MODEL Facility Policy

POLICY NAME: Sanctions for Privacy and Information Security Violations

DATE: (facility to insert date here)

NUMBER: (facility to insert number here)

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), the Company's Responsible AI Policy (EC.031), 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 _____ committee (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 as well as procedures for phishing test failures and follow-up 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.

[Before implementing this Policy, the facility's executive management must decide how to address disciplinary actions for physicians and reference the process or corresponding policy or procedure in this Policy. For facilities in a **union environment**, confer with labor counsel and/or corporate human resources prior to implementing this Policy; however, note that this is a required policy.]

The Facility Privacy Official (FPO) and/or Facility Information Security Official (FISO) and workforce member's manager must investigate several factors before assigning a category of violation where applicable (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 or the enterprise systems or networks at risk?
- Was the inappropriate action **negligent** or **grossly negligent**?
- 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 Human Resource (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 workforce member'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 grossly negligent violations. Depending on the severity of the issue, facilities may suspend a workforce member 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 violation categories are:

1. **Negligent**
2. **Gross Negligence**

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. Responsible AI Policy, EC.031
7. Reporting Compliance Issues and Occurrences to the Corporate Office, EC.025
8. Appropriate Use of Communications, Resources and Systems, EC.026
9. Information Security - Program Requirements, IP.SEC.001
10. WS.SWB.01 - Management Responsibilities
11. WS.SWB.02 - Security Awareness & Training
12. WS.SWB.03 - Sanctions Process

Minimum Recommended Privacy and Information Security Violation Level Grid

*Note: This list is not all inclusive. A complete investigation must be performed to determine the most appropriate sanction for the particular situation given the severity and frequency of the violation(s) (*i.e., *a single Negligent Violation could result in termination of employment). The policy must be applied consistently.*

Examples of Violations	**Minimum Recommended Range of Actions for <u>Negligent</u> Violations** *Accidental/inadvertent and/or due to lack of proper education or an unacceptable number of previous violations*	**Minimum Recommended Range of Actions for <u>Gross Negligence</u> Violations** *Purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations*
• Inappropriate access, use, disclosure, or disposal of sensitive information • Inappropriate use, disclosure, or submission of sensitive information through an Artificial Intelligence-based platform, system, program, or tool (e.g., chatbots, generative text or image programs such as ChatGPT or DALL-E) in a manner inconsistent with EC.031 • Sending sensitive information via mail, email or fax to a non-authorized individual or the wrong provider • Sending sensitive information via email unencrypted • Improper protection of sensitive information • Failure to properly sign-off a workstation • Failure to properly safeguard username and passwords and/or sharing passwords • Opening an attachment in an unexpected email from an unknown third party, or opening an unknown link,	• Re-training and Re-evaluation. *To* • Re-training and re-evaluation and • Written warning with discussion of policy, procedures and requirements.	• Re-training and re-evaluation and • Written warning with discussion of policy, procedures and requirements. *To* • Termination of employment • Termination of vendor contract

Examples of Violations	Minimum Recommended Range of Actions for <u>Negligent</u> Violations *Accidental/inadvertent and/or due to lack of proper education or an unacceptable number of previous violations*	Minimum Recommended Range of Actions for <u>Gross Negligence</u> Violations *Purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations*
resulting in the computer becoming infected with malware • Not accounting for disclosures outside of treatment, payment or health care operations within the correct system or manual process • Registering an account as worker's compensation that is unrelated to a worker's compensation injury • Leaving detailed sensitive information on an answering machine • Not properly verifying individuals by phone, in person or in writing • FPO and/or FISO/DISA provides inadequate privacy or information security training procedures • Shipping or transporting computers, devices, or media offsite without using encryption, appropriate media sanitization, or required physical safeguards • Failure to properly handle a request for confidential communications • Failure to verify a patient's Directory Opt Out status • Improper control of security credentials/badge	• Re-training and Re-evaluation *To* • Re-training and Re-evaluation and • Written warning with discussion of policy, procedures and requirements	• Re-training and Re-evaluation and • Written warning with discussion of policy, procedures and requirements *To* • Termination of employment • Termination of vendor contract

Examples of Violations	**Minimum Recommended Range of Actions for <u>Negligent</u> Violations** *Accidental/inadvertent and/or due to lack of proper education or an unacceptable number of previous violations*	**Minimum Recommended Range of Actions for <u>Gross Negligence</u> Violations** *Purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations*
• Misusing the Company network to view inappropriate material • Intentionally bypassing Company network security controls for unauthorized reasons • Posting sensitive information on the internet or a violation of the Appropriate Use of Communications Resources and Systems policy, EC.026 • Photographing a patient within the facility for personal use • Sale of sensitive information to any source • Stealing sensitive information to commit identity theft • Disabling information security tools, bypassing security measures, and misusing tools that can compromise information security systems (*e.g.*, deliberately compromising electronic information security measures)	• Re-training and Re-evaluation *To* • Re-training and Re-evaluation and • Written warning with discussion of policy, procedures and requirements	• Re-training and Re-evaluation and • Written warning with discussion of policy, procedures and requirements *To* • Termination of employment • Termination of vendor contract

Phishing Test Failure Follow-Up Actions

Note: The follow-up plan must be applied consistently.

Number of Phishing Test Fails	Consequence/Actions
1	• Colleague receives email education • Colleague is assigned a phishing training in HealthStream • Failure list is shared with local facility leadership
2	• Colleague's manager is emailed and asked to discuss phishing failures with colleague • Failure list is shared with local facility leadership
3	• Colleague is invited to in-person/WebEx training about phishing • Colleague's Expanded Internet Access (EIA) access and computer administrative access is reviewed (and removed, if appropriate) • Failure list is shared with local facility leadership
4	• Ability to receive {EXTERNAL} email removed, unless manager deems colleague must receive {EXTERNAL} email • Failure list is shared with local facility leadership
5	• Sanctions up to and including termination at the equivalent of five occurrences in one, rolling 12-month period • Failure list is shared with local facility leadership

37518337.2