Sample Information Security Program

Information Security Program

XYZ Hospital **Effective Date**

.....

1. Policy

Information is a corporate asset and must be protected as any other asset; therefore, information shall be protected with a formal security program. Security of information shall be addressed through the development, implementation, and administration of policies, procedures, technical controls, and education.

All external rules and regulations, as well as internal policies and procedures governing the access to and use of information, must be honored.

2. Rationale and Objectives

Information security is defined as the availability, the integrity, and the confidentiality of information. Availability of information assures the information is accessible by authorized users whenever needed. Disaster recovery and business continuity plans are examples of ways to assure availability. Integrity of information refers to the protection of data from intentional or accidental unauthorized changes. Confidentiality is the protection of information so that unauthorized persons cannot access it. Physical and electronic access controls, such as user authentication and authorization mechanisms, are examples of ways to assure integrity and confidentiality.

Information security program objectives include preventing the misuse, loss, or unauthorized disclosure of clinical or business information; establishing individual security responsibilities for the generation, handling, servicing, and use of XYZ information; and establishing a basis for auditing and compliance.

All information relating to our patients, employees, staff, and business demands stringent safeguards. Protection of privacy is of utmost importance. Every individual shall be accountable for maintaining security and confidentiality of XYZ Hospital information acquired during a work relationship with XYZ Hospital.

3. Scope

This policy applies to XYZ Hospital information in any form including spoken, written, or electronic, and about patients, employees, medical staff, research, and business affairs.

This policy applies to all XYZ Hospital employees, professional staff, volunteers, students, interns, and persons providing professional services to any XYZ Hospital entity or affiliate hereinafter referred to as XYZ Hospital.

This policy assures the implementation and maintenance of a security program for the protection of information systems hardware, software, and data; the development and implementation of policies and procedures; the monitoring and evaluation of data security in order to reduce risks to corporate computing resources; and the investigation of security exposures and breaches. This policy assures the development and implementation of a corporate-wide security education and awareness program for delivery to all levels of the company, including new employee orientation.

4. Procedures

N/A

5. Related Information

See also Information Security: Confidentiality Policy.

See also Information Security: Access Policy.

6. Sponsor

XYZ Hospital Information Systems
Information Security Department
(123) 555-1234

7. Review Cycle

Annual

8. Effective Date

Source: Ballam, Holly. "HIPAA, Security, and Electronic Signature: A Closer Look." *Journal of AHIMA* 70, no. 2 (1999): 28.
