Inappropriate Access to Protected Health Information (PHI)

OUTCOME STATEMENT:

Access to SSM Health (“SSM”) protected health information (“PHI”) is only allowed when it is required for treatment, payment and health care operations purposes, and when otherwise permitted by law. Processes and tools have been implemented to monitor access of PHI, identify improper access, use, or disclosure, and take corrective actions necessary to deter such inappropriate activities.

SCOPE:

This policy is applicable to SSM Health hospitals* and other operated ministries.

FILE MAINTENANCE INFORMATION:

Original Effective Date: September 12, 2013
Revision Dates: 04/19/2022
Review Dates:
Author(s): Corporate Responsibility, Privacy Officer
Key Stakeholder Reviews: System VP, Corporate Responsibility
Body or Person Last Approved: Chief General Counsel

* As required by CMS Regulation §482.12 A-0043 Conditions of Participation: Governing Body, the following hospitals are included as SSM entities:
Missouri: (1) SSM Health St. Mary’s Hospital – St. Louis and SSM Health Cardinal Glennon Children’s Hospital, (2) SSM Health DePaul Hospital – St. Louis, (3) SSM Health St. Clare Hospital – Fenton, (4) SSM Health St. Joseph Hospital – Lake St. Louis, (5) SSM Health St. Joseph Hospital – St. Charles and SSM Health St. Joseph Hospital – Wentzville, (6) SSM Health Saint Louis University Hospital (Effective 2/8/2021), (7) SSM Health St. Mary’s Hospital – Jefferson City,
Oklahoma: (1) SSM St. Anthony Hospital and Bone & Joint Hospital at St. Anthony, (2) SSM St. Anthony Shawnee Hospital, (3) SSM Health St. Anthony Hospital Midwest City
Wisconsin: (1) SSM Health St. Mary’s Hospital – Madison, (2) SSM Health St. Clare Hospital – Baraboo, (3) SSM Health St. Mary’s Hospital – Janesville, (4) SSM Monroe Hospital (Effective 2/7/2020), (5) SSM Health Ripon Community Hospital (Effective 2/7/2020), (6) SSM Waupun Memorial Hospital (Effective 2/7/2020), (7) SSM St. Agnes Hospital (Effective 2/7/2020).
Illinois: (1) SSM Health St. Mary's Hospital – Centralia and (2) SSM Health Good Samaritan Hospital – Mt. Vernon

Printed copies are for reference only. Please refer to the electronic copy in PolicyTech for the latest version.
DEFINITIONS:

I. Clinicians: Health care professionals, including, but not limited to, physicians, physician assistants, nurse practitioners, nurses, therapists and ancillary staff.

II. Family Member: For the purposes of this policy, the term “family member” is defined broadly, regardless of legal representation, and includes:
   A. spouse;
   B. natural or adoptive parent, child or sibling;
   C. step-parent, step-child, stepbrother or stepsister;
   D. father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law;
   E. grandparent, grandchild, or the spouse of grandparent or grandchild;
   F. any person who resides in the same household as the employee; and
   G. A step-relationship or an in-law relationship continues to exist even if the marriage upon which the relationship is based is terminated by the divorce of the parties or the death of one of the parties.

III. Inappropriate Access Audit: An audit may be done as a periodic event, as a result of a patient complaint, or because of suspicion of employee wrongdoing. Inappropriate access audits provide documentation regarding who (login credentials) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time).

IV. Protected Health Information (PHI): individually identifiable health information concerning a patient’s health, healthcare or payment for their care that is transmitted by or maintained in electronic media (ePHI) or transmitted by or maintained in any other form or medium (including paper and oral). Protected health information excludes individually identifiable health information in certain educational records, certain postsecondary education records, and employment records held by a covered entity (CE) in its role as employer.

V. Workforce - All employees, consultants, temporary employees, contractors, physicians and vendors.

PROCESS:

I. Inappropriate Access
   a. Patient information is only to be accessed when authorized for treatment, payment, or health care operations purposes, and with a need to know. SSM Health (SSM) prohibits workforce members from viewing or accessing their own PHI, or the PHI of their friends, family, co-workers, or any other patient without an authorized business purpose, through any mechanism other than through the entity’s established release of information process.
   b. Workforce members should adhere to the Self-Treatment or Treatment of Family Members by Clinicians Policy and except in cases of emergency, where no other clinician is available, clinicians should not access PHI to treat themselves nor members of their family as defined above.
   c. In order to maintain data integrity, SSM imposes the reasonable requirement that to access PHI, workforce members must use the same policies in place for all patients to request access to their own PHI through the HIM department release of information process, MyChart, or other publicly available patient portal.
   d. Unless the access is to provide direct care or to carry out your SSM job responsibilities, the following examples represent inappropriate access to the EHR regardless of intent:
i. accessing your own health information (Employees must follow the same processes as patients to access their health records.)

ii. accessing a child or other dependent’s health information

iii. accessing a parent or other relative’s health information directly in the EHR (even if you have durable power of attorney)

iv. accessing a spouse’s health information

v. accessing a co-worker’s or any SSM Health employee’s health information

vi. accessing a friend’s, neighbor’s, newsworthy person’s, or any other person’s health information

vii. accessing patient information out of curiosity or for purposes of validating gossip, news stories, social media posts, etc.

II. Duty to Report

a. SSM requires all workforce members to report any matter which may reasonably present a violation of this policy.

b. Reports shall be made to:
   i. the reporter’s immediate supervisor;
   ii. a senior leader at the ministry where the concern arose;
   iii. the ministry’s Privacy Specialist or other Corporate Responsibility (CR) contact; or
   iv. the CRP Helpline, which includes an option to report concerns anonymously.

c. No form of retaliatory action will be permitted against any workforce member with respect to her or his involvement in an investigation or reporting or seeking advice on a matter which they believe in good faith is an ethical, legal, regulatory or policy violation.

III. Monitoring and Auditing for Inappropriate Access

a. Access will be monitored for all users of EPIC including workforce members, vendors, consultants, students and other non-SSM Health users.

b. Inappropriate Access audits may be performed on all users to evaluate information system access and activity (e.g., log-ins, file accesses and security incidents).

   i. Routine Audits will be performed on a regular basis to identify potential inappropriate access involving, but not limited to, any of the following: self-access, same household/neighbor snooping, co-worker snooping, family member snooping, patients of interest, high-volume access, and “break-the-glass.”

   ii. Event-driven audits will be performed as needed in order to investigate concerns and allegations of inappropriate access. The audits may include use of the audit trail viewer function and other technical mechanisms that track and record computer/system activities to detect and/or validate suspicious events.

c. Privacy Specialists will review all inappropriate access audit findings and involve the user’s manager, or other responsible individual, as needed, in the determination of whether the access was appropriate.

d. If the inappropriate access is substantiated, the Privacy Specialist will work with the appropriate manager and Human Resources leader to apply the Corrective Action for Violation of SSM Privacy Policies and/or HIPAA Rules policy. The Privacy Specialist will also conduct a breach analysis and conduct any required notifications.

e. The System CR/HIPAA Office shall retain all documentation of the investigations and corrective actions taken in accordance with Record Retention and Destruction requirements.

IV. Violations of This Policy
Any breach of confidentiality should be brought to the attention of a manager or SSM CR/HIPAA leader. All reported privacy violations will be investigated, and appropriate disciplinary action will be taken in accordance with the Corrective Action for Violation of SSM Privacy Policies and/or HIPAA Rules Policy. Consultants, temporary employees, contractors, physicians or vendors will be investigated for any reported breach of confidentiality and appropriate disciplinary actions will be taken.

a. All workforce members must follow all SSM Health policies relating to preventing improper use or access to patient information and other confidential information and/or information related to SSM Health ministry, business strategies, reimbursement information, negotiations with employer, other organizations, or community groups. Persons who violate this policy will be referred to the appropriate administrative representative or medical staff committee for discipline, up to and including termination/dismissal.

REFERENCES:

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy standards (45 CFR Part 164.506) require covered entities to implement safeguards to protect the privacy of protected health information (“PHI”).

SSM Policy: Corrective Action for Violation of SSM Privacy Policies and/or HIPAA Rules
SSM Policy: Self-Treatment or Treatment of Family Members by Clinicians