spaces are currently reserved for specific patient parking in a number of areas. Parking in such areas is by permit only. These areas include, but are not limited to:

- Cardiac Rehab (between Parking Deck and Neldberg Building)
- Radiation Oncology (Lot A)
- Rehab Services (Parking Deck – 3rd level)
- Hemodialysis (Lot A)
- Other areas, as those designated for expectant mothers.

Escorts
MGHS Security Police officers may be contacted at 361-3368 or paged through the hospital operator by employees for an escort to/from the car/worksite at any time. This is strongly encouraged for employees leaving alone after hours.

Parking Violations
The MGHS Security Police, Marquette City Police, EMS, Maintenance, and other employees may randomly patrol parking lots. Employees are strongly encouraged to report parking violations to the MGH Security Police at 361-3368. If possible, obtain the make and model of the vehicle and license plate number.

Employees who choose not to use street or public parking and elect to utilize MGHS Parking Lots B, C, D, E, F, G or the Parking Deck Levels 2, 5, or 6 may be subject to towing, wheel-boot installation, and/or disciplinary action if it is found that the restrictions identified in the Parking Policy are not adhered to. If the vehicle is not employee-owned, the individual will be contacted and asked to remove their vehicle from the restricted areas. Absent any extenuating circumstances, failure to do so will result in the vehicle being towed at the owner's expense.

Examples of parking violations (including, but not limited to):
- Parking in a non-employee area when on duty
- Parking in an employee area without display of assigned MGHS parking tag
- Parking inappropriately (double-parked, on the grass areas, in a restricted area, or other)
- Parking in a handicapped spot without proper display of State of Michigan approval tags
- Failure to report damage to property, gates or other vehicles

Employee parking violations will require Department Manager's to issue corrective actions. The employee's Department Manager will provide Human Resources with a copy of corrective actions when completed. Ongoing problems may result in a wheel-boot being applied to the vehicle. Damage to vehicles during wheel-boot installation or removal is the responsibility of the vehicle owner. An additional warning may accompany the wheel-boot installation and will be issued to the employee through Human Resources or from their Department Manager. A parking warning will be placed on the vehicle indicating a wheel-boot has been applied. Procedure for wheel-boot removal will apply, including contacting MGHS Security at 361-3368. Timeframe for removal is done based on availability of the Security Police.
Additional violations of parking requirements may result in the vehicle being towed at the owner's expense. The cost of vehicle towing will be billed to the employee directly from the towing company. A copy of the violation resulting in towing will be provided to the Department Manager and also copied to their Executive Leadership team member.

An employee will have **three business days to obtain an MGHS-Issued parking tag in the event it is lost**. A reminder may be placed on the employee vehicle indicating the date the tag must be displayed on the rearview mirror or front dash.

Employees with oversized vehicles, or those equipped with plows are to park in rows on the perimeter of designated lots to maximize as much space as possible. All vehicles are to be parked within the identified lines, avoiding taking up multiple spots.

Marquette General Health System is not responsible for lost, stolen, or misplaced items stored on or in vehicles, motorcycles, and bicycles, or for damage to any vehicles, which are parked in the parking lots or Parking Deck.

This policy is in effect 24 hours per day/7 days per week.

**Off-site Clinics and Locations**

Off-site clinics are governed by the parking policy in effect for the facility they are located in or their specific department policy.

*End of Policy*
SCOPE:

All facilities affiliated with the Company including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, physician practices, and all corporate departments and divisions.

PURPOSE:

To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with workforce members, and external entities to protect Company information resources, including confidential patient information.

POLICY:

A. Information Confidentiality and Security Agreements with Individuals

1. All Company employees and other individuals granted access to Company and/or patient protected health information (PHI) must sign and abide by the Confidentiality and Security Agreement (Agreement). The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.

2. Entities not owned and individuals not employed by the Company or an affiliate of the Company shall sign an Agreement if (i) the entity and individual provides services on premises owned or operated by the Company or an affiliate of the Company; (ii) the entity or individual has remote access to the Company's or its affiliates' information systems; or (iii) the entity or individual has access to Company's confidential information or PHI. All contracts for these services must contain enforcement provisions that are consistent with the Company's or its affiliates' disciplinary policies.

3. Any changes to the Agreement must be reviewed and approved in advance by Corporate Information Technology & Services (IT&S) and Legal Counsel.

B. Business Contracts with Business Partners. Relationships with an external entity involving access to Company information systems or the exchange, transmission, storage and maintenance or use of sensitive Company information require a formal contract including provisions to protect the confidentiality and security of Company information and/or systems in accordance with federal HIPAA Security Requirements.
C. **Sanctions.** Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the Information Security Policy, LPNT.IS.SEC.001, Protected Health Information Incident Response, HIPAA.GEN.007 and the Discipline section of the Code of Conduct. Violations may be reported in accordance with the HIPAA Complaint Process & Disciplinary Actions Policy, HIPAA.GEN.003 located on the Compliance SharePoint site. In addition, violations may be reported to the Ethics Line at 1-877-508-LIFE.

D. **Policy Exceptions.** Exceptions to Information Security Policy are to be submitted to the Corporate IT&S Information Security Policy key contact for review and approval.

**PROCEDURE:**

A. The Confidentiality & Security Agreement form will be posted and maintained by Corporate IT&S on the Company Intranet located under Security.

B. Each Company and Company affiliate employee and member of the workforce (e.g. volunteers, contract labor, etc.) must sign the Agreement at the time of employment. The completed Agreement will be maintained in the individual's personnel folder.

C. Each physician and allied health professional must sign the Agreement at the time he or she is appointed to a facility's medical staff. Completed Agreements will be maintained in the individual's credentials file.

D. Non-employed physician office staff must sign the Agreement at the time information system access is granted. Completed Agreements must be maintained in a central location by the Physician Support Coordinator or individual with a similar role in the business unit.

Representatives of vendors and other external entities must sign the Agreement at the time information access is granted. Completed Agreements must be maintained in the individual contract folder or system (e.g., ShiftWise) by Facility personnel.

**REFERENCES:**

**Government:**

American Recovery and Reinvestment Act of 2009, Title XIII, Health Information Technology, Subtitle D: Privacy

Medical Records Confidentiality Act of 1995 (MRCA)

Health Insurance Portability and Accountability Act, Security Standards for the Protection of Electronic Protected Health Information, 45 CFR Parts 160, 162, and 164

**LifePoint:**

Information Security – Program Requirements – LPNT.IS.SEC.001

HIPAA Complaint Process & Disciplinary Actions – HIPAA.GEN.003

Protected Health Information Incident Response – HIPAA.GEN.007

Patient Right to Access – HIPAA.PRI.006
HCA:

Information Security – Program Requirements, IS.SEC.001
Information Security - Confidentiality and Security Agreements Policy, IS.SEC.005

Attachments: Confidentiality and Security Agreement
SYSTEM HUMAN RESOURCE POLICY: CONFIDENTIALITY & PROPRIETARY INFORMATION

EFFECTIVE DATE: 11/1/75

REVISION DATE: 4/1/93; 3/1/96; 1/30/97; 9/5/00; 1/12/04; 2/1/04; 2/10/14

SCOPE:

This policy applies to Marquette General Hospital and its affiliates with employees who provide services in the Hospital’s primary and secondary service area (the “Company”). References to Facility or Facilities throughout the policy are meant to include the Hospital and/or its affiliates with employees providing services in Marquette General Hospital’s primary and secondary service area.

PURPOSE:

To establish a policy that protects the Company from the unauthorized dissemination of proprietary and confidential information

POLICY:

A. All employees will be required to sign a Confidentiality Statement at the time of hire as part of their new hire paperwork process.

B. From time to time employees may have access to confidential information involving Company operations such as patient information, business data, and news stories prior to their release date. Unauthorized disclosure of confidential information is detrimental to the Company and no time should an employee knowingly discuss such information. Confidential information must be kept confidential. Failure to maintain confidential information may result in an employee’s discipline, up to and including termination.

C. While employed with the Company, employees may have access to and become acquainted with information of a proprietary or secret nature. This information is or may be applicable or related to the Company’s present and future business, research or development. Trade secret information includes, but is not limited to, devices, secret inventions, processes, compilations of information, records, specifications, and information concerning vendors or patients. Employees shall not disclose any Company trade secrets directly or indirectly, use them in any way, either during the term of their employment or any time thereafter, except as required in the course of Company employment.

D. All information concerning a present or former patient’s care, treatment, diagnosis, prognosis and personal affairs is strictly confidential and is to be discussed or disclosed only by authorized personnel on a need-to-know basis. “Patient” also includes Company employees when they are patients at the hospital.

Whether information concerning the patient is obtained during the course of one’s regular duties or accidentally overheard while performing work, employees must refrain from discussing such information with unauthorized persons, in or out of the hospital, in order to ensure the patient’s right to privacy.

External Regulating Authority: HR Gov
Policy Owner: Human Resources
Policy Number: 200-041, HR 004

All references to Marquette General Hospital, the “Facility” or the “Company” used in this policy refer to one or all of Marquette General Hospital and/or its affiliates with employees who provide services to Marquette General Hospital’s primary and secondary service area.
Violation of employee/patient confidentiality is grounds for discipline, up to and including termination.

Nothing in this policy is intended to restrict whatever rights you may have under Federal, State or local laws.

REFERENCES:
HIPAA Program Policy
Code of Conduct
LPNT.IS.SEC.005 - Confidentiality and Security Agreements Policy

FORMS
IS Confidentiality and Security Agreement Form
HIPAA Program Acknowledgement Form
Code of Conduct Acknowledgement Form

External Regulating Authority: HR Gov
Policy Owner: Human Resources
Policy Number: 200-041, HR 004

All references to Marquette General Hospital, the "Facility" or the "Company" used in this policy refer to one or all of Marquette General Hospital and/or its affiliates with employees who provide services to Marquette General Hospital's primary and secondary service area.
MARQUETTE GENERAL HEALTH SYSTEM

SYSTEM HUMAN RESOURCE POLICY: HARASSMENT

EFFECTIVE DATE: 8/1/99

REVISION DATE: 4/1/02; 7/1/06; 2/1/09; 1/1/10; 2/10/14

SCOPE:

This policy applies to Marquette General Hospital and its affiliates with employees who provide services in the Hospital’s primary and secondary service area (the “Company”). References to Facility or Facilities throughout the policy are meant to include the Hospital and/or its affiliates with employees providing services in Marquette General Hospital’s primary and secondary service area.

PURPOSE:

To establish a policy to ensure that all Company employees are aware of the Company’s position and its intent to comply with federal, state, and local laws regarding harassment on any protected basis (i.e., color, race, gender, age, religion, national origin, disability, genetic information, gender identity, sexual orientation, veteran’s status, etc.)

HARASSMENT POLICY AND PROCEDURE:

I. Harassment

In accordance with applicable law, the Company prohibits sexual harassment and harassment because of color, race, gender, age, religion, national origin, disability, genetic information, gender identity, sexual orientation, veteran’s status or any other basis protected by applicable federal, state or local law. All such harassment is prohibited and will not be tolerated.

II. Sexual Harassment

A. It is unlawful to harass a person (an applicant or employee) because of that person’s sex. Harassment can include “sexual harassment” or unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment of a sexual nature.
B. Harassment does not have to be of a sexual nature, however, and can include offensive remarks about a person’s sex.
C. Both victim and the harasser can be either a woman or a man, and the victim and harasser can be the same sex.
D. Although the law doesn’t prohibit simple teasing, offhand comments, or isolated incidents that are not very serious, harassment is illegal when it is so frequent or severe that it creates a hostile or offensive work environment or when it results in an adverse employment decision (such as the victim being fired or demoted).
E. The harasser can be the victim’s supervisor, a supervisor in another area, a co-worker, or someone who is not an employee of the employer, such as a vendor, patient or other visitor.

External Regulating Authority: EEOC
Policy Owner: Human Resources
Policy Number: 200-066, HR.008

All references to Marquette General Hospital, the “Facility” or the “Company” used in this policy refer to one or all of Marquette General Hospital and/or its affiliates with employees who provide services in Marquette General Hospital’s primary and secondary service area.
F. Applicable state and federal law defines sexual harassment as unwanted sexual advances, request for sexual favors, or visual, verbal, or physical contact of a sexual nature when:
   • Submission to the conduct is made a term or condition of employment; or
   • Submission to or rejection of the conduct is used as basis for employment decisions affecting the individual; or
   • The conduct has the purpose or effect of unreasonably interfering with the employee’s work performance or creating an intimidating, hostile or offensive work environment.

G. Sexual Harassment includes many forms of offensive behavior. The following is a partial list of prohibited behaviors:
   • Unwanted sexual advances;
   • Offering employment benefits in exchange for sexual favors;
   • Visual conduct such as leering, making sexual gestures, or displaying sexually suggestive objects, pictures, cartoons or posters;
   • Dissemination through e-mail or other electronic communication material that contains sexually suggestive content;
   • Verbal conduct such as making or using derogatory comments, epithets, slurs, sexually explicit jokes, or inappropriate comments about any employee’s body or dress;
   • Verbal sexual advances or propositions;
   • Verbal abuse of a sexual nature, graphic verbal commentary about an individual’s body, sexually degrading words to describe an individual, or suggestive or obscene letters, notes or invitations;
   • Physical conduct such as unwanted touching, assault or impeding or blocking movements; and
   • Retaliation for reporting harassment or threatening to report harassment.

H. It is unlawful for males to sexually harass females or other males, and for females to sexually harass males or other females. Sexual harassment on the job is prohibited, whether it involves coworker harassment, harassment by a subordinate or manager, or harassment by persons doing business with or for the Company.

III. Other Types of Harassment

A. Prohibited harassment on the basis of color, race, gender, age, religion, national origin, disability, genetic information, gender identity, sexual orientation, veteran’s status or any other basis protected by applicable federal, state or local law, includes behavior similar to sexual harassment, such as:
   • Verbal conduct such as threats, epithets, derogatory comments or slurs;
   • Visual conduct such as derogatory posters, photographs, cartoons, drawings or gestures;
   • Dissemination of offensive/inappropriate e-mail or other electronic communication;
   • Physical conduct such as assault, unwanted touching, or blocking normal movements; and
   • Retaliation for reporting harassment or threatening to report harassment.

External Regulating Authority: EEOC
Policy Owner: Human Resources
Policy Number: 200-006, HR.008

All references to Marquette General Hospital, the “Facility” or the “Company” used in this policy refer to one or all of Marquette General Hospital and/or its affiliates with employees who provide services in Marquette General Hospital’s primary and secondary service area.
IV. Complaint Procedure

A. All employees are responsible for helping to avoid unlawful harassment. If employees feel that they or another applicant or employee have been harassed in violation of this policy, they should report their concerns to their supervisor, a member of Senior Management or to Human Resources and/or file a formal complaint in accordance with the Complaint Filing and Investigative Procedures policy. The employee may also voice complaint by calling the Hospital Support Center Ethics Line at 1-877-508-5433. Any Supervisor who becomes aware of conduct in violation of this policy shall report such conduct to Human Resources immediately.

B. The Company will not allow retaliation against anyone who expresses a concern about harassment or who participates in an investigation.

V. Discipline/Liability for Harassment

A. Any employee of the Company, whether a co-worker or manager, who is found to have engaged in prohibited harassment or retaliation is subject to disciplinary action, up to and including discharge from employment.

B. Any employee, who engages in prohibited harassment, including any manager who knew about the harassment but took no action to stop it, may be held personally liable by the court or other agency for monetary damages.

C. The Company does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one’s duties. Accordingly, to the extent permitted by law, the Company reserves the right not to provide a defense or pay damages assessed against employees for conduct in violation of the policy.

Nothing in this policy is intended to restrict whatever rights you may have under federal, State or local laws.

REFERENCES:
Equal Employment Opportunity Commission
HR.002 - Bulletin Boards and Posting of Employee Rights
HR.003 - Complaint Filing and Investigative Procedures
HR.006 – Equal Employment Opportunity
Code of Conduct

External Regulating Authority: EEOC
Policy Owner: Human Resources
Policy Number: 200-006, HR.008

All references to Marquette General Hospital, the "Facility" or the "Company" used in this policy refer to one or all of Marquette General Hospital and/or its affiliates with employees who provide services in Marquette General Hospital’s primary and secondary service area.
Compliance Plan for Claim Reimbursement, 100-024

Mission Statement

Marquette General Health System (MGH) is committed to conducting its affairs in accordance with applicable laws. To this end, MGH strives to assure that all patient care claims are submitted so that claims are not only in compliance with applicable law, but also with the applicable requirements of third party payment programs. While compliance in this area can be difficult due to the complex nature of the applicable requirements and the fact that such requirements are often subject to differing interpretations, MGH strives to assure that it is accurate in claim submission. To further MGH’s goal of ensuring that patient care and submitted claims are appropriate, MGH has adopted this plan for complying with applicable legal, regulatory and third party payment requirements.

The compliance program set forth herein is not an exhaustive recitation of all compliance programs and activities of MGH that are currently in effect. MGH will continue to maintain various compliance practices in addition to those set forth in this plan as part of its overall legal compliance efforts.

Compliance Officer

The Chief Executive Officer will recommend to the Board who should be designated to serve as the Compliance Officer for this Plan. As such, the Compliance Officer will oversee the implementation and operation of the Plan, and will implement modifications to the Plan as appropriate. The Compliance Officer is authorized to engage legal counsel, where appropriate, to assist in the implementation, operation and modification of this Plan, including serving as a resource for responding to issues arising through the compliance activities of MGH as related to the Plan.

In furtherance of the responsibilities of the Compliance Officer, the Compliance Officer will, with the assistance of the Compliance Committee, oversee the following matters:

1. The formulation, review and revision, as appropriate, of policies concerning the submission of claims by the System and its employees;

2. The formulation, review and revision, as appropriate, of training and educational materials and programs designed for all System personnel related to their scope of duties and responsibilities.

3. Establishment of internal and external billing reviews;
4. Establish a mechanism whereby inquiries concerning billing questions or issues are answered in a
decisive manner. In this regard, because of the need to assure uniformity of appropriate practices by the
System and its personnel, the Compliance Officer shall serve as the final System authority on specific
billing practices, such as the use of particular codes for designated services, the procedures and
processes for billing, and determining whether a compliance issue exists;

5. Establish reporting and other mechanisms to enable reports of non-compliance (in addition to those
identified through other means, such as internal or outside audits) and formulate an appropriate response
when such issues arise; and

6. Preparation of an annual report in cooperation with the Business Office and the Manager of Revenue
Integrity that shall be delivered to the Chief Executive Officer and the Board of Trustees of the System
summarizing the compliance efforts of MGH during the past year and identifying any changes
recommended.

7. Under the oversight of the Compliance Officer, MGH shall establish policies and guidelines, as necessary,
designed to achieve the goal that all claims for reimbursement shall be billed under the proper code for
the services provided, that the Medical Record and the care provided relative to the record support the
documentation required for such claim, and that the claim is submitted to the appropriate payer or payers.
To this end, the Compliance Officer shall review existing policy statements, make or cause to be made
such revisions to those statements as necessary, develop any additional statements that seem advisable
and assure that such statements are disseminated among all MGH personnel whose job function includes
matters covered within such statements.

Compliance Responsibilities of Employees

Under the oversight of the Compliance Officer, all claims for reimbursement relative to patient care shall be
billed under the proper code for the services provided, that the supporting documentation required with respect
to each such claim is in place and that the claim is submitted to the appropriate payer or payers. Electronic
programs used for billing will be in compliance with applicable laws and third party payment programs. If
outside contractors are retained, steps should be taken to ensure their compliance with applicable regulations
as it pertains to MGH hospital business. To this end, the Compliance Officer shall review existing policy
statements, make or cause to be made such revisions to those statements as necessary, develop any
additional statements that seem advisable and assure that such statements are disseminated among all MGH
personnel whose job function includes matters covered within such statements. Violations of this policy or with
compliance to applicable Federal/State laws are serious matters and employees will be disciplined
accordingly.

Education and Training

The Compliance Officer shall, in conjunction with the Human Resources Department, assure that relative to
this policy, personnel receive systematic and ongoing training, both upon hire and on a continuing basis that
enables such personnel to properly perform their job functions. As one facet of continuing training, the
Compliance Officer shall assure that appropriate personnel attend outside seminars as necessary to update
information. Not all personnel are required to attend outside seminars, but the Compliance Officer shall
undertake measures to assure information learned at such seminars is disseminated to appropriate System
personnel. Records demonstrating that such training has occurred shall be in personnel files or departmental
files.

In addition to training for billing personnel, physicians and all other System employees who provide the care
and documentation which is relied upon for billing purposes shall receive annual training concerning
compliance issues related to their services. All employees will receive inservice training regarding recognition and reporting of non-compliance issues during orientation and annually. The Department Head shall retain records indicating that such training has occurred shall be maintained.

The Compliance Officer will establish a method whereby responsibility for monitoring reimbursement rules changes is delegated to one or more individuals who shall be responsible for disseminating that information among appropriate personnel pursuant to policies and protocols established under the direction of the Compliance Officer.

Internal and External Audits

Under the direction of legal counsel, who shall oversee and coordinate such activities with the Compliance Officer, a representative sample of medical records and corresponding claims submissions for medical education billing issues shall be reviewed each quarter by internal reviewers qualified to assess the appropriateness of the documentation and claims submitted. In addition, on an annual basis, or more frequently as the Compliance Officer shall determine necessary, the System shall engage a qualified external consultant to evaluate a representative sample of medical records and corresponding claims submissions to evaluate the appropriateness of documentation and claims submitted. Such external review can, but need not be, accomplished in connection with the annual audit of the System.

With respect to both internal and external audits, written reports summarizing the results of such audits shall be provided to legal counsel at LifePoint, Manager of Revenue Integrity, the Compliance Officer and the Chief Financial Officer. The Compliance Officer shall, in consultation with legal counsel and the Chief Financial Officer, review the results of the audit to determine whether any action is warranted based on the audit findings.

Reporting and Investigation of Compliance Issues

Employees and physicians will report activity they believe to be inconsistent with Hospital policies or legal requirements to the Compliance Officer. Matters of potential non-compliance may be reported through any of the following mechanisms:

1. Report incident to immediate supervisor
2. 24-hour hotline, 1-877-508-LIFE (5433).
3. Interdepartmental memo or email to the Compliance Officer

All reports of potential non-compliance will be handled in a confidential and sensitive manner. Such reports can be reported anonymously, but if not, the employee is not to be subject to retaliation/ harassment. Employees/physicians engaging in non-compliant activity may be subject to disciplinary action including termination.

Employees and physicians, who have concerns about safety or quality of care, may choose to report these concerns to an appropriate regulatory agency. As with all compliance reporting, reports of safety or quality care concerns to an appropriate regulatory agency will not result in any retaliatory or disciplinary action.

Compliance Corrective Action Plan

Whenever the Compliance Officer identifies an issue as to which corrective action is indicated, the Compliance Officer shall develop a formal plan to address the issue. Such a plan can include, without limitation, additional education and/or training, seeking clarification from appropriate personnel and/or obtaining the advice of legal counsel and/or other outside consultants.
The purpose of all corrective action plans will be to address the issue appropriately in order to bring the System into legal compliance and to consider actions which may facilitate future compliance. The Compliance Officer shall be responsible for determining whether certain individuals or groups of individuals are responsible for particular problems and to consider actions, such as monitoring of such personnel, in order to implement the policies set forth in the Compliance Plan.

<table>
<thead>
<tr>
<th>Attachments:</th>
<th>No Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee</td>
<td>Approver</td>
</tr>
<tr>
<td></td>
<td>Stephen Embree: Chief Financial Officer</td>
</tr>
<tr>
<td></td>
<td>Kathleen Grisham: Sr Administrative Assistant</td>
</tr>
</tbody>
</table>
Workplace Violence Prevention Plan, 100-213

Purpose

To outline the key components of a Workplace Violence Prevention Plan, including the process to identify, prevent and handle threats in the workplace. To create an awareness of actions that can reduce the likelihood of threats that escalate into violent behavior.

Policy

It is policy of Marquette General Hospital (MGH) to promote a safe and non-violent environment for employees, patients, and visitors. The organization is committed to working with employees to maintain a work environment free from acts or threats of violence. MGH has "Zero Tolerance" towards all expressions of violence, including both physical and non-physical threats.

Violent behavior shall not be tolerated. Individuals who commit such acts may be removed from the premises and may be subject to criminal penalties. Employees may also be subject to disciplinary action up to and including termination.

Weapon is an item or material capable of inflicting harm. Weapons may include, but are not limited to, knives, stabbing instruments, electronic incapacitating devices, firearms, or chemical incapacitating devices.

Weapons are not permitted on health system property. However, sworn law enforcement and corrections officers may bear weapons as required by their job duties. Exception is delineated in APU Policies.

Each MGH employee has the responsibility of maintaining a nonviolent work environment by refraining from engaging in any violent behavior and reporting any occurrence that would be considered inappropriate under this policy.

For situations placing individuals in immediate danger, e.g., a person brandishing a gun, the employee will call law enforcement at 911 (9-911 on the main campus, or "5" for the Switchboard), or the emergency number in the local community, at that time.

Definition

Workplace Violence – violence which an individual inflicts, or threatens to inflict, on others at the place of work and may include:

- Damage to property
Serious harm
Injury
Death

Violence – includes physically harming another, shoving, pushing, brandishing weapons, and threatening or talking of engaging in these activities. It is behavior used to frighten, injure, damage, or destroy another person or property. This may include a direct or indirect threat of harm. It is usually an expression of anger, and can take the following forms:

• Gestures/verbal abuse
• Physical force
• Rough action
• Stalking
• Some acts of theft
• Vandalism

Threat – A direct or implied expression of intent to inflict physical harm and/or actions that a reasonable person would perceive as a threat to physical safety or property. The following are some examples of behaviors that may be considered threats. (Additionally, because intent may not always be discerned by co-workers, jokes about physical acts of violence will not be tolerated.)

• Verbal threats which include descriptions of what the violent person plans to do.
• Threatening conduct, ranging from threatening gestures to showing or actually brandishing a weapon, or what appears to be a weapon.
• Bizarre statements or actions threatening physical harm including retaliation.
• Written threats.

Zero-tolerance – The standard that states no behavior, implied or actual, that violates this policy, will be tolerated.

Procedure

Workplace Violence Prevention through Education – At the time of hire, all new employees will receive a copy of the Workplace Violence Prevention Plan and sign a statement that they have received and reviewed it. The statement will be kept in the employment file. In addition, information regarding workplace violence is provided to all employees with the annual mandatory safety education.

Response

Immediate Response to Threats/Assault

• During normal business hours, physician offices and off-site facilities will contact the Police at 911, or the emergency number in their specific community, for Immediate threats or acts of violence.
• Employees who believe they are subject to, or aware of threats (implied or direct), or physical/verbal abuse from employees, patients, visitors, or others, need to report these specific circumstances to their Manager/Supervisor and/or Hospital Supervisor who will contact Director of Safety and Risk Management. Management personnel will seek the assistance of the MGH Security Police, and/or outside law enforcement agencies as necessary.
• Employees who believe they may be at risk for violence at work as a result of a domestic dispute are encouraged to report the situation to their manager/supervisor, who will involve the Director of Safety and Risk Management. Copies of any restraining/personal protection orders shall be provided to Risk Management, Human Resources, and/or the Hospital Supervisor, as necessary, including a description or
photograph of the individual, if available. Management personnel will notify the MGH Security Police of potentially violent situations as necessary.

- Workplace violence and/or threats will be recorded on an Unusual Occurrence Report in accordance with policy.
- In non-emergent situations, the employee will call the Director of Safety and Risk Management or the Administrator on-call, if Risk Manager is not available, for assistance. The employee should report all threats that are direct or imminent in nature immediately to MGH Security Police. The Hospital Supervisor or Director of Safety and Risk Management or designee will determine if outside law enforcement needs to be contacted. The Hospital Supervisor will also notify the Administrator on-call and Risk Management.

Follow-Up Action – Risk Management will investigate the incident in conjunction with others as appropriate, e.g. MGH Security Police, Director of Employment, Department Manager, Hospital Supervisor, Law Enforcement, etc.

Confidentiality – In the interest of safety, any person reporting a violent threat (or other behavior listed previously) may ask that their name be withheld. When an investigation follows, the individuals involved, including witnesses or others familiar with the situation will need to answer questions. The investigation will be completed in a confidential manner. In the event that investigation or issue involves law enforcement, legal action, or union grievance, the name of the individual reporting the event may need to be released.

Management of Violent Conduct

Employee – All employees are expected to behave in accordance with Human Resource Policies. Any employee engaging in violent behavior as defined in this plan may be subject to disciplinary action, up to and including termination. Physician code of conduct concerns will be addressed per Medical Staff Bylaws. A Medical Staff Conduct Incident Report may be completed for events involving physicians.

Patient – Physical/mental, mental/emotional illness and situational stress/crisis may all be reasons for violent behavior. Direction for care or treatment of patients behaving in a threatening or violent manner will be per the healthcare provider or physician in charge. Exception: If a patient’s behavior poses an imminent danger to the safety of employees, other patients, or visitors, and cannot be managed through existing hospital or departmental policies and procedures, direction towards resolution of the incident will be per Risk Management, MGH Security Police or other law enforcement, if involved. Discharge from care or service following continued violence will be determined by the attending physician and the Chief Nursing Officer.

Visitor – Physical, mental/emotional illness and situational stress/crisis may all be reasons that precipitate violent behavior. However, if a visitor displays violent behavior, staff will explain to the visitor that any behavior which is threatening or violent in nature is not acceptable. If the behavior continues, staff will notify the MGH Security Police who will assist the involved person(s) off of the premises. Law enforcement may be involved at the discretion of Risk Management, the Hospital Supervisor or the MGH Security Police.

Employee Post-Assault Management

Management personnel should:

- Assist the individual, if injured, to receive medical services.
- Assure that the employee’s manager/supervisor, Risk Manager, and Employee Health Services have been notified, if the injured person is an employee.
- Assist the employee to document the incident on an Unusual Occurrence Report form. Documentation should describe the event, factors surrounding the event including where it occurred, type/condition of patient or visitor if applicable, injuries sustained and if medical treatment was obtained. Injuries will be
recorded in the medical record or the Unusual Occurrence Report. If the employee is unable to provide this documentation, a co-worker and/or manager will do so.

- MGH Security Police, Risk Management, the Hospital Supervisor, or the off-site manager will notify law enforcement.
- The employee’s manager will encourage employees who are involved in, or witness, a violent act to use the Employee Assistance Program as may be needed.

Guideline for Responding to Telephone and Written Threats

Telephone Threats – The employee receiving the call should:

- Notify his/her manager/supervisor immediately
- Note the time, date, and telephone number at which the threat was received
- The manager/supervisor should contact Risk Management immediately, who may involve Telecommunications to secure information about the call.

Written Threats – The employee receiving the written threat should:

- Notify his/her manager/supervisor immediately;
- Handle the written material and any envelopes as little as possible, and then only by the corners;
- Place both the written material and any envelope in a large envelope;
- Note the names of anyone who handled the material after its arrival;
- Turn the material over to Risk Management, the Hospital Supervisor or the MGH Security Police.

If the telephone or written threat involves an imminent act of violence, the employee should report immediately to the MGH Security Police, Risk Management, or the Hospital Supervisor.

If the threat is not imminent, the employee should report the threat to his/her immediate supervisor or manager. The manager/supervisor will then consult with Risk Management, MGH Security Police or the Hospital Supervisor regarding the course of action.

The employee shall complete an Unusual Occurrence Report.

Annual Assessment

The Director of Safety and Risk Management will evaluate the Workplace Violence Prevention Plan as part of the Security Management Plan biannual review, which is reported to the Safety Committee and the Board of Trustees. Evaluation of effectiveness includes data trends/summaries of reported incidents of assaults or other acts of violence, employee/visitor/patient reported complaints or concerns, and where applicable, results from high-risk area surveys. Ongoing additions or changes to the program may occur as a result of different types of services provided by a component of the organization, geographic relocation of services, community changes, such as increased violence or gang activity or other new information available to the Office of Safety and Risk Management and the Environment of Care Committee.

<table>
<thead>
<tr>
<th>Attachments:</th>
<th>No Attachments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee</td>
<td>Approver</td>
</tr>
<tr>
<td></td>
<td>Stephen Embree: Chief Financial Officer</td>
</tr>
<tr>
<td></td>
<td>Kathleen Grisham: Sr Administrative Assistant</td>
</tr>
</tbody>
</table>
EMPLOYEE RIGHTS AND RESPONSIBILITIES
UNDER THE FAMILY AND MEDICAL LEAVE ACT

Basic Leave Entitlement
FMLA requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to eligible employees for the following reasons:

- for incapacity due to pregnancy, prenatal medical care or child birth,
- to care for the employee's child after birth, or placement for adoption or foster care,
- to care for the employee's spouse, son, daughter or parent, who has a serious health condition,
- for a serious health condition that makes the employee unable to perform the employee's job.

Military Family Leave Entitlements
Eligible employees whose spouse, son, daughter or parent is on covered active duty, or call to covered active duty status may use their 12-week leave entitlement to address certain qualifying exigencies. Qualifying exigencies may include attending certain military events, arranging for alternative childcare, addressing certain financial and legal arrangements, attending certain counseling sessions, and attending post-deployment reintegration briefings.

FMLA also includes a special leave entitlement that permits eligible employees to take up to 26 weeks of leave to care for a covered service-member during a single 12-month period. A covered service-member is:
- a current member of the Armed Forces, including a member of the National Guard or Reserves, who is undergoing medical treatment, recuperation or therapy, and is otherwise in outpatient status, or is otherwise on the temporary disability retired list, in a serious injury or illness;
- or a veteran who was discharged or released under conditions other than dishonorable at any time during the five-year period prior to the date the eligible employee takes FMLA leave to care for the covered veteran and who is undergoing medical treatment, recuperation, or therapy for a serious injury or illness.

*The FMLA definitions of "serious injury or illness" for current servicemembers and veterans are distinct from the FMLA definition of "serious health condition".

Benefits and Protections
During FMLA leave, the employer must maintain the employee's health coverage under any "group health plan" on the same terms as if the employee had continued to work. Upon return from FMLA leave, most employees must be restored to their original or equivalent positions with equivalent pay, benefits, and other employment terms.

Use of FMLA leave cannot result in the loss of any employment benefit that accrued prior to the start of an employee’s leave.

Eligibility Requirements
Employees are eligible if they have worked for a covered employer for at least 12 months, have 1,250 hours of service in the previous 12 months, and if at least 50 employees are employed by the employer within 75 miles.

*Special hours of service eligibility requirements apply to airline flight crew employees.

Definition of Serious Health Condition
A serious health condition is an illness, injury, impairment, or physical or mental condition that involves either an overnight stay in a medical care facility, or continuing treatment by a health care provider for a condition that either prevents the employee from performing the functions of the employee's job, or prevents the qualified family member from participating in school or other daily activities.

Subject to certain conditions, the continuing treatment requirement may be met by a period of incapacity of more than 3 consecutive calendar days combined with at least two visits to a health care provider or one visit and a regimen of continuing treatment, or incapacity due to pregnancy, or incapacity due to a chronic condition. Other conditions may meet the definition of continuing treatment.

Use of Leave
An employee does not need to use this leave entitlement in one block. Leave can be taken intermittently or on a reduced leave schedule when medically necessary. Employees must make reasonable efforts to schedule leave for planned medical treatment so as not to unduly disrupt the employer’s operations. Leave due to qualifying exigencies may also be taken on an intermittent basis.

Substitution of Paid Leave for Unpaid Leave
Employees may choose or employers may require use of accrued paid leave while taking FMLA leave. In order to use paid leave for FMLA leave, employees must comply with the employer’s normal paid leave policies.

Employer Responsibilities
Employees must provide 30 days advance notice of the need to take FMLA leave when the need is foreseeable. When 30 days notice is not possible, the employee must provide notice as soon as practicable and generally must comply with an employer’s normal call-in procedures.

Employees must provide sufficient information for the employer to determine if the leave may qualify for FMLA protection and the anticipated timing and duration of the leave. Sufficient information may include that the employee is unable to perform job functions, the family member is unable to perform daily activities, the need for hospitalization or continuing treatment by a health care provider, or circumstances supporting the need for military family leave. Employees also must inform the employer if the requested leave is for a reason for which FMLA leave was previously taken or certified. Employees may be required to provide a certification and periodic recertification supporting the need for leave.

Employer Responsibilities
Covered employers must inform employees requesting leave whether they are eligible under FMLA. If they are, the notice must specify any additional information required as well as the employees' rights and responsibilities. If they are not eligible, the employer must provide a reason for the ineligibility.

Covered employers must inform employees if leave will be designated as FMLA-protected and the amount of leave counted against the employee’s leave entitlement if the employer determines that the leave is not FMLA-protected, the employer must notify the employee.

Unlawful Acts by Employers
FMLA makes it unlawful for any employer to:

- interfere with, restrain, or deny the exercise of any right provided under FMLA, and
- discharge or discriminate against any person for opposing any practice made unlawful by FMLA or for involvement in any proceeding under or relating to FMLA.

Enforcement
An employee may file a complaint with the U.S. Department of Labor or may bring a private lawsuit against an employer.

FMLA does not affect any Federal or State law prohibiting discrimination, or supersede any State or local law or collective bargaining agreement which provides greater family or medical leave rights.

FMLA section 109 (29 U.S.C. § 2619) requires FMLA covered employers to post the text of this notice. Regulation 29 C.F.R. § 825.300(a) may require additional disclosures.

For additional Information:
1-866-4-US-WAGE (1-866-487-9243) TTY 1-877-889-5627
WWW.WAGEHOUR.DOL.GOV

I-9 Form: U.S. Department of Labor | Wage and Hour Division
**Use Of Tobacco Products, 100-025**

U P Health System – Marquette Health System (MGHS) is committed to promotion of health, which includes prevention as well as treatment of illness. Second hand smoke and tobacco related illnesses compromise the largest proportion of preventable diseases. The increased danger of fire associated with smoking presents additional hazard to our facility, workers and visitors. For these reasons, MGHS prohibits smoking and tobacco use inside and outside all facilities owned and leased, on adjacent grounds and sidewalks, parking lots, ramps and in MGHS owned vehicles and personal vehicles, at all main campus, home health, and clinic locations, and facilities within 100 feet from any building and/or property. Additionally, this policy is in compliance with Michigan Law PA 135 of 1988, which bans smoking in hospitals, and Marquette City Ordinance #469 which prohibits smoking in all workplaces, except in bars, restaurants, and casinos.

All employees, patients, visitors, physicians, contractors and subcontractors, faculty, students, and all others at or on MGHS facilities, grounds, parking lots, ramps, and in MGHS owned vehicles on Main Campus, Home Health, and Clinic locations are covered by this policy.

Tobacco products covered by this policy are cigarettes, pipes, cigars, and chewing tobacco, and are not solely limited to these items.

All MGHS employees who smoke and desire to quit are encouraged to request a free Michigan Smokers "Quit Kits" from EHW. Additionally employees are urged to utilize the Employee Assistance Programs in Marquette and Escanaba.

**ENFORCEMENT of POLICY**

Enforcement is the responsibility of all employees of MGHS.

- All new employees will be informed of the policy at interview, hire, and orientation.
- Employees observing a co-worker violating the policy are requested to courteously remind the offender of the policy and suggest desisting from the use of nicotine.
- Employees are expected to inform any manager or supervisor if they witness another employee violating this policy. The manager receiving the report will then inform the offending employee's direct supervisor.
- All information regarding the source of the information will be confidential.
- Infractions of this policy are subject to corrective action, up to and including termination.

**Attachments:**

No Attachments
<table>
<thead>
<tr>
<th>Committee</th>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitchell Leckelt: Assistant Administrator</td>
<td>01/2014</td>
<td></td>
</tr>
<tr>
<td>Kathleen Grisham: Sr Administrative Assistant</td>
<td>01/2014</td>
<td></td>
</tr>
</tbody>
</table>
MARQUETTE GENERAL HEALTH SYSTEM
MARQUETTE, MICHIGAN
SYSTEM HUMAN RESOURCES POLICY

Subject: Identification Badges
Policy No. 200-015
Effective Date: 9-1-75
Revision Date: 5-14-84; 2-24-92;
6-1-94; 2-24-03.

Distribution: All Departments

Human Resources will provide each new employee with a photo identification badge which includes name, job title as designated by job class code, and bar code as appropriate. Employees who work in nursing units will also be issued a non-photo name badge identifying their first name and job title. Identification badges are considered property of Marquette General Health System and must be returned to Human Resources when an employee terminates or replaces a badge. Defacement or abuse of identification badges is a violation of System policy and may result in corrective action. It is mandatory that employees wear identification badges while working with photo side facing out. (See Policy #200-097 for cafetera discount.)

Identification badges will be provided by the System at no charge for employees who receive a promotion, change their name, or are newly hired or if the identification badge is broken or worn. Employees who request identification badges for any other reason will be charged a $6.00 replacement fee prior to receiving the new badge. Arrangements need to be made by the employee with Human Resources to set up a time for a new badge to be issued.

This charge will be used to offset the cost involved in making the badge. Fees collected by the Human Resources Office will be turned into the Accounting Department on a monthly basis.

The non-picture side of the identification badge is bar-coded and used exclusively by the employee to access the time and attendance terminals. Employees are not to leave name badges in areas where access can be gained by other persons.

Identification badges contain four different color-coded borders identified as the following: White=employee; Blue=physician; Green=temporary employee; Gold=employee of the month.

All requests for identification badges must be processed through Human Resources.

END OF POLICY