

	Johns Hopkins [insert provider or plan name]	Policy Number	C.1
	PROVIDERS and HEALTH PLANS	Effective Date	04/20/05
		Page	1
	GENERAL POLICY ON SECURITY REGULATIONS	Supercedes	

HIPAA Security Regulations require covered entities to protect the security of patient and plan member information. Information security related to HIPAA is addressed in four policies:

1. *General Policy on Security Regulations (HIPAA Policy C.1)*
2. *Administrative Security Policies (HIPAA Policy C.2)*
3. *Physical Security Policies (HIPAA Policy C.3)*
4. *Technical Security Policies (HIPAA Policy C.4)*

In addition to the above security policies, protection of E-PHI also is subject to all applicable privacy, information technology and other policies.

DEFINITIONS

E-PHI means PHI which is (1) transmitted by electronic media or (2) maintained in electronic media.

E-PHI System(s) means systems owned by and/or administered within Johns Hopkins and all applications and data contained on those systems that process, store or transmit E-PHI, and principally includes servers, database applications, networks, e-mail systems, and Web applications. Workstations and other devices used to access E-PHI and supporting software (e.g. operating systems, Web servers, etc.) are considered components of E-PHI Systems. A workstation or other device that stores substantial amounts of E-PHI in any form – including as a spreadsheet, word processing document, or e-mail client – generally is deemed to be an E-PHI System and subject to all Johns Hopkins HIPAA Policies.

HIPAA means the Health Insurance Portability and Accountability Act of 1996.

Johns Hopkins means the Johns Hopkins covered entity that adopted this policy.

PHI means protected health information, i.e., individually identifiable health information.

Responsible Administrator means the senior manager for a Responsible Site who has responsibility for overseeing E-PHI and E-PHI Systems and for assuring compliance with HIPAA security policies and HIPAA privacy policies for such Site (working with other Responsible Administrators where appropriate).

Responsible Site means those entities or functional areas that have been charged with the administrative oversight responsibilities for compliance with the HIPAA Privacy and Security Regulations. [Click here for a listing of Responsible Sites.](#)

Security Regulations means the regulations promulgated by the Secretary of the Department of Health and Human Services to implement portions of HIPAA that concerns the security of electronically transmitted or maintained health information, as amended from time to time; these regulations currently include 45 CFR §§ 160 and 164, subparts A and C.

Workforce members, for purposes of this policy only, are persons under the direct or indirect control of Johns Hopkins, including, but not limited to, employees, students, interns, residents, fellows, researchers, staff, faculty, volunteers and temporary personnel.

POLICY

It is the policy of Johns Hopkins to protect and maintain the confidentiality, integrity and availability of electronically transmitted and maintained patient information, health plan member information, medical records, research information and business operations; and to comply with all applicable laws and regulations, including the Security Regulations under HIPAA.

Johns Hopkins will take steps:

- (i) to ensure the confidentiality, integrity and availability of all E-PHI that it creates, receives, maintains or transmits;
- (ii) to protect against any reasonably anticipated threats or hazards to the security or integrity of E-PHI;
- (iii) to protect against any reasonably anticipated uses or disclosures of E-PHI that are not permitted or required under the Johns Hopkins policies related to privacy of PHI; and
- (iv) to ensure compliance with the Johns Hopkins security policies by its workforce members.

The Responsible Site shall integrate E-PHI security compliance with privacy compliance.

The HIPAA security policies are in addition to all other Johns Hopkins Information Technology policies and privacy policies for all electronically held information and for information systems and devices that transmit or store E-PHI.

REQUIREMENTS

1. Each Responsible Site shall identify to the Chief Information Security Officer and the HIPAA Office a Responsible Administrator and a senior IT person to be responsible for implementing and overseeing the Johns Hopkins HIPAA security policies for that Site. The Responsible Administrator and the senior IT person must be two different individuals.
2. Compliance with the Johns Hopkins HIPAA security policies shall be overseen by the Johns Hopkins Chief Information Security Officer with the assistance of the Johns Hopkins Privacy Officer as appropriate. The Johns Hopkins Chief Information Security Officer, in coordination with the Johns Hopkins HIPAA Office, shall be responsible for strategies and policies for complying with the Security Regulations.
3. Each Responsible Site shall implement each Johns Hopkins security policy for each of its E-PHI records and E-PHI Systems. (Implementation of such policies, standards and requirements shall serve as the vehicle for each Responsible Site to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Regulations.)
 - a. Compliance for each set of E-PHI records and/or E-PHI System must be documented in one or more Security Compliance Workbooks to be maintained by each Responsible Site. Each set of E-PHI records and each E-PHI System must be tied to a specific workbook.

- b. If compliance with a particular policy or requirement (or portion of a policy or requirement) is impracticable, such impracticability shall be documented and compensating controls shall be specified and implemented. For purposes of this policy, "impracticability" means not reasonably capable of being done or carried out based on consideration of all of the following factors: the risk involved; what risk mitigation and security measures are, or readily can be, put in place; operational realities; and costs (in both financial and human resource terms). If compliance is impracticable, a plan and time line must be specified to achieve compliance.
4. E-PHI Systems that process, store or transmit E-PHI shall be designed to collect and maintain the minimum amount of PHI necessary to ensure operational effectiveness.
 5. The Johns Hopkins Chief Information Security Officer, together with other Johns Hopkins Information Technology support services, shall publish periodic security up-dates and reminders through various methods to reach the broadest Johns Hopkins workforce member audience, including system-wide e-mail messages and broadcast announcements.
 6. In the event that a Responsible Site involves a non-Johns Hopkins third party in any aspect of its use or maintenance of E-PHI or E-PHI Systems, or its activities to comply with the Security Policies or the Security Regulations, the Responsible Site shall consider whether a Business Associate Agreement with such third party is required. See HIPAA Policy Template A.9.1.
 7. All plans, reports, evaluations and other documentation of risk management and compliance strategy shall be retained in conformity with the HIPAA Privacy Policy A.8.9-Retention and Destruction.

[References: HIPAA Regs.--Section 164.306
164.308(a)(1)(ii)(B)
164.308(a)(5)(ii)(A)]