Origination:	*04/2003*
Effective:	*11/2020*
Last Reviewed:	*11/2020*
Last Revised:	*11/2020*
Next Review:	*11/2022*
Sponsor:	*Brian Kozik: SVP, COMPLIANCE & PRIVACY*
Section:	*GA-Corporate Compliance*
Manuals:	*Compliance*

GA-004-160 Sanctions for Non-Compliance with Information Privacy and Security Policies

I. Purpose

To describe the sanctions that can be imposed against Broward Health workforce members that violate HIPAA Privacy/Security policies, procedures and state or federal laws or regulations.

II. Key Terms

Availability: Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Business Associate: a person or entity that is not a member of the workforce, who, on behalf of Broward Health creates, receives, maintains or transmits protected health information in the performance their contracted activity including claims processing or administration, data analysis, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, re-pricing; or who provides services including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where the provision of the service involves the disclosure of protected health information.

Confidentiality: Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Disclosure: Disclosure means the release, transfer, sharing, employment, application, utilization, examination, analysis, or provision of access to any individually identifiable Protected Health Information within an entity or to any of its outside parties.

Health Care Operations: Any activities of Broward Health that are related to the functions covered under HIPAA including, but not limited to: quality assessment and improvement activities, competency evaluations for medical staff, contracting for health insurance or health benefits, medical review, legal services, auditing functions, business planning and development, business management and administrative activities, resolution of internal grievances.

Integrity: Integrity means the property that data or information have not been altered or destroyed in an

unauthorized manner.

Payment: Activities undertaken by Broward Health or associated covered entity as (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (2) a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Privacy Incident: Any known or suspected violations of Broward Health privacy policies or any attempt to compromise patient privacy or confidentiality.

Protected Health Information (PHI): Individually identifiable health information that is either created, transmitted, received or maintained electronically or in any other form or medium.

Personally Identifiable Information (PII): Is any information about an individual maintained by Broward Health, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records' and any other information that is linked or linkable to an individual, such as medical, financial, and employment information.

Treatment: the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use: with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Security Incident: Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Workforce Member: Any employee, independent contractor, agent, volunteer, trainee, or other person who performs work for or on behalf of Broward Health. This includes full-time, part-time, and pool employees; associates; directors; officers; managers; supervisors; volunteers; members of the Board and members of standing committees; medical staff employed by or otherwise affiliated with Broward Health; medical students and all other affiliated students or others receiving training at any Broward Health facility; and others who provide goods or services to Broward Health.

III. Policy

Broward Health will take appropriate corrective action against any member of its workforce that violates privacy or information security, organizational policies related to applicable state, federal laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Final Omnibus Rule. Sanctions as a result of a violation of Privacy or Information Security Policies or procedures shall be imposed consistently across the organization.

All Workforce Members whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy will be subject to appropriate remedial and/or disciplinary action, up to and including termination of any employment or other relationship, in accordance with the Enforcement of Disciplinary Standards Policy, Policy No. GA-004-238 and any applicable Human Resources Policy.

IV. Procedures

All employees have an affirmative duty and responsibility for promptly reporting any known or suspected misconduct, including actual or potential violations of laws, regulations, policies or procedures. There are multiple ways for employees to report any known or suspected privacy and security incidents of non-compliance, including actual or potential violations of laws, regulations, policies or procedures, as indicated in policy GA-004-233, Disclosure Program. Any form of retaliation against any employee who reports a perceived problem or concern in good faith is strictly prohibited, in accordance with policy GA-004-305, Non-Retaliation Policy. If a workforce member violates any policy or procedure relating to information privacy and security, Broward Health has the right to implement corrective action procedures as defined by HR-003-010 Progressive Action (Corrective Action and Performance Improvement) Policy, and impose penalties/sanctions appropriate to the intent and severity of the violation. Additionally, workforce members may be subject to civil and criminal penalties for misappropriation of PHI/PII pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Final Omnibus Rule.

Types of Incidents

1. Information Privacy Incidents
2. Information Security Incidents

A. **LEVELS OF INCIDENT SEVERITY-** Violations of the privacy and information security policies and procedures will be classified as Accidental or Intentional. Corrective actions will be applied in accordance with Broward Health's policy HR-003-010 Progressive Action (Corrective Action and Performance Improvement) Policy.

i. **Level 1-Accidental:** This type of incident occurs when a Broward Health workforce member unintentionally or carelessly accesses, reviews, or reveals PHI/PII that he/she has no business need to know in order to carry out his/her job functions. Such accidental incidents will be reviewed on a case by case basis and may be subject to progressive discipline. Examples of accidental incidents are as follows:

a. Inadvertently transposing a medical record number and accessing the incorrect patient

b. Sending a fax or email to the incorrect recipient

ii. **Level 2 or 3 - Intentional**: This type of incident occurs when a workforce member intentionally accesses, reviews, discloses or discusses PHI/PII without authorization. Such intentional incidents are subject to termination. Examples of intentional incidents are as follows:

a. Posting PHI/PII to social media or other internet sites

b. Unauthorized changes to business or health records.

c. Accessing information that you do not have a business need to know to execute your job duties

d. Accessing your own medical record or billing information

e. Sharing PHI/PII with another employee without appropriate authorization

B. **REMEDIATION PROCESS**- The steps outlined below may be followed when a Workforce Member violates, or is suspected of violating Broward Health privacy or information security policies and procedures:

i. **Initial Reporting** – According to Broward Health policy GA-004-095 Reporting of Privacy and Security Incidents, members of Broward Health's workforce have the individual responsibility to report all known or suspected information privacy and security incidents. Failure to report an incident of which one has knowledge will result in appropriate disciplinary action. Reporting of an incident in bad faith or for malicious reasons will also result in appropriate disciplinary action.

ii. **Investigation** – After an incident is reported, proper measures shall be followed to verify that the incident occurred.

iii. **Documentation and Reporting** – After incidents are investigated by the Corporate Compliance & Ethics Department, it may be necessary to document any action taken to remediate the matter. The Corporate Compliance & Ethics Department will require that the Workforce Member's immediate supervisor or manager consult with the appropriate Regional Chief Human Resource Officer or designee to determine the level and severity of the remediation or corrective action. For incidents of greater severity, consultation with the Chief Compliance/Privacy Officer, or designee, to determine the level and appropriateness of the remediation or corrective action may be necessary. The Human Resources Department, along with the Workforce Member's immediate supervisor or manager, will keep the appropriate documentation, according to Broward Health records retention schedules, and provide written notification to the Corporate Compliance & Ethics Department of the remediation or corrective action.

Remediation or corrective action must comply with applicable federal and state laws and regulations, Broward Health policies, Medical Staff By-Laws, and any other applicable documents or agreements related to the Workforce Members' status as employee, medical student, medical resident, student or volunteer.

The Secretary of the Department of Health and Human Services, state licensure agencies, or Florida State Attorney General may investigate complaints and may seek criminal prosecution or impose civil monetary penalties to Broward Health and/ or individual workforce members.

iv. **Other Workforce Members (Non-Employees)** — If a Workforce Member, who is not an employee (e.g., a student or volunteer), violates any information privacy and security policy or procedure, the Chief Compliance/Privacy Officer or designee will work with the responsible administrator or manager to establish appropriate corrective actions.

V. **Related Policies and Compliance Documents**

- Business Associate Agreements, Policy No. GA-004-015

- Information Access Management, Policy No. GA-003-138
- Minimum Necessary Uses, Disclosures, and Requests, Policy No. GA-004-100
- Reporting of Information Privacy and Security Incidents, Policy No. GA-004-150
- Information Security Management, Policy No. GA-003-139
- Progressive Action Policy (Corrective Action and Performance Improvement Plan) – HR-003-010
- Non-Retaliation and Retribution, Policy No. GA-004-305

VI. **Regulation/Standards**

- 45 CFR 164.308

VII. **References**

U.S. Department of Health and Human Services – Health Information Privacy https://www.hhs.gov/hipaa/for-professionals

Attachments

GA-004-160 Exhibit 1.docx

Approval Signatures

Step Description	Approver	Date
Final Approver	Brian Kozik: SVP, COMPLIANCE & PRIVACY	11/2020
	Lucia Pizano-Urbina: AVP, COMPLIANCE	11/2020