PROVIDENCE
Sacred Heart Medical Center
Sacred Heart Children's Hospital
Holy Family Hospital

TITLE: Confidentiality Guidelines for Credentialed Staff

Approval Date:
PHFH MEC 5/2017
PSHMC MEC – 5/2017

Purpose: To provide guidelines for maintaining confidentiality of information and provide guidelines for responding when guidelines are breached.

Policy statement:
Credentialed providers at all Providence hospitals shall maintain all information (financial, technical, intellectual, and clinical) acquired in the course of their duties in a confidential manner. Providers are prohibited from the use or disclosure of confidential information for any personal gain or in a manner detrimental to the best interests of any facility under the umbrella of PH&S. Inappropriate discussion or release of patient's condition, nursing or medical care, or any personal information about a patient (including financial status) is considered to be a violation of privacy.

Specifics

- Confidentiality is a basic responsibility for all credentialed staff members as defined in the bylaws.
- All medical staff members who have direct or indirect access to data pertaining to the admission, care, and disposition of any and all patients treated must maintain that information with the strictest confidentiality.
- Providers will only access records for patients that they are caring for, with the exception of access for the purpose of hospital-authorized peer review.
- Credentialed Providers may access their personal medical records, but they may not access the medical records of family members and others without providing a valid HIPAA compliant authorization to Health Information Management. All providers and patients are encouraged to utilize 'My Chart.'
- Epic 'in-basket' is for communication between members of the treating team. It is not to be used for communication (such as routed results and documents, staff messages, etc.) with family members or physician-patients, as this may inadvertently give access to the full patient medical record and result in a HIPAA violation. (This does not apply to MyChart communication received and acted on from the "InBasket")
- This policy applies to any and all information obtained through the EHR or any other data source regarding diagnostic test information, financial data, and/or other personal information.
- Records, discussions, minutes, and other activities related to the evaluation of patient

care, risk management, quality assessment, peer review, and medical staff meetings, etc are also considered confidential and privileged. Access to such data is on a 'need to know' basis.

- Medical staff professional and credential files are considered confidential and privileged and access is granted to only those who have a 'need to know'.
- Each individual is responsible for helping ensure the security of patient health information by taking appropriate measures to prevent its access, modification by, or disclosure to unauthorized personnel.
- This responsibility pertains to both the physical security of paper documents, personal computers, printers, fax, and copy machines, as well as computer-based access passwords and other locking devices.
- Providers must also take precautions regarding verbal information. Patient information should not be discussed in public areas (elevator, halls, cafeteria, etc).
- 'Provsecure' encryption must be used for all confidential information being sent or forwarded outside the organization.

.

Any unauthorized access, modification, releasing, or casual discussion of confidential information by an employee, student, volunteer, physician, contract worker or other agent shall be considered to be a violation of the patient's privacy and shall be considered gross misconduct and subject to discipline by the medical staff, up to and including summary suspension. Failure to consistently act in a responsible manner regarding the security and protection of patient health information may also result in dismissal.

Guidelines

Level I Violation

A Level 1 Violation is accidental or due to lack or privacy or security training. Examples include but are not limited to:

- Failure to sign off a computer terminal when left unattended for an extended period of time
- Access records of family members or any other patient without written authorization and/or direct involvement in the care.
- Sharing passwords
- Failure to secure protected health information viewed on personal devices such as smart phones and IPads.

Level I corrective action can include the following sanctions:

- Verbal warning or written notification from the practitioner's section/department chair/division chief.

Level II Violation

A Level II Violation is a purposeful disregard of organizational policy or a repeated Level I Violation. Examples can include but are not limited to:

- Using aggregate data without institutional approval
- Repeat level I violation

Level II corrective action can include the following sanctions:

- Requirement to meet with the section/department chair/division chief, written warning.

Level III Violation

A Level III Violation is a malicious disregard of organizational policies. Examples can include but are not limited to:

- Accessing record for the purposes of gaining information regarding competing physicians and/or physician group
- Releasing data for personal gain
- Destroying or altering data intentionally
- Releasing data with the intent to harm an individual or the organization
- Repeat level II violation

Level III corrective action has high likelihood for temporary suspension and/or termination of privileges.

Retention and accounting for disclosures

- Privacy Record Violations are recorded and maintained in the practitioners credential file. All confirmed violations are tracked in the disclosures for the respective patient.