Ascension

Origination:	*10/23/2017*
Last Reviewed:	*11/16/2017*
Last Revised:	*10/23/2017*
Next Review:	*11/15/2020*
Owner:	*Sarah Kleaveland-Kupczak: VP-Corp Responsibility*
Policy Area:	*Compliance*
Reference Tags:	
Applicability:	*Ascension Wisconsin*

Safeguards for Patient Information, AW

SCOPE

This policy applies to entities that are wholly owned and/or managed by Ascension Wisconsin and subject to HIPAA.

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

PURPOSE/RATIONALE

Our Value of Integrity calls us to ensure that we respect a patient's right to the privacy of their health information and requires us to understand and comply with the applicable state and federal laws.

DEFINITIONS

"Ascension Wisconsin" means all healthcare organizations wholly owned, controlled and/or managed indirectly or directly by Columbia St. Mary's, Inc., Ministry Health Care, Inc. or Wheaton Franciscan Healthcare – Southeast Wisconsin, Inc. or their successor organization.

"Electronic Protected Health Information" (ePHI) means any Individually Identifiable Health Information protected by HIPAA that is transmitted or maintained in electronic media.

"HIPAA" means Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted on August 21, 1996, as amended, provisions of which are found at 45 C.F.R. Subpart 164, and other similar Federal and state laws and regulations protecting patient privacy unless otherwise specified.

"Individually Identifiable Health Information" is information, including demographic data, that relates to:

1. The individual's past, present or future physical or mental health or condition,
2. The provision of health care to the individual, or
3. The past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

"Minimum Necessary" means 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" (PHI) means all Individually Identifiable Health Information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

"Workforce" means 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, as defined by HIPAA.

POLICY

It is the policy of Ascension Wisconsin 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.

PROCEDURE

1. REASONABLE SAFEGUARDS AND INCIDENTAL DISCLOSURES
    a. Incidental disclosures that occur as a by-product of another permissible or required use or disclosure are permitted as long as reasonable safeguards and Minimum Necessary Standards have been put into place.
2. SOCIAL SECURITY NUMBERS (SSN)
    a. Ascension Wisconsin will take reasonable steps to protect patients from identity theft.
    b. Patient social security numbers are Protected Health Information.
    c. Ascension Wisconsin will apply a minimum necessary standard to the use and disclosure of SSN. While there may be instances in which a patient's full social security number is needed, as a general practice, Ascension Wisconsin will only print or display the last four digits of a patient's social security number if feasible.
3. WHITEBOARDS AND MONITORS WITH PATIENT INFORMATION
    a. Ascension Wisconsin uses whiteboard, whether manual or electronic, and monitors to track essential patient information. Ascension Wisconsin 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.

4. OVERHEAD PAGING SYSTEMS
    a. Ascension Wisconsin may use overhead paging systems as a means of communication within its facilities.
    b. Ascension Wisconsin 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. Ascension Wisconsin 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.
        i. Examples of pages that could be used are:
            1. 'The family of the patient in room ___, please contact the operator.'
            2. 'The XXX family, please contact the operator.'
5. MESSAGES FOR PATIENTS AND REMINDER CARDS
    a. Ascension Wisconsin 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, Ascension Wisconsin 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 Ascension Wisconsin associate will ask for a return phone call from the patient.
    b. Ascension Wisconsin 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.
6. FACILITIES
    a. Ascension Wisconsin 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 Ascension Wisconsin may make as reasonable safeguards are:
        i. Areas in which patients are asked protected health information should include signage asking other individuals to stand a few feet back from a counter.
        ii. In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers to safeguard information.
    b. The Office of Civil Rights has indicated that HIPAA does not require the following types of structural or systems changes for patient privacy:
        i. Private rooms.
        ii. Soundproofing of rooms.
        iii. Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
        iv. Encryption of telephone systems.
7. CONVERSATIONS IN PUBLIC SPACES/VISITORS
    a. Associates should conduct conversations involving Protected Health Information in private settings. To the extent that a conversation that involves Protected Health

Information must occur in a public space, associates 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. Associates should ask the patient whether they object to sharing information in front of visitors **prior to starting the conversation**.

8. SIGN IN SHEETS AND CALLING NAMES IN WAITING AREAS
    a. Ascension Wisconsin 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. Ascension Wisconsin will limit the patient information used to call a patient in a waiting room to the patient's first and last name.
9. SECURITY OF PHI IN PAPER FORM
    a. Ascension Wisconsin will ensure that it maintains appropriate safeguard to protect the confidentiality of PHI maintained in a paper form. Ascension Wisconsin may use a combination of safeguards, which include, but are not limited to:
        i. Housing the records in locked files,
        ii. Maintaining the record in areas that has reasonably limited access to the public,
        iii. Ensuring that the area in which the PHI is maintained is supervised,
        iv. 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. Ascension Wisconsin 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 original 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. Ascension Wisconsin will only display the last 4 digits of a SSN on paper forms or reports generated by Ascension Wisconsin when the information is necessary or system will not allow the repression of the full number unless prior approval is received as outlined above.
    e. Ascension Wisconsin may maintain patient charts at bedside or outside of exam rooms, display patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms provided that Ascension Wisconsin reasonably limits access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or 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.
10. FAX MACHINES
    a. Fax machines should be located in areas that are not accessible to the public.
    b. Associates should ensure that the correct number is being used when faxing Protected

Health Information, whether the number is entered manually or is preprogrammed.

c. If a fax is transmitted to the incorrect recipient, report this occurrence to Corporate Responsibility to determine whether breach notification needs to occur.

d. If an associate receives a fax in error, please contact the sender to alert them to the error and destroy the facsimile. Please contact Corporate Responsibility to report the issue.

11. E-MAIL

a. PHI should NOT be transmitted via e-mail (either in the body or as an attachment) over the Internet (externally) unless using secure Zix encryption. To enable Zix encryption, insert either the word **-secure- or -phi-** (hyphens MUST be included without any spaces between the hyphen and words) in the subject field of the email.

i. Underscore cannot be substituted for hyphens

ii. The -secure- or -phi- is not case sensitive

iii. Do not include any PHI in subject line.

b. PHI transmitted internally is acceptable provided that the recipient(s) of the e-mail are verified before the message is sent. Always be aware of email content and the recipient(s) email addresses to know if the email address is external.

c. If an e-mail 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 e-mail in error, please contact the sender to alert them to the error and destroy the email.

12. 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

i. It relates to an appointment reminder and only includes information outlined under the reminder card/phone message section above, or

ii. 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.

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

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

2. An e-mail to a physician's Ascension e-mail account is considered a secure e-mail

3. If a non-Ascension e-mail is to be used, you must type the word -secure- or -phi- in the subject line without spaces. 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.

ii. 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.

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

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

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

13. SHARING INFORMATION WITH INSURANCE COMPANIES
When sending a copy of a remittance advice to an insurance company for billing purposes, all PHI about patients that are not insured by that insurance company must be blacked out (redacted) before forwarding the remittance advice. The information should not be visible through the black mark.

14. DISPOSAL OF PROTECTED INFORMATION

a. No associate of Ascension Wisconsin will dispose of PHI, whether in paper or electronic form, in containers or dumpsters that are accessible to the public.

b. All 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.

REFERENCES

IS-4 Information Security Requirements

ATTACHMENT NAMES

N/A

Attachments:

No Attachments

Approval Signatures

Approver	Date
Sarah Kleaveland-Kupczak: VP-Corp Responsibility	11/16/2017
Nancy Fazio: Compliance Specialist	11/8/2017