Ascension

Origination:	*6/19/2017*
Last Reviewed:	*10/4/2017*
Last Revised:	*10/4/2017*
Next Review:	*10/3/2020*
Owner:	*Sarah Kleaveland-Kupczak: VP-Corp Responsibility*
Policy Area:	*Compliance*
Reference Tags:	
Applicability:	*Ascension Wisconsin*

Patient Privacy Program, AW

SCOPE

This policy applies to all Ascension Wisconsin workforce members, including but not limited to, officers, directors, medical staff members, associates, independent contractors, volunteers, students, and any others having access to health information either through written, verbal or electronic means. This policy applies to all Ascension Wisconsin organizations.

PURPOSE/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.

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.

"Business Associate" is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to a covered entity, who creates, receives, maintains or transmits use or disclosure of individually identifiable health information.

"Confidential Information" means sensitive information, the unauthorized disclosure of which could seriously and adversely impact Ascension Wisconsin. This includes, for example

- Protected Health Information;
- Highly Confidential Information;
- Information regarding health care operations;
- Information about employees; and
- Financial, strategic and other business related information.

"ePHI" means any Protected Health Information that is transmitted or maintained in electronic media.

"Highly Confidential Information" means very sensitive information, requiring greater protection

than Confidential Information. It includes information that is subject to specific confidentiality requirements established by state and federal regulations, such as behavioral health or Alcohol Or Other Drug Abuse (AODA) treatment records . This also includes business related information that could seriously affect Ascension Wisconsin if disclosed inappropriately.

"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:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- 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" is the standard that only the minimum necessary PHI is accessed, used or disclosed to accomplish the intended purpose of the use, disclosure, or request. The Minimum Necessary standard applies to all PHI in any form.

"Notice of Privacy Practices" is a document which outlines how protected health information about an individual may be used and disclosed and under what circumstances specific authorization from the individual may not be required. The Notice of Privacy Practices also describes the HIPAA defined patient rights related to use and disclosure of the individual's health information.

"Organized Health Care Arrangement" means a clinically integrated care setting in which individuals receive health care from more than one health care provider and in which the participating healthcare providers:

1. Hold themselves out to the public as participating in a joint arrangement; and
2. Participate in joint activities that include at least one of the following:
    a. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
    b. Quality assessment and improvement activities, in which treatment provided by participating covered entities are assessed by other participating covered entities or by a third party on their behalf; or
    c. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a healthcare provider is reviewed by other participating healthcare providers or by a third party on their behalf for the purpose of administering the sharing of financial risk.

"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, as defined by HIPAA, 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.

POLICY

It is the policy of the Ascension Wisconsin to protect the privacy of any and all Protected Health Information.

PROCEDURE

PRIVACY OFFICER DESIGNATION AND OVERSIGHT

Ascension Wisconsin's Corporate Responsibility Officer will act as the Ascension Wisconsin privacy officer. The Corporate Responsibility Officer is responsible for the design, implementation and oversight of Ascension Wisconsin's privacy program and provides guidance, direction and authority for the program. The Ascension Wisconsin Regional Security Officer will act as the Security Officer.

Under the direction and guidance of Ascension Wisconsin's Corporate Responsibility Officer, the Corporate Responsibility Department will support privacy program activities including:

1. Developing and directing implementation of procedures relative to the safeguarding of PHI consistent with this and other relevant system and regional policies. This includes changes to procedures in response to changes in law and corresponding policies.
2. Coordinating education and training, as well as ongoing reminders, for workforce members on policies and procedures for safeguarding of PHI.
3. Documenting, investigating, and resolving all privacy complaints, incidents and issues in cooperation with human resources, information systems, and other appropriate personnel.
4. Coordinating ongoing monitoring activities of privacy safeguards and improving procedures based on findings.
5. Providing guidance, when needed, to health information (medical records) to administer patient requests regarding access to, amendments of, confidential communication of, and restrictions on use of PHI.
6. Ensuring that health care operations functions that utilize PHI are consistent with HIPAA requirements.
7. Serving as a resource with regard to the safeguarding of PHI, including serving on committees and participating in meetings, as reasonably requested.

MINIMUM NECESSARY

1. The amount of Confidential and Highly Confidential Information, including PHI, used by a member of the workforce or a Business Associate is limited to the minimum amount needed to perform a specific type of work or to complete an authorized function.
2. Third parties may be given access to a system organization's internal information only

when:

a. A demonstrable need-to-know exists, and

b. The access is consistent with policies or such a disclosure has been expressly authorized by the appropriate leader within Ascension Wisconsin.

- Ascension Wisconsin reserves the right to determine the form in which this information will be provided (e.g., hard copy, electronic data feed, system access) See appropriate specific policies (such as Uses and Disclosure policies) for specific information on the release of PHI to external parties

3. The minimum necessary requirement does not apply to the following disclosures of PHI:
   a. Those for treatment;
   b. Those made directly to the patient or authorized representative;
   c. Those made via a valid patient authorization;
   d. Those required for compliance with HIPAA's electronic transaction standards;
   e. Those to the Secretary of the Department of Health and Human Services;
   f. Those required by state and federal law.
4. Confidential Information, regardless of the medium, shall be restricted through administrative (e.g., policies and procedures), technical (e.g., unique user IDs, passwords, ID badges, etc.), and physical safeguards (e.g., restricted spaces, data centers, etc.). Access to Confidential Information shall be managed through Role-Based Access parameters that have been developed based on the Workforce members' assigned work responsibilities. In general, the determination of appropriate Role-Based assignment of access to Confidential Information shall be the responsibility of the Workforce member's immediate supervisor or designee.
5. The Organization shall specifically have in place a process to determine the appropriate level a Workforce member's access to patient PHI that includes:
   a. An assessment of appropriate Access by the Workforce member to PHI by the individual's supervisor based on:
   b. Job description/position scope/role.
   c. Need-to-Know or Minimum Necessary Access to carry out work responsibilities.
   d. Patient care needs.
   e. Administrative needs.
6. Workforce members with unrestricted access to PHI are limited to accessing only that information required for carrying out job duties for which they are assigned (e.g., provision of healthcare or carrying out related operational duties such as quality audits, infection control monitoring, risk management activities, utilization review, etc.).
7. As needed, Ascension Wisconsin shall perform periodic monitoring of user access audit trails created in applications and systems to ensure compliance by Workforce members to appropriate access of electronic PHI. Methods for the appropriateness of Workforce member access may include:

a. Conducting random audits of access to patient records to determine appropriateness of access.

b. Utilizing exception reports to determine time of access, length of access, access to "confidential" or "VIP" PHI.

c. Focusing on identified problem prone or risk areas in response to complaints or concerns.

d. Auditing "same-name" access.

8. Workforce members who are creating data bases, reports, or other media containing confidential information shall apply the minimum necessary standard and only provide that information needed to meet the needs of the project/requestor. All sensitive data shall be masked, truncated, or eliminated whenever possible (e.g., patient names, SSN, other identifying information, etc.).

EDUCATION AND TRAINING

1. Ascension Wisconsin shall ensure that all members of its Workforce are trained on their role in maintaining the privacy and security of PHI, including training on relevant Ascension Wisconsin policies.

   a. As appropriate, training and education is tailored to a workforce member's role, level of use or contact with PHI.

   b. Members of the workforce are provided reminders on a periodic and ongoing basis to maintain awareness of privacy and information security.

2. An individual that becomes a member of the Ascension Wisconsin Workforce will receive training within a reasonable time of the commencement of his or her association with Ascension Wisconsin. Training is role-based such that certain workforce members may need to receive their training before actually beginning to perform their duties.

3. Training on privacy will be included in annual mandatory training for all associates.

4. Additional training is conducted in a timely manner whenever there is a material change in laws or regulations affecting the confidentiality, privacy or security of PHI.

5. Managers are responsible for verifying that training is completed on a timely basis. This management responsibility includes other Workforce Members in addition to department employees, such as students, volunteers, contingent workers who are providing services within the manager's scope of responsibility.

6. Ascension Wisconsin will retain documentation within its e-learning system demonstrating the fact that education and training has taken place, the scope of the training program and the names of individuals who have completed training. To the extent that the education takes place outside of the e-learning system, the manager of the workforce members will maintain information about the training as outlined above.

BUSINESS ASSOCIATES

1. Ascension Wisconsin may engage individuals or entities that are not part of its workforce to assist it in performing a business function. These individuals or entities may be considered Business Associates to the extent they receive PHI. If Ascension Wisconsin engages a Business Associate, managers within Ascension Wisconsin must assure that

that a Business Associate Agreement is in place. Assistance in determining if an organization or person is a Business Associate is available from the Corporate Responsibility Department or the Office of General Counsel.

2. Contracts or relationships with Business Associates include a Business Associate Agreement that contains all provisions required by HIPAA to ensure that the necessary privacy and security protections can be expected of such Business Associates. A template Business Associate Agreement will be available through the Office of General Counsel and on the intranet.
3. If an Ascension Wisconsin associate suspects or knows of a violation of the Business Associate Agreement by a Business Associate, the associate must contact the Corporate Responsibility Department. The Corporate Responsibility Officer (or designee) will conduct an investigation and work with the business lead and the Business Associate to take reasonable steps to end the violation if it has occurred.
    a. If such steps are unsuccessful, the Ascension Wisconsin organization will terminate the underlying agreement with the Business Associate.
    b. If the underlying agreement cannot feasibly be terminated because the Business Associate is a unique provider of the product or service and a suitable replacement could not be found, the Corporate Responsibility Officer or the Office of General Counsel will determine appropriate actions.

MONITORING, AUDITING AND EVALUATION

1. Ascension Wisconsin maintains an on-going monitoring program, including periodic auditing, of Ascension Wisconsin's compliance with respect to the safeguarding of PHI, based on the risk analysis, to assess the extent to which its privacy and information security policies and procedures are effective.
2. To ensure compliance with system policies as well as applicable laws and regulations, system management reserves the right to monitor, inspect and/or search at any time all system information systems and other applicable business related areas. This right applies to all users, including staff, members of the workforce, vendors and persons with remote access. This examination may take place with or without the consent, presence, or knowledge of the involved user. The information systems and areas subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voicemail files, printer spool files, fax machine output, desk drawers, and storage areas.

PRIVACY AND INFORMATION SECURITY COMPLAINT OR INCIDENT REPORTING AND INVESTIGATION

1. A Workforce member who receives any privacy related complaint or incident from a patient, Business Associate or other third party or has a reasonable belief that an intentional or unintentional breach of privacy has occurred, is required to immediately report such information to:
    a. his or her immediate supervisor,
    b. human resources department,
    c. Corporate Responsibility Officer (or designee),

d. Information Security (if related to electronic Protected Information),or

e. the Values Line, if anonymity is desired.

f. If the Corporate Responsibility Officer (or designee) was not initially contacted, those receiving such an initial report must immediately notify the Corporate Responsibility Officer (or designee). A goal of this reporting and subsequent investigation is to mitigate harmful effects of privacy breaches.

g. All suspected policy violations, system intrusions, virus infestations, and other security incident which might jeopardize system information or information system are immediately reported to the Ascension Information Services help desk. If the incident may affect patient privacy, the Corporate Responsibility Officer (or designee) will be notified.

2. All privacy complaints and reports of potential breaches are promptly and thoroughly investigated. Investigations shall be conducted with involvement of the Corporate Responsibility Department. The Office of General Counsel, Human Resources, Risk Management or the Information Services department are involved as necessary.
3. All information security incidents are promptly and thoroughly investigated by Information Services. The Corporate Responsibility Officer (or designee) is involved as necessary.
4. For potential privacy breaches involving more than 20 individuals, the Corporate Responsibility Officer will bring together an incident response team (in conjunction with the IS incident response team) to complete any investigative and notification steps determined to be appropriate.
5. Where appropriate, implementation of a corrective action plan to resolve and correct the incident is developed. Corrective action with regard to a workforce member may include sanctions. If appropriate, the Corporate Responsibility Officer (or designee), or his or her designee, communicates the outcome of investigations to the individual filing the complaint or reporting the incident. Notice of a confirmed breach will be given in accordance with Breach Notification-Protected Health Information, AW policy (*3446164)*.

DOCUMENTATION OF PRIVACY COMPLAINTS, BREACHES AND INCIDENTS

1. The Corporate Responsibility Officer (or designee) will maintain a log of all reported privacy complaints, incidents and breaches including information such as:
   a. Date and time of complaint or incident;
   b. Name of person making the complaint, as applicable;
   c. Objective description of the nature of the complaint or incident;
   d. Ultimate resolution of the complaint or incident; and
   e. Whether breach notification occurred.
2. On a regular basis, the Corporate Responsibility Officer reports information about privacy complaints to the appropriate board committee.
3. Upon receipt of a complaint from the Office for Civil Rights, the recipient will forward the complaint to the Corporate Responsibility Officer. The Corporate Responsibility Officer (or his/her designees) will investigate, notify legal counsel and draft a response.

NOTICE OF PRIVACY PRACTICES TO PATIENTS

1. As part of Ascension Wisconsin's privacy program, Ascension Wisconsin will provide all patients with information that gives patients written notice of the uses and disclosures of PHI that Ascension Wisconsin may make according to the Confidentiality and Patient Privacy Rights With Regard to Protected Health Information, AW policy. Ascension Wisconsin will also provide information about the patient's rights and Ascension Wisconsin's legal duties with respect to PHI (the 'Privacy Notice'). The Privacy Notice is made available no later than the date of the first service delivery.
2. To document receipt of the Privacy Notice, a good faith effort to obtain a written acknowledgment from the patient shall be made at each initial distribution of the Privacy Notice, at a minimum. Acknowledgment will most often be contained in the patient's general treatment consent or conditions of treatment form signed prior to services.
3. Ascension Wisconsin promptly revises and distributes the Privacy Notice whenever there is a material change to the uses or disclosures, the individual's rights, Ascension Wisconsin's legal duties, or other privacy practices stated in the Privacy Notice. Except when required by law, a material change to any term of the Privacy Notice may not be implemented prior to the effective date of the Privacy Notice in which such material change is reflected.

ORGANIZED HEALTH CARE ARRANGEMENTS (OHCA)

1. Ascension Wisconsin organizations have entered into OHCAs with other health care providers (including medical staff members) in order to provide direct patient care services through clinically integrated settings (e.g., inpatient or outpatient hospital settings and/or other hospital-based clinic settings). This type of arrangement facilitates the flow of PHI for purposes of treatment, payment, and health care operations.
2. Each Ascension Wisconsin organization is part of an OHCA with:
    a. All entities owned, operated and managed by Ascension Wisconsin, and
    b. All treating health care professionals and others who enter information into the health record Ascension Wisconsin maintains, including, but not limited to Ascension Wisconsin medical and allied health staff members.
3. Members of the OHCA must agree to issue the same Privacy Notice for services provided within the OHCA, however, only one member of the OHCA must deliver the joint Privacy Notice for patients treated through the OHCA.
4. If a member of an OHCA also operates his/her own private practice with privacy practices different from that of the OHCA, that provider must deliver his/her own Privacy Notice for patients of the private practice.

Each health care provider who is part of the OHCA is required to abide by the terms of the joint Privacy Notice with respect to PHI created or received by each health care provider.

DOCUMENT RETENTION REQUIREMENTS

Ascension Wisconsin will retain documentation of its privacy program, including but not limited to, copy of each Notice of Privacy, the log of privacy complaints and acknowledgement of receipt for a minimum of six years.

REFERENCES

N/A

ATTACHMENT NAMES

N/A

Attachments:

No Attachments

Approval Signatures

Approver	Date
Sarah Kleaveland-Kupczak: VP-Corp Responsibility	10/4/2017
Nancy Fazio: Compliance Specialist	10/4/2017