SUB-SECTION: HIPAA
INCLUDES:

POLICY

It is the policy of MercyOne Northeast Iowa ("MercyOne") to have reasonable administrative, physical and technical safeguards in place necessary to maintain the confidentiality, privacy and security of any and all Protected Health Information (PHI), including electronic (ePHI), (collectively referred to as PHI, unless otherwise noted), in accordance with applicable state and federal law, specifically the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The health plan maintained by MercyOne, as HIPAA applies, shall comply with HIPAA's privacy and security requirements in accordance with applicable law. When necessary, the plan document shall be amended to include required provisions.

RATIONALE

Our Value of Respect calls us to ensure that we respect a person's right to privacy of their health information. Our Value of Integrity requires us to understand and comply with the applicable state and federal laws. Furthermore, our Value of Stewardship calls us to respect the resources entrusted to MercyOne by complying with policies intended to safeguard PHI.

SCOPE

This policy MercyOne Northeast Iowa.

This policy applies to all members of MercyOne's workforce including, officers, directors, medical staff members, colleagues and independent contractors, volunteers, students, and any others having access to individually identifiable health information either through written, verbal or electronic means.

PROCEDURE

I. SOCIAL SECURITY NUMBERS (SSN)

A. MercyOne will take reasonable steps to protect patients from identity theft consistent with our Identity Theft Prevention Program.

B. Patient social security numbers are Protected Health Information.

C. MercyOne will apply a minimum necessary standard to the use and disclosure of SSN. Starting in November 2015 and rolling out over a reasonable period of time, unless required by a law or regulation, MercyOne will only display or print the last 4 digits of a patient's SSN unless prior approval is given by the Information Security Committee (or its delegate) after obtaining documentation outlining the reasonable need for the full social security number. MercyOne will make its uses of a patient's full social security number available upon request.

II. WHITEBOARDS AND MONITORS WITH PATIENT INFORMATION

A. MercyOne uses whiteboard, whether manual or electronic, and monitors to track essential patient information. MercyOne will make reasonable attempts to safeguard information contained on whiteboards and monitors by locating them in areas not readily accessible to the public and limiting the information contained on the whiteboard and/or monitor to the minimum necessary to provide safe care to the patient.

B. Once it is no longer necessary to maintain a patient's information on the whiteboard and/or monitor, the patient's information will be removed from the whiteboard and/or monitor.

III. OVERHEAD PAGING SYSTEMS

A. MercyOne may use overhead paging systems as a means of communication within its facilities.

B. MercyOne will use overhead paging that contains patient information only to the extent that another means of communication is not available, and an emergency circumstance exists. MercyOne will limit the patient information contained in the page to the minimum amount necessary to alert the paged parties. Person being paged should be directed to call the operator instead of any specific patient unit.

C. Examples of pages that could be used are:

'The family of the patient in room ___, please contact the operator.'
'The XXX family, please contact the operator.'

IV. MESSAGES FOR PATIENTS AND REMINDER CARDS

A. MercyOne may leave messages for patient on their answering machines or with household members who answer the patient's phone. However, to reasonably safeguard the patient's privacy, MercyOne will limit the information left without a patient's authorization to do otherwise. Information left as a message should be limited to the name of the organization, our phone number and other minimal information necessary to confirm an appointment. If more information is needed, the MercyOne colleague will ask for a return phone call from the patient.

B. MercyOne may send appointment reminder or lab results cards if the card is either in an envelope or where the card is folded and secured to protect any PHI.

V. FACILITIES

A. MercyOne will take reasonable steps to ensure patient privacy in the design of its facilities. Examples of the types of adjustments or modifications to facilities or systems that MercyOne may make as a reasonable safeguard are:

- Areas in which patients are asked protected health information should include signage asking other individuals to stand a few feet back from a counter.
- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers to safeguard information.

The Office of Civil Rights has indicated that HIPAA **does not** require the following types of structural or systems changes for patient privacy:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

VI. CONVERSATIONS IN PUBLIC SPACES/VISITORS

A. Colleagues should conduct conversations involving Protected Information in private settings. To the extent that a conversation that involves Protected Information must occur in a public space, colleagues must use lowered voices.

B. Patients have the right to agree or object to the sharing of information with their family and/or others involved in their care. Colleagues should ask the patient whether they object to sharing information in front of visitors prior to starting the conversation.

VII. SIGN IN SHEETS AND CALLING NAMES IN WAITING AREAS

A. MercyOne will limit the information used on all sign in sheets to the minimum necessary to identify the individual that was signed in. Sign in sheets will not contain medical information specific to the patient.

B. MercyOne will limit the patient information used to call a patient in a waiting room to the patient's first and last name.

VIII. SECURITY OF PHI IN PAPER FORM

A. MercyOne will ensure that it maintains appropriate safeguard to protect the confidentiality of PHI maintained in a paper form. MercyOne may use a combination of safeguards, which include, but are not limited to:

1. Housing the records in locked files,
2. Maintaining the record in areas that has reasonably limited access to the public,
3. Ensuring that the area in which the PHI is maintained is supervised,
4. Placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

B. MercyOne will use courier bags with a closure mechanism when paper records with PHI are transported. A mechanism must be in place to document when any record with PHI has left the facility.

C. Medical records stored in the facility or in off-site storage must be secured as well as protected to minimize damage from fire and water.

D. MercyOne will only display the last 4 digits of a SSN on paper forms or reports generated by MercyOne when SSNI information is necessary unless prior approval is received as outlined in Section I above.

IX. FAX MACHINES

A. Fax machines should be located in areas that are not accessible to the public.

B. A cover sheet with a confidentiality statement should be used. Patient specific information should not be included on the cover sheet. The cover sheet is acting as a safeguard against the wrong individual obtaining patient information.

C. Associates should ensure that the correct number is being used when faxing Protected Information, whether the number is entered manually or is preprogrammed.

D. If a fax is transmitted to the incorrect recipient, report this occurrence to the privacy officer to determine whether breach notification needs to occur.

E. If an associate receives a fax in error, please contact the sender to alert them to the error and destroy the facsimile.

X. E-MAIL

A. All email should be sent in a manner in compliance with the Electronic Communications policy. Any e-mails with patient specific information must be sent with Secure in the subject line. Patient specific information may not be in the subject line.

B. Prior to sending an email with Protected Information within it, associates will confirm that they are using a correct email address.

C. If an email is transmitted to the incorrect recipient, report this occurrence to the privacy officer to determine whether breach notification needs to occur.

D. If an associate receives an email in error, please contact the sender to alert them to the error and destroy the email.

XI. TEXT MESSAGING

A. Sharing patient information using an unsecure method of electronic communication may violate HIPAA and is open to legal discovery. Unsecure electronic communication includes unsecure texting. Unsecure text messages to patients are not allowed under this policy, unless
1. It relates to an appointment reminder and only includes information outlined under the reminder card/phone message section above, or
2. The patient has specifically requested a text message and has signed an authorization that includes the risk of sharing information through an unsecure text.

B. In some circumstances, texting may be needed to appropriately care for a patient. Please follow these guidelines when texting information to a provider related to patients.

1. **Preferred Method**

Send an e-mail with patient information to the provider's e-mail address using a secure WFH e-mail If needed, also send text or page asking caregiver to check their email for urgent communication.

- Example

Text message: Please read email 'Colonoscopy Urgent' to contact patient immediately.

- Tips
  - An e-mail to a physician's WFH e-mail account is considered a secure e-mail
  - If a non-WFH e-mail is to be used, you must type the word 'Secure' in the subject line. No patient information may be in the subject line. The physician should know that s/he will need to log in to a secure e-mail server to retrieve the message.

2. **Alternative Method**

While the method above is preferred, the following information may be texted or e-mailed if the preferred method cannot be used, another communication method is not available and patient care will be impacted.

- (Best Option) First name, last initial and home phone number. There should be no mention of the individual as a patient or their condition.
  - Example: Please call Clark K. at 999-999-9999
- First initial, last name and home phone number. There should be no mention of the individual as a patient or their condition.
  - Example: Please call C. Kent at 999-999-9999
- Limited use combinations: Use with caution
  - First name, last initial and medical condition
  - Medical Record Number (MRN) and medical condition
  - MRN and home phone number
  - MRN and first name with last initial
  - First Name, Last Initial, Phone Number and General Description of Issue
  - Examples:
    - "Please call Sheldon C. re swelling in his knee "
    - "Call patient at 999-999-9999 re this morning's procedure"

3. **Must not be used**

Sharing the following information using unsecure electronic communication poses a significant privacy risk. Do not share in a text or unsecure e-mail:

- Patient's first name, last name and medical condition

- Patient's phone number and medical condition
- Patient's first name, last name, phone number and medical condition
- Patient's MRN, first and last name and medical condition
- Examples:
  - "Please call at 999-999-9999 who is bleeding through his dressing"
  - "Patient 123456 wants call at 999-999-9999 for dizziness and vomiting"

XII. WORKSTATION SECURITY

A. **Authorized Use:** System computers and communication systems are used for their authorized purposes: to support the treatment, payment, operations, research, educational functions, and other business purposes. Refer to IS policies related to use of computer and communication systems for more information.

B. **Prohibited Activities:** The following categories of use are inappropriate, may jeopardize the security of systems and are therefore prohibited:

1. Tests or attempts to compromise computer or communication system security measures.
2. Attempts to defeat or crack system security passwords, compromise room locks or block alarms.
3. Use damaging the integrity of MercyOne's or other information technology systems, including the following:

   a. Unauthorized access or use, including deliberate and unauthorized changes to data or applications.
   b. Disguised use, such as masquerading or impersonating others.
   c. Modification or removal of data or equipment without specific authorization.
   d. Use of unauthorized devices, such as attachment of any external disk drive, printer, video system, to the information system.
   e. Distributing or launching computer viruses or other forms of malware;
   f. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others, such as by "resource hogging" or "spamming." Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is prohibited, such as distribution of chain letters.

C. **Mobile Workstations:** Mobile workstations such as portable computers and laptops are secured using passwords, locks and other methods, as appropriate.

1. PDAs, given their size and use, require extra precautions to prevent loss or theft. PDAs also require encryption software. See Use of Personal Mobile Technology.

D. **Terminate Access:** Users terminate their session on the computer by either logging out of the application or securing the workstation to a password protected screen saver. Workstations automatically log-off to a password protected screen saver after a period of inactivity, or otherwise terminate an electronic session after a predetermined period of inactivity, as determined by the risk analysis.

E. All workstations are located within a controlled access area or operated in a manner that PHI is not viewable by unauthorized persons.

XIII. DISPOSAL OF PROTECTED INFORMATION

A. No associate of MercyOne will dispose of Confidential or Highly Confidential Information, whether in paper or electronic form, in containers or dumpsters that are accessible to the public.

B. All Confidential and Highly Confidential Information, including PHI, on paper is to be incinerated, shredded or other otherwise physically destroyed. This includes information contained on labels affixed to bottles, IV bags or other containers. All PHI that is shredded must be cross cut shredded to be considered destroyed.

C. See IS-3: Destruction of Confidential Data on Computer Storage Media for procedures on destroying ePHI stored on computer storage media.

XIV. CONTINGENCY AND DISASTER PLANS

A. MercyOne maintains procedures to protect the confidentiality and integrity of ePHI in the case of emergency or disaster.

B. MercyOne has downtime procedures in place to maintain operations in the case of planned or unanticipated information system unavailability.

C. If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the situation is reported to the Vice President of Corporate Compliance.

XV. INFORMATION SYSTEM ACTIVITY REVIEW AND AUDIT CONTROLS

A. Hardware, software and/or procedural mechanisms that record and examine activity in information system that contains or use ePHI are in place, per risk analysis. Records of information system activity, such as audit logs, access reports and security incident tracking reports are maintained for review by MercyOne's information security officer, Vice President of Corporate Compliance and regional privacy officer, as appropriate.

XVI. INTERNET

A. **Internet Access:** Users using the system information technology system to access the Internet are representing the organization. Therefore, users conduct all business on the Internet in a professional manner. Refer to IS-5: Internet Usage and Security for more information.

B. **E-Commerce:** Users are prohibited from establishing any electronic commerce arrangement over the Internet unless the information services department and MercyOne privacy and security officer have first evaluated and approved of such arrangements. Refer to IS-5: Internet Usage and Security for more information.

XVII. PHYSICAL SECURITY OF SYSTEMS WITH ELECTRONIC PROTECTED HEALTH INFORMATION

A. System organizations safeguard facilities and equipment therein from unauthorized physical access, tampering, and theft. PHI is stored and maintained by system organizations in a manner that safeguards it from unauthorized or unintentional access, destruction and damage.

1. Portable computers within the facility are secured, per risk analysis, to prevent theft, manipulation or tampering. Laptop computers outside of the facility are secured per the IS-6 Policy: Remote Access.

2. Network servers, network switches, etc. are placed in locked cabinets, locked cabinets or otherwise physically secured, per risk analysis.
3. Computer and network gear may not be removed from system premises unless the involved person has approval from his or her manager.

B. In the case of a disaster or emergency, facility access is allowed to authorized personnel in support of restoration of lost data.

C. System organizations limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Access to medical records files, computer rooms, offices and other work areas, including patient care or staff work areas containing PHI are physically restricted to those with a business need to access the area. Access to such areas is controlled via lock and key, key card access, keypad combination lock, or other physical security measure, including, but not limited to, visitor control. Access to such restricted areas is terminated when a workforce member's relationship with the organization ceases. Workforce members who are not authorized to have access to information systems containing ePHI but have been authorized to work in a location where there is access to ePHI shall be supervised to the extent required by the nature of their work and potential for access to ePHI.

XVIII. TECHNICAL SAFEGUARDS OF ELECTRONIC PROTECTED HEATLH INFORMATION

A. The information system is protected by a variety of technical safeguards to protect the confidentiality, integrity, and availability of PHI, based on the risk analysis. Safeguards include, but are not limited to:

1. MercyOne has defined standard software for use for a majority of business purposes. Refer to IS policies related to use of computer and communication systems for more information.
2. Users do not forward or execute programs received via e-mail or that come from the Internet.
3. Users, who suspect infection by a computer virus, immediately stop using the involved computer and call the IS help desk.
4. Copyrighted information and software that MercyOne does not have specific approval to store and/or use should not be stored on System systems or networks. Refer to Refer to IS policies related to use of computer and communication systems for more information.
5. Departments with stand-alone system that maintain PHI are responsible for backup and other security measures to protect the confidentiality, integrity, and availability of the information.

XIX. TRANSMISSION SECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION

A. MercyOne shall implement measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. These measures include, as appropriate, integrity controls and encryption.

B. Users are responsible for identifying PHI that is being transmitted electronically and contacting the IS help desk to ensure the proper transmission safeguards are in place.

C. Users who require a modem on require authorization prior to installation by the IS department. Failing to get prior authorization or inappropriately using the modem is sanctionable.

XX. PERSONAL WIRELESS HANDHELD DEVICES

A. Use of all wireless devices must be done in compliance with all MercyOne policies and procedures, including, but not limited to, the Use of Personal Mobile Technology policies.

B. Use of the camera or video function on such devices is prohibited in the workplace, unless specifically authorized by a member of senior management.

C. Any authorized photograph or images is the sole property of MercyOne, and the distribution of the image or photograph may only be made consistent with the applicable Uses and Disclosure of Health Information policy.

DEFINITIONS:

Electronic Protected Health Information: Any individually identifiable health information protected by HIPAA that is transmitted or maintained in electronic media.

Minimum Necessary: PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard applies to all PHI in any form.

Protected Health Information: Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual;
- The provision of health care to an individual; and
- The past, present, or future payment for the provision of health care to an individual.

Security Incident: The unauthorized access, use, disclosure, modification, or destruction of ePHI or interference with system operations in an information system.

User: A person or entity with authorized access to MercyOne's information system.

Workforce: As defined by the HIPAA Privacy Rule, any and all medical staff members, employees, volunteers, trainees and students, and other persons whose conduct in the performance of work for a system organization is under the direct control of a system organization, whether or not they are paid for their activity.

Workstation: An electronic computing device, such as desktop or laptop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit PHI. Workstation devices may include but are not limited to: laptop or desktop computers, personal data assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, workstation also includes the combination of hardware (i.e. Ethernet ports, hard drive, etc.), operating system, application software, and network connection (including remote and wireless).

REFERENCES:
SEE ALSO:
DATE OF ORIGIN: 01/2011
REVIEWED:
REVISED: 05/01/13; 04/01/16
ATTACHMENT:

OTHER COMMITTEE REVIEW / APPROVAL:	MERCYONE NEIA	WATERLOO	OELWEIN	CEDAR FALLS