



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 1 of 12

Effective Date: 041403
Board Motion No:

TITLE: SANCTIONS FOR FAILURE TO COMPLY WITH PRIVACY POLICIES

PURPOSE:

The purpose of this policy is to define the disciplinary actions for employees of the Harris County Hospital District (HCHD) who violate patient privacy rules.

This policy supports the Harris County Hospital District's HIPAA policy and may require development of department specific procedures.

[Key Words: Use, Disclosure, Authorization, Protected Health Information (PHI), Provider, Administrator, Workforce]

POLICY STATEMENT:

Harris County Hospital District is strongly committed to ensuring compliance with all applicable privacy laws, regulations, standards, policies, and procedures, including the Health Insurance Portability and Accountability Act of 1996. The Office of Privacy Administration and Harris County Hospital District's Management will thoroughly investigate any alleged patient privacy violation and take the appropriate disciplinary action regarding the employee, including reporting to Federal, state and local entities as appropriate.

POLICY ELABORATION:

I. DEFINITIONS

- A. Clear-Cut Violation – there is clearly no question of severity, intent and pattern of the violations.
- B. Protected Health Information (PHI) is individually identifiable patient health information in any form,



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 2 of 12

Effective Date: 041403
Board Motion No:

including demographic information, that is created or received by a healthcare provider, and relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare.

- C. HIPAA Response Team – is a multidisciplinary team established to respond to certain privacy or patient confidentiality violations and to evaluate and recommend sanctions.
- D. Privacy Officer – is a person designated by the Covered Entity to be responsible for the development and implementation of the privacy policies and procedures of the Covered Entity and responding to complaints of violations of HCHD's privacy policies and procedures.
- E. Office of Privacy Administration – responsible for the administration and compliance activities related to HCHD's privacy policies and procedures.
- F. HIPAA Security Officer (TBD) – is responsible for the management of HCHD's HIPAA IT Security Program.
- G. HIPAA Security Program – oversees HIPAA security issues.
- H. Levels of Violation – are the three levels determined according to the severity, intent and pattern or practice of the violation.



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 3 of 12

Effective Date: 041403
Board Motion No:

- I. Need to Know – is limiting access to PHI to only those with a legitimate business reason needed to perform their job.
- J. Non Clear Cut Violation – is any violation not covered by “Clear-Cut Violation” (I.A.)
- K. Patient Confidentiality – is protecting confidential patient information from use or disclosure to unauthorized individuals, entities or processes.
- L. Patient Privacy – is the patient’s right to determine whether, when and to whom their confidential information is released.
- M. Privacy Training – is mandatory privacy training required by the Office of Privacy Administration for HIPAA compliance. Additional training is required as part of the “Disciplinary Process.”
- N. Privacy or Patient Confidentiality Violations – applicable non-compliance with HCHD patient privacy and confidentiality policies and procedures.
- O. Security – shielding confidentiality.
- P. Whistleblower - is an individual who believes in good faith that the facility has acted unlawfully or violated professional or clinical standards, or that its care or services potentially endanger a patient, employee, or the public, and in that connection discloses PHI to a health oversight



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 4 of 12

Effective Date: 041403
Board Motion No:

agency, accrediting agency, appropriate public health authority, or to an attorney retained by the individual.

- Q. Workforce - means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

II. LEVELS OF VIOLATIONS

The level of the breach in patient confidentiality or privacy violation is determined according to the severity of the breach or violation, whether the breach or violation was intentional or unintentional, and whether the breach or violation indicates a pattern or practice of improper use or release of confidential patient information or violation of patient privacy. The degree of discipline may range from a verbal warning to immediate termination.

The three levels of breach or violation are as follows:

- A. Level 1—Carelessness or Inadvertent. This level of breach or violation occurs when a HCHD employee unintentionally or carelessly accesses, reviews, or reveals confidential patient information to himself/herself or others without a legitimate “need to know.” Examples include, but are not limited to:
1. employee discusses confidential patient information in a public area;
 2. employee leaves a medical record unattended in an accessible area;
 3. employee fails to log off a computer terminal or shares a password;



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 5 of 12

Effective Date: 041403
Board Motion No:

4. employee leaves a computer unattended in an accessible area with confidential patient information unsecured.
- B. Level 2—Curiosity or Concern (no personal gain). This level of breach or violation occurs when an employee intentionally accesses or discusses confidential patient information for purposes other than the care of the patient or other authorized purposes but for reasons unrelated to personal gain. Examples include but are not limited to:
1. employee looks up birth dates or addresses of friends or relatives;
 2. employee accesses and reviews a record of a patient out of concern or curiosity; employee reviews a public personality's record.
- C. Level 3—Personal Gain or Malice. This level of breach or violation occurs when an employee accesses, reviews, or discusses confidential patient information for personal gain or with malicious intent. Examples include but are not limited to:
1. employee reviews a patient record to use information in a personal relationship;
 2. employee gathers patient information to be sold.

III. INVESTIGATIVE PROCESS

The following process is followed when an employee breaches or is suspected of breaching patient confidentiality or violates or is suspected of violating patient privacy.

A. Initial Reporting



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 6 of 12

Effective Date: 041403
Board Motion No:

1. Individual who observes or is aware of a breach or violation reports it to his/her immediate supervisor and/or the HIPAA Privacy Officer, who shall notify the other as appropriate.
2. Failure to report a Level 2 or 3 breach or violation of which one has knowledge will result in a disciplinary action up to the disciplinary action accorded the violator.
3. There is no retaliation for a report made in good faith.

B. All Level 1 and/or Non Clear-Cut Level 2

For all Level 1 breaches or violations and/or non clear-cut Level 2 breaches or violations, the Supervisor or Department Director, in conjunction with Human Resources and the HIPAA Privacy Officer as appropriate, and the HIPAA Security Officer (when any security implications exist) will identify and implement an appropriate corrective action plan as required under this policy in a timely manner. The action plan shall be maintained in the Office of Privacy Administration, the employee department and Human Resources employee personnel file.

C. Clear-Cut Level 2 and/or All Level 3

1. For Clear-Cut Level 2 breaches or violations and/or all Level 3 breaches or violations, the HIPAA Privacy Officer will establish a investigating team called the "HIPAA Incident Response Team" and may contain representation as follows:



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 7 of 12

Effective Date: 041403
Board Motion No:

- (1) Employee's immediate Supervisor
 - (2) Administration
 - (3) Human Resources
 - (4) Corporate Compliance Officer
 - (5) Privacy Officer
 - (6) HIPAA Security Officer
 - (7) Other Representation
2. The HIPAA Incident Response Team shall conduct the necessary and appropriate investigation commensurate with the level of the breach and include specific facts, which may include, but not be limited to, interviewing the employee accused of the breach, interviewing other individuals, and reviewing documentation.
3. Upon conclusion of the investigation, the HIPAA Privacy Officer shall prepare a written corrective action report for the HIPAA Incident Response Team, including its findings, conclusions and recommendations with regard to the alleged breach. The report shall be communicated by the HIPAA Privacy Officer to the employee's Supervisor/ Department Director/Administrator who will determine the appropriate disciplinary action. The final decision regarding disciplinary action will be communicated to the employee and the HIPAA Privacy Officer.
- D. Repercussions for those who obstruct or retaliate against individuals participating in investigations or inquiries will be



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 8 of 12

Effective Date: 041403
Board Motion No:

applied as referenced in Policy 3.11.101, Privacy Officer, roles and Responsibilities.

IV. DISCIPLINARY ACTION

Disciplinary action shall be administered in a progressive manner as appropriate under Human Resources Policies and Procedures. Disciplinary action shall be reported to the applicable professional licensing board as appropriate.

The following steps are guidelines for disciplinary action for confidentiality breaches and privacy violations. Risks to patients or staff and other serious offenses may warrant deviation from these guidelines

A. All Level 1 and Non Clear-Cut Level 2

1. Depending on the facts, verbal warning, written warning, suspension, or termination documented in writing and maintained in the employee's file.
2. Except in the case of termination, the employee shall be required to repeat the Privacy Training in a timely fashion.

B. Clear-Cut Level 2

1. First offense: Depending upon the facts, verbal or written warning documented and maintained in the employee's file
2. Second offense: Depending upon the facts, a final written warning and suspension up to three days



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 9 of 12

Effective Date: 041403
Board Motion No:

without pay, documented and maintained in the employee's file, or termination

3. Third offense: Termination with report to the appropriate agencies.
4. Except in the case of termination, the employee shall be required to repeat the Privacy Training in a timely fashion.

- C. All Level 3
Termination with reports to the appropriate agencies.

V. DISCLOSURES NOT RESULTING IN SANCTIONS

- A. Disclosure by Whistleblowers: Any Disclosure of PHI by a Workforce member, acting as a Whistleblower, to a health oversight agency, appropriate public health authority, or the Workforce member's attorney will not subject the Workforce member to sanctions for violation of HCHD's privacy policies and procedures, provided the Workforce member in good faith believes that HCHD has acted unlawfully, violated professional or clinical standards, or potentially endangered a patient in providing care or service.
- B. Disclosure by Victims of Crime: A Workforce member will not be subject to sanctions for violation of HCHD's privacy policies and procedures if the Workforce member is a victim of a crime and Discloses to a law enforcement official the following PHI about the suspected offender:



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 10 of 12

Effective Date: 041403
Board Motion No:

1. Name and address;
 2. Date and place of birth;
 3. Social security number;
 4. ABO blood type and rh factor;
 5. Type of injury;
 6. Date and time of treatment;
 7. Date and time of death, if applicable; and
 8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- C. Other Disclosures: A Workforce member will not be subject to sanctions for violation of HCHD's privacy policies and procedures if the Workforce member:
1. Files a complaint with the Secretary of DHHS pursuant to the HIPAA Regulations;
 2. Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act; or
 3. Opposes any act or practice as unlawful under the HIPAA Regulations, if the Workforce member has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a Disclosure of PHI in violation of the HIPAA Regulations.

VI. APPEALS PROCESS

Refer to Human Resources Policies and Procedures for filing an appeal through the established grievance procedures.



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 11 of 12

Effective Date: 041403
Board Motion No:

VII. PRIVACY SANCTIONS LOG

- A. Each instance of employee disciplinary action regarding patient privacy and confidential patient information is to be documented and reported to the HIPAA Privacy Officer. The HIPAA Privacy Officer will notify the HIPAA Security Officer of any security implications.
- B. The HIPAA Privacy Officer shall maintain a Privacy Sanctions Log. Documentation is to include:
 - 1. Name of employee
 - 2. Level of breach or violation
 - 3. Location of breach or violation
 - 4. Date and time of breach or violation
 - 5. Disciplinary action provided

VIII. REVIEW

The HIPAA Privacy Officer is responsible for the management and content of this policy. This policy shall be reviewed and evaluated by the HIPAA Privacy Officer annually from its effective date.

IX. EXCEPTION

Any exceptions or deviations to this policy may only occur with the written authorization of the Chief Executive Officer or his designee.

X. CIVIL AND MONETARY PENALTIES

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides for Federal criminal penalties for violations for either



Harris County Hospital District

POLICY AND REGULATIONS MANUAL HIPAA ADMINISTRATIVE POLICY

Sanctions for Failure to
Comply with Privacy
Policies

Policy No: 3.11.104
Page Number: 12 of 12

Effective Date: 041403
Board Motion No:

the covered entity and/or the individual who committed the violation.
The current violation types and the respective penalties are listed below.

- A. Up to \$50,000 and one year in prison for obtaining or disclosing protected health information.
- B. Up to \$100,000 and five years in prison for obtaining protected health information under "false pretenses."
- C. Up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

REFERENCES/BIBLIOGRAPHY:

- Policy 3.11.000, HCHD HIPAA Policy
- Policy 3.11.101, Privacy Officer, Roles and Responsibilities

OFFICE OF PRIMARY RESPONSIBILITY:

Office of Privacy Administration.

REVISION HISTORY:

Record revisions below:

Effective Date	Version	Approved by: