HIPAA Violation Sanction Policy

**PURPOSE:**

[Insert Covered Entity or Business Associate name] is committed to safeguarding the confidentiality, integrity, and availability of PHI applications, systems, and networks.

It is in the best interest of [Insert Covered Entity or Business Associate name] to address the issue of securing the Privacy and Security of individually-identifiable health information in a proactive manner through implementation of sanction practice standards.

Aside from the necessity to ensure patient privacy as an ethical obligation, it is smart business. Data breach notification laws in more than 40 states require an organization to notify breach victims, which can damage its reputation.

In the event, that you as an employee of [Insert Covered Entity or Business Associate name] are responsible for a Violation of the Privacy Practices and/or violate the Health Insurance Portability and Accountability Act of 1996 (HIPPA), the following sanction guidelines would apply.

**DEFINITION OF OFFENSES:**

Class I offenses: Unintentional breach of privacy or security that may be caused by lack of knowledge, lack of judgment, or human error such as:

1. Accessing information that you do not need to know to do your job.
2. Sharing PHI with another employee without authorization.
3. Copying PHI without authorization.
4. Changing PHI without authorization.
5. Discussing confidential information in a public area or in an area where the public could overhear the conversation.
6. Discussing confidential information with an unauthorized person.

Class II offenses: Unintentional breach of privacy or security that may be caused by carelessness, such as:

1. Leaving your computer unattended while you are logged into a PHI program.
2. Failure to cooperate with privacy officer.
3. Sharing PHI with another employee without authorization.
4. Copying PHI without authorization.
5. Changing PHI without authorization.
6. Misdirecting a faxed document containing PHI.
7. Discussing confidential information with an unauthorized person.

Class III offenses: Failure to follow Policies and Procedures. Examples include:

1. Second offense of any class I or class II offense (does not have to be the same offense).
2. Sharing your computer access codes (username & password).
3. Using another person’s computer access codes (username & password).
4. Unauthorized use or disclosure of PHI.
5. Copying PHI without authorization.
6. Changing PHI without authorization.
7. Failure to comply with policies and procedures already in place.
8. Failure to comply with a resolution team resolution or recommendation.

Class IV offenses: Deliberate or purposeful violation without harmful intent. This is an intentional violation due to curiosity or desire to gain information for personal use. Examples of this type of incident include:

1. Accessing the information of high profile people or celebrities.
2. Accessing or using PHI without a legitimate need to do so, such as checking the results of a coworker's pregnancy test.
3. Requesting his/her own prescription refill via EMR.
4. Making changes in his/her own chart.

Class V offenses: Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples include:

1. Third offense of any class I or class II offense (does not have to be the same offense).
2. Second offense of any class III or class IV offense (does not have to be the same offense).
3. Obtaining PHI under false pretenses.
4. Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm.
5. Deliberately destroying or altering records with intent to defraud [Insert Covered Entity or Business Associate name] or the government.

**SANCTIONS:**

Class I offenses may include, but are not limited to:

1. Verbal reprimand.
2. Written reprimand in employee’s personnel file.
3. Retraining on HIPAA Awareness.
4. Retraining on [Insert Covered Entity or Business Associate name] Privacy Policy and how it impacts the said employee and said employee’s department.
5. Retraining on the proper use of internal forms and HIPAA required forms.
6. Termination of employment.

Class II offenses may include, but are not limited to:

1. Written reprimand in employee’s personnel file.
2. Retraining on HIPAA Awareness.
3. Retraining on [Insert Covered Entity or Business Associate name] Privacy Policy and how it impacts the said employee and said employee’s department.
4. Retraining on the proper use of internal forms and HIPAA required forms.
5. Suspension of employee [Insert suspension period here/In reference to suspension period: minimum of two (2) day/ maximum of three (3) days].
6. Termination of employment.

Class III offenses may include, but are not limited to:

1. Written reprimand in employee’s personnel file.
2. Retraining on HIPAA Awareness.
3. Retraining on [Insert Covered Entity or Business Associate name] Privacy Policy and how it impacts the said employee and said employee’s department.
4. Retraining on the proper use of internal forms and HIPAA required forms.
5. Suspension of employee [In reference to suspension period: minimum of two (2) day/ maximum of three (3) days].
6. Termination of employment.

Class IV offenses may include, but are not limited to:

1. Written reprimand in employee’s personnel file.
2. Retraining on HIPAA Awareness.
3. Retraining on [Insert Covered Entity or Business Associate name] Privacy Policy and how it impacts the said employee and said employee’s department.
4. Retraining on the proper use of internal forms and HIPAA required forms.
5. Suspension of employee [In reference to suspension period: minimum of two (2) day/ maximum of five (5) days].
6. Termination of employment.

Class V offenses may include, but are not limited to:

1. Termination of employment;
2. Civil penalties as provided under HIPAA or other applicable Federal/State/Local law; or,
3. Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law.

**PROCEDURE:**

1. Responsibility to Report
	1. Workforce members and Business Associates have a responsibility to report known HIPAA Violations.
	2. Reports may be made to one of the following:
		1. The Regional Privacy or Security Officer for HIPAA violations.
		2. The Institutional Privacy or Security Officer for HIPAA violations.
	3. Failure to report a known HIPAA Violation may result in disciplinary action in accordance with [Insert Covered Entity or Business Associate name] policies.
2. This Policy will be readily accessible to all employees.
3. All training regarding the Policy will be provided by the Privacy Officer.
4. Investigation
	1. Upon receipt of an allegation of a HIPAA Violation, the Institutional Privacy Officer (IPO) and/or Institutional Security Officer (ISO) or their designees, depending on the type of HIPAA Violation reported, shall conduct a confidential and timely investigation of the matter in accordance with [Insert Covered Entity or Business Associate name] policies. If necessary, advice may be sought from the legal department/risk management department at any point during the investigation.
	2. Based upon the circumstances revolving around the violation or breach, management or human resources will determine the specific disciplinary action taken for the employee.
5. Sanction Exemptions
	1. Sanctions will not apply to disclosures by employees who are whistleblowers or crime victims.
	2. [Insert Covered Entity or Business Associate name] is not considered to have violated PHI disclosure requirements if the disclosure is by an employee or business associate as follows:
	3. Disclosure by Whistleblowers:
		1. The employee is acting in good faith on the belief that [Insert Covered Entity or Business Associate name] has engaged in conduct that is unlawful or otherwise violates professional or clinical standards.
		2. That the care, services and conditions provided by [Insert Covered Entity or Business Associate name] potentially endangers one (or more) patients, employees or a member of the general public.
		3. The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered entity.
		4. The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by [Insert Covered Entity or Business Associate name].
		5. The disclosure is made to an attorney retained by or on behalf of the employee or business associate for the purpose of determining legal options regarding disclosure conduct.
	4. Disclosure by Crime Victims:
		1. A covered entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official about the suspected perpetrator of the criminal act, and the disclosed PHI is limited to identification and location purposes.
6. Mitigation
	1. Mitigating circumstances include conditions that would support reducing the sanction in the interest of fairness and objectivity. [Insert Covered Entity or Business Associate name] will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of PHI in violation of HIPAA regulations.
7. [Insert Covered Entity or Business Associate name] will not allow retaliatory action against a workforce member. There will be no intimidation, threatening, coercion, or discrimination against an individual who participates in the following activities:
	1. Files a complaint within the organization.
	2. Files a complaint with the secretary of Health and Human Services.
	3. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing.
	4. Opposes any act or practice unlawful under state and federal regulations, providing that the individual acted in good faith believing that the practice was unlawful, the manner of opposition was reasonable, and the individual's opposition did not involve disclosure of patient PHI in violation of regulation.
8. Audit and Reporting Process
	1. [Insert Covered Entity or Business Associate name] will continuously monitor sanctions to ensure consistent and equitable application across roles by violation category. Sanction data gathered for reporting purposes should include, but not be limited to, the following:
		1. Number of violations (by category) resulting in sanction.
		2. Severity of sanction by category.
		3. Severity of sanction by business unit and by role.
		4. Trended data over time (e.g., monthly, quarterly, yearly).
	2. The data will be reported to an interdisciplinary oversight committee to include at minimum the chief privacy official, chief security official, and senior personnel representing a broad array of departments such as compliance, labor, legal, IT, administration, medical staff, risk management, finance, and internal audit. The board of trustees or directors should also be included in the auditing and reporting process.
	3. The oversight committee will evaluate the data collected on disciplinary patterns to ensure comparable violations result in comparable sanctions for all roles within the organization and across all entities within a multisite health system.
	4. The data will also be used to identify gaps and opportunities for improvement to the organization's privacy and security programs. In addition, the data can be communicated to the workforce as a deterrent and used to justify sanctions at grievances and other labor hearings.

**DOCUMENTATION:**

The Privacy or Security Officer will maintain all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.