

Title: HIPAA Compliance and Responsibility for Information Privacy and Security	No.: IM 4.39 Replaces 4.15, 4.16, 4.18, 4.20
	Effective: 04/2003
	Revised: 05/11 Reviewed:05/11
Approved By: Beth Fleming, Chief Compliance Officer, Tanya Kuehnast, Director HIM/Chief Privacy Officer Christi Rushnell, VP Information Technology /CISO	Page 1 of 3

Applies to Entity: Health First, Inc

I. OBJECTIVE

To provide guidelines for the establishment of internal responsibility for the oversight of privacy and security issues, provide direction for Health First workforce team members in addressing patient privacy and information security issues, and establish an on-going evaluation process in order to certify compliance with Health First privacy and security policies and regulations required by other organizations including federal and state government agencies.

II. DEFINITION

Protected health information (PHI), also individually identifiable information, as used in the Health First Information Privacy policies, is defined as a subset (record or transmission) of health information, including demographic information, collected from an individual. It is created or received by a health care provider (including Health First), health plan, employer, or health care clearinghouse. It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. In addition, the information identifies the individual; or can be used to identify the individual.

Workforce (for use in this policy) is defined as associates, contract employees, physicians, volunteers, students, board members and any other temporary worker who have access to PHI generated by any Health First entity.

III. POLICY

- A. It is the role of the Health First workforce to maintain the confidentiality and security of PHI in order to ensure the patient’s right to privacy.
- B. Health First will establish and maintain a formal Compliance Program and management structure responsible for monitoring and maintaining privacy, security and confidentiality standards throughout the organization.
- C. The Corporate Compliance Committee shall play an active role in recommending, monitoring and developing internal systems and controls to ensure adherence to organizational standards, policies and procedures, including acting as the oversight Committee for privacy and security standards of the Health Information Portability

- and Accountability Act (HIPAA), Joint Commission (JC) and Health Information Technology for Economic and Clinical Health Act (HITECH). The Chief Compliance Officer, Chief Privacy Officer and Chief Information Security Officer will participate in the Corporate Compliance Committee as key members. In this way, the organization will have a formal point of contact responsible for the management of privacy and security issues.
- D. The Health Information Management (HIM) Department plays an integral part in the management of privacy and security matters because of their responsibility to keep and maintain all patient medical information.
 - E. The Health First Health Information Technology Department will review, annually, its operational policies and practices, and evaluate computer systems and network design to certify that the appropriate security has been implemented. This evaluation will be done internally by the Information Technology Security Office whenever possible. If needed, the department will use an external consulting company to augment the internal process.
 - F. Health First has implemented policies and procedures, with respect to PHI, designed to comply with the provisions of all federal, state and voluntary accrediting bodies for the protection of individually identifiable health information.
 - G. Health First reserves the right to revise its policies and procedures. When changes are made, Health First will promptly notify and educate Health First associates and other workforce members on these changes. Workforce members are responsible for understanding and complying with these policies and procedures.
 - H. Violations of these policies and procedures will not be tolerated. Depending on the role of the workforce member, appropriate actions will be taken according to Information Management policy and procedure, IM 5.01 "Inappropriate Access Investigations". Associates who violate privacy policies will be subject to disciplinary action based upon Human Resources policy and procedure, HR 4.01 "Positive Discipline/Corrective Action Guide". Contractors who violate privacy policies will be in violation of contract specifications and will be acted on in accordance to specific contract language. Medical Staff members who violate privacy policies will be subject to disciplinary action according to the Medical Staff By-Laws of the Health First facilities and Information Management policy and procedure, IM 5.18 "Practitioner System Access Policy".

IV. PROCEDURE

The Chief Compliance Officer, Chief Privacy Officer and Chief Information Security Officer will:

- A. Guide the development of information privacy & security objectives and policies.
- B. Develop implementation plans and budgets to support objectives and policies.
- C. Guide the implementation of information privacy & security objectives and policies.
- D. Determine the methodology and procedures for accomplishing the goals of the information privacy and security functions.
- E. Manage privacy and security incidents.
- F. Conduct on-going privacy and security monitoring processes.
- G. Assist with personnel and administrative functions such as hiring, termination, and training as these functions pertain to privacy and security.

- H. Research and understand privacy and security related regulatory requirements to include HIPAA, HITECH, State privacy regulations, as well as applicable Joint Commission standards.
- I. Research and understand security-related technologies.
- J. Monitor and document bugs, viruses, software patches and service pack upgrades associated with correcting system security flaws.
- K. Inform senior management and the Corporate Compliance Committee on information privacy and security issues, and make recommendations.
- L. Execute the directives of senior management and the Corporate Compliance Committee related to security and confidentiality of patient information.
- M. Maintain information privacy and security policies and procedures in electronic form to be viewable by the entire organization via the Health First Intranet.
- N. Retain all policies and procedures according to Information Management policy and procedure, IM 2.09 “Records Management” (see IM 2.09 attachment, “Record Retention Schedule”).
- O. Adhere to Administration policy and procedure, AD 1.02 “Health First Policy and Procedure Life Cycle” when creating Information privacy and security policies and procedures.
- P. Review applicable information privacy and security policies and procedures on an annual basis.

V. REFERENCES

Health Insurance Portability and Accountability Act of 1996

45 C.F.R. Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule; August 14, 2002.

45 C.F.R. Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule; February 20, 2003.

45 C.F.R. Parts 160 and 164, HITECH Breach Notification Interim Final Rule, August 19, 2009.

Federal Register/Vol. 65, No. 250/Thursday December 28, 2000/Rules and Regulations/

The Joint Commission Information Management, Privacy and Security Standards IM.02.01.01 EP1-5, IM.02.01.03 EP 1-8., 2009

HIPAA Compliance Program Organizational Structure (access via Inside Health First <http://intranet.health-first.org/departments/hipaa/orgchart/index.cfm>)

Developed: January 2003

Reviewed: 5/2004, 3/2005, 3/2006, 5/2007, 9/2008

Revised: 5/2007, 4/2010, 5/2011

Owner: Health First Health Information Management