IT Sanction
HIPAA Policy: Security 25

Summary: Outlines disciplinary procedures for security breaches involving PHI

Affected Individuals: Employees in HIPAA covered entities; IT staff

Purpose of Policy

University of Mississippi's (UM) workforce members and third parties must comply with information security policies and procedures, federal regulations (e.g., HIPAA, HITECH), and state regulations (e.g., data breach notification laws, health codes).

The purpose of this policy is to ensure that violations of information security policies, procedures, regulations, and standards are addressed through a disciplinary process that includes sanctions.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Scope

This policy applies only to covered entities as defined in the University of Mississippi (UM) HIPAA hybrid policy.

This policy applies to all workforce members and all personnel affiliated with third parties regardless of physical location.

Policy

A. Sanctions Policy

1. UM ensures that information security policies, procedures, regulations, and standards are followed and that appropriate sanctions are taken against workforce members and third parties who violate them.

B. Disciplinary Process

1. UM develops and employs a formal disciplinary process for workforce members who fail to comply with policies, federal regulations (e.g., HIPAA, HITECH), and state regulations (e.g., data breach notification laws, health codes).

2. The formal disciplinary process commences after verification that a security incident has occurred.
3. The formal disciplinary process ensures correct and fair treatment for workforce members who are suspected of committing security incidents.
4. Potential sanctions resulting from the disciplinary process include but are not limited to:
   - Remedial training
   - Informal counseling
   - Formal counseling
   - Suspension or removal of access rights to the UM's information assets
   - Performance evaluation impacts and documentation
   - Suspension or rescinding of promotion
   - License, registration, or certification denial or revocation
   - Transfer from current job position
   - Termination of employment and/or relationship with UM.
5. UM appoints Human Resources to handle security incidents involving workforce members.
6. UM maintains a list of workforce members involved in security incidents including the outcome of the investigation.
7. In cases where civil or criminal charges are involved, the CISO works together with Human Resources and Legal Counsel to determine and take appropriate legal action.
8. Third parties that fail to comply are sanctioned according to the *Third Party Risk Management Policy*.
9. UM provides for disciplinary actions to be taken against UM employees who violate the provisions of the Compliance Plan. The following list of employee infractions and violations apply to the UM Compliance Program. These are supplemental to existing employee disciplinary guidelines.

IT Sanction
HIPAA Policy: Security 25

IT Sanction
HIPAA Policy: Security 25

Employee Action	**Disciplinary Action**
Employees willfully providing materially false information to UM, or a government agency, patient, insurer, or the like. Employees willfully disclosing Protected Health Information (PHI) to unauthorized individuals or entities. Employees intentionally misusing the Compliance Hotline or other reporting mechanism by knowingly and willfully providing false information to the Office of Integrity and Compliance or the Compliance Committee.	Disciplinary action shall be termination of employment.
Employees willfully viewing Protected Health Information for reasons other than treatment, payment, health care operations, approved Research or those required by law.	**First Offense:** Disciplinary Action shall range from 10 consecutive working days or 80 consecutive working hours without pay up to and including termination. **Second Offense:** Termination
Employees negligently providing incorrect information to UM, or a government agency, patient, insurer, or the like. Employees violating any relevant State or Federal Law, Rule, or Regulation.	Disciplinary Action shall range from counseling up to and including termination. Egregious situations may result in suspension pending termination.

Employees failing to report another employee's violations of duty pursuant to this Compliance Plan. Employees failing to detect and/or report conduct by an employee that a reasonable person should know is criminal and could reasonably be expected to be detected. Employees failing to take action as prescribed under this Compliance Plan or to comply with duties expressed or implied as set forth in this Compliance Plan. Employees engaging in any conduct prohibited by the terms of this Compliance Plan. Employees unintentionally or carelessly revealing patient information to oneself or others for reasons other than treatment, payment, health care operations, approved research or those required by law.	Subsequent or repeat violation shall result in a progressive application of disciplinary sanctions.

10. In the event that periodic audits reveal any noncompliant behavior or improper or mistaken billing incidents, all mistaken payments shall be returned to the appropriate payer(s) and a report shall be made to the appropriate subcommittee. Depending on the nature and severity of the conduct revealed through the audit procedure, the disciplinary action as

listed above may be instituted. Appropriate reports mandated by Federal or State law shall be made as required.

11. Certain factors as listed below may be considered as mitigation in any proposed disciplinary action: (a) whether the employee promptly reported his/her own violation, (b) whether the report constitutes UM's first awareness of the violation and the employee's involvement, and (c) whether the employee cooperated fully in investigating and/or correcting the violation.
12. Any employee disciplinary action resulting from a violation of this Compliance Plan should be coordinated through the Office of Integrity and Compliance and the Department of Human Resources. Any such disciplinary action must be reviewed by the Compliance Committee to determine if the Compliance Program needs to be revised.

Policy Compliance

Enforcement

The Chief Information Security Officer (CISO) has general responsibility for the implementation and enforcement of this policy.

Future Revisions

UM reserves the right to add, delete, or revise any provision of this Policy (approval by committee) at any time, or any other Information Security Policy without prior notice to users.

Sanctions

Any user violating these policies or applicable local, state, or federal laws while using UM’s computing environment is subject to loss of network privileges and any other disciplinary actions deemed

appropriate, up to and including termination and criminal and/or civil prosecution in accordance with policy..

Exceptions

Exceptions to this policy must follow the approved exception process as outlined in the *Information Security Waiver Policy*. All approved policy exceptions will be reviewed periodically for appropriateness by the CISO and may be revoked at any time with or without notice

Regulatory and Standards References

The following regulations and standards are applicable to this policy:

- **HIPAA Regulatory References**: HIPAA §164.308(a)(1)(ii)(C), HIPAA §164.414(a), HIPAA §164.530(e)
- **HITRUST Reference**: 02.f Disciplinary Process

Related Documents:

- Glossary
- Third Party Risk Management Policy

Approval

Chief Information Security Officer

<date>