Health ONE® Swedish Medical Center

Origination:	*01/2015*
Last Approved:	*01/2015*
Last Revised:	*01/2015*
Next Review:	*01/2018*
Owner:	*Jaime Kocanda: Director, HIM*
Area:	*Health Information Management*
References:	
Applicability:	*Swedish Medical Center*

Sanctions for Privacy and Information Security Violations

Purpose:

To facilitate compliance with the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), 45 CFR Parts 160 and 164, Administrative Requirements, the HIPAA Standards for the Protection of Electronic Protected Health Information (Security Standards), 45 CFR Parts 160, 162, and 164, the Health Information Technology for Economic and Clinical Health Act (HITECH), Subtitle D – Privacy, and 45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information; Interim Final Rule. To establish guidelines for sanctions for violations of the Company Privacy Policies (IP.PRI.001 through IP.PRI.013), the facility's Privacy Policies, Company Information Security Policies (IP.SEC.001 through IP.SEC.021), and Company Information Security Standards.

Policy:

Sanctions for privacy and information security-related violations must be applied consistently. Each of the examples in the Procedure section, as well as any patient privacy-related and/or information security-related violation, must be addressed through privacy and information security sanctions as outlined by the Facility Ethics & Compliance Committee (FECC) (the committee(s) with responsibility for privacy and information security oversight).

Refer to the HIPAA Privacy Standards, 45 CFR Parts 160.101 and 164.501, and IP.PRI.001, the Patient Privacy Program Requirements Policy, for definitions.

Procedure:

This section describes methods for determining the response to a privacy and/or information security violation. The procedure includes an outline of categories of violations with examples and recommended appropriate actions. The facility Human Resources Director should be involved in all policy and disciplinary action decisions. Please note: The examples and recommended actions are not designed to capture every situation involving privacy and information security violations.

The Facility Privacy Official (FPO) and/or Facility Information Security Official (FISO) and employee's manager must investigate several factors before assigning a category of violation (see Violation Categories and Examples). Questions to consider are:

- What is the severity?
  - How many patients were affected?
  - To what degree was a patient harmed?
  - What type of information was inappropriately accessed, used, or disclosed (*e.g.*, was the protected health information (PHI) considered sensitive as described in EC.025, the Reporting Compliance Issues and Occurrences to the Corporate Office policy)?
  - To what degree was the confidentiality, integrity, and/or availability of systems or data impacted?
  - To what degree did the action place the facility's or the enterprise's systems or network at risk?
- Was the inappropriate action **negligent** or **intentional**?
- Did the inappropriate action cause harm or is it likely to cause harm to a patient or others?
- To what degree was the facility able to verify the specifics of a situation through audit trails, interviews, or other facts?

In addition to the nature of the violation itself, answers to the following questions may affect the severity of disciplinary action:

- What is the workforce members' past work record?
- Has the workforce member been disciplined for violations of Policies and Procedures or Information Security Standards in the past?
- How long has the workforce member been employed?
- What is the workforce member's quality of service to the facility?
- Does the workforce member have any written warnings for violations in his or her HR file?

Any actions that indicate a workforce member's considered lack of focus on and commitment to basic privacy and security principles should result in termination regardless of all other aspects of the workforce member's past performance and/or work history. In addition, referrals to law enforcement may be made for incidents of stealing information from company information systems to commit identity theft and to investigate incidents involving accessing inappropriate material on the Company network, depending on the nature of the material accessed.

As the FPO and/or FISO becomes aware of a potential violation with a Company or facility policy or standard, the FPO and/or FISO must discuss the situation with the affected employee's department supervisor and, depending upon the severity of the issue, the FPO and/or FISO or individual's supervisor may consult with the Ethics & Compliance Officer (ECO), Human Resources, the Corporate Ethics & Compliance Department, Corporate Human Resources, the Company's Chief Privacy Officer, the division's Director of Information Security Assurance (DISA), Company's Chief Information Security Officer, the Corporate Privacy Program, and/or the Company's Information Security Program. The ECO must be notified of intentional violations. Depending on the severity of the issue, facilities may suspend an employee during the investigation of the potential violation, in accordance with other human resources policies and procedures. In addition, privileges to mobile devices or laptops may be suspended or revoked depending on the specific issue that has occurred.

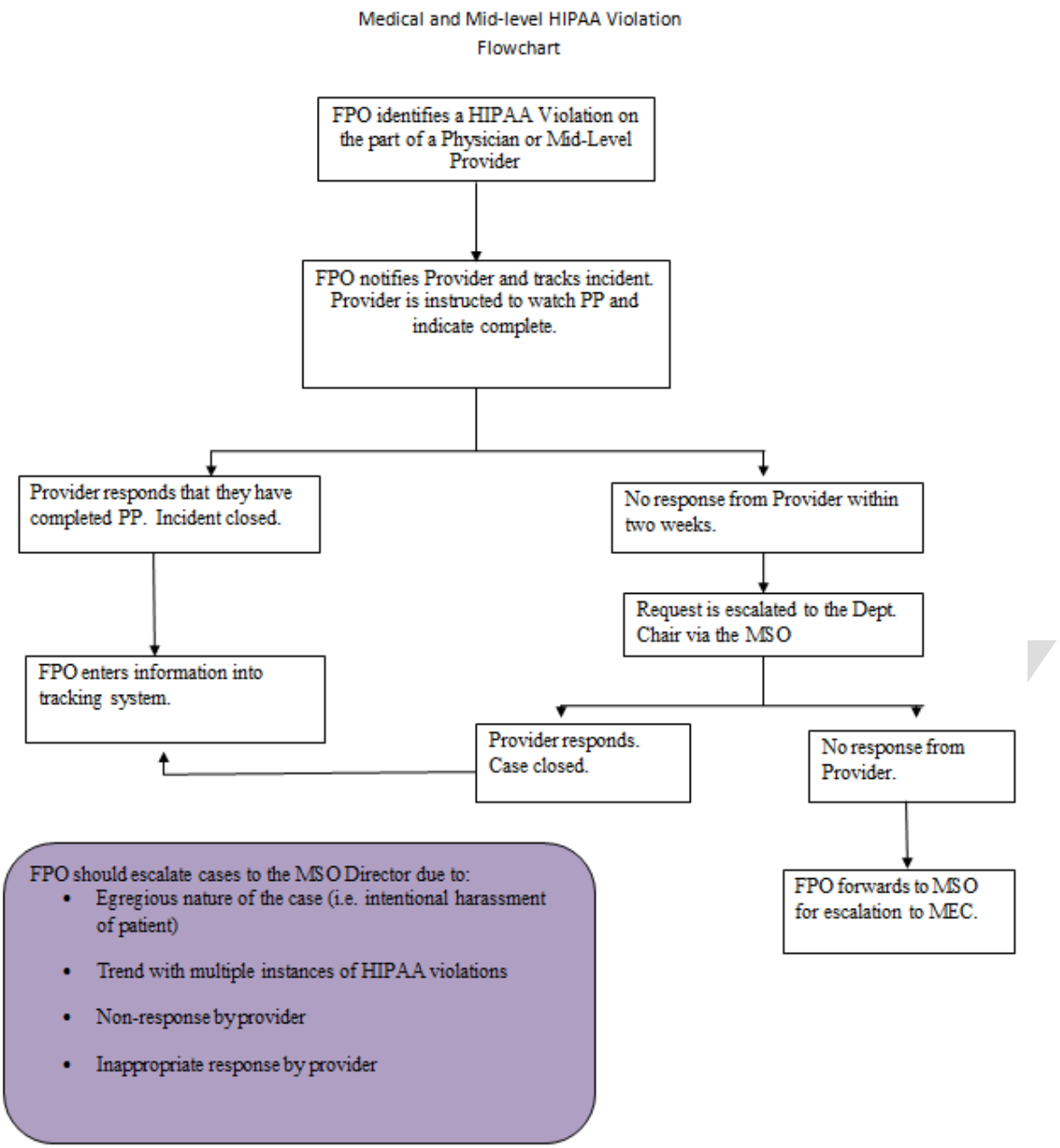
All documentation relative to disciplinary action pursuant to this policy, to include documentation pertaining to oral warnings, must be maintained/retained per the Records Management Policy, EC.014, or for six (6) years, whichever is longer.

Violation Categories and Examples

For purposes of this policy two violation categories will be used and examples of each provided. The two categories are:

- **Negligent**

- **Intentional**



References

1. Patient Privacy Program Policies, IP.PRI.001 –IP.PRI.013
2. Records Management Policy, EC.014
3. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164
4. American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D
5. Information Security Policies, IP.SEC.001 – IP.SEC.021
6. Reporting Compliance Issues and Occurrences to the Corporate Office, EC.025

7. Appropriate Use of Communications, Resources and Systems, EC.026
8. IP.SEC.001 Information Security - Program Requirements
9. WS.SWB.01 - Management Responsibilities
10. WS.SWB.02 - Security Awareness & Training
11. WS.SWB.03 - Sanctions Process

POLICY NUMBER: FAC.IM.336

Attachments:

Image 01

Medical and Mid-Level HIPAA Violation Flowchart