


|   |  |                |          |
|---|--|----------------|----------|
|  | Johns Hopkins [insert provider or plan name] | Policy Number  | C.3      |
|   | <b>PROVIDERS and HEALTH PLANS</b>            | Effective Date | 04/20/05 |
|   |  | Page           | 1        |
|   | <b>PHYSICAL SECURITY POLICIES</b>            | 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** means a system owned by and/or administered within Johns Hopkins and all applications and data contained on such system that process, store or transmit E-PHI, and principally include servers, database applications, networks, e-mail systems and Web applications. Workstations, other devices and supporting software (e.g. operating systems, Web servers, etc.) used to access E-PHI 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 Security 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 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.

**Vendor** means a vendor, consultant, contractor or other non-Johns Hopkins third party who may have access to E-PHI or an E-PHI System for any reason or purpose (other than those who may have incidental access) or the Johns Hopkins facilities housing the information technology assets that support E-PHI or E-PHI Systems or related infrastructure.

**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.

#### **A. POLICY - FACILITY ACCESS CONTROLS**

Physical access to E-PHI Systems and the facility or facilities in which they are located shall be limited to authorized access only. Johns Hopkins shall protect information assets from unauthorized physical access, theft, loss or environmental hazards by using an appropriate balance of documented technologies and practices.

#### **REQUIREMENTS**

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document access controls to facilities housing information technology assets that are part of its E-PHI Systems and/or supporting infrastructure. In many cases, physical access is controlled by an entity different than the Responsible Site. In such cases, it is the responsibility of the Responsible Site to verify that appropriate security controls are implemented and documented, especially those related to high risk facilities (e.g. data centers, computer labs, file servers, network closets, etc.). Responsible Sites periodically shall review facility security controls and adjust according to changing risk environments. Facility controls shall include, without limitation, the following:

##### *Facility Access Authorization*

1. Regular review of authorization for facility access of workforce members and vendors, ensuring that facility access is limited to only those with a business need for physical, rather than electronic, access to facilities and equipment. Authorization procedures shall, without limitation, address change in work or contractual status.
2. Vendors may be authorized to access high risk physical facilities. All physical access to facilities by vendors shall be logged (i.e. through sign-in sheets) for entry, exit and purpose and it is recommended that vendors are escorted by workforce members.
3. Procedures for providing facility access in support of restoration of lost data under disaster recovery plans in the event of a contingency.
4. Procedures that ensure emergency access, in the event of a contingency or otherwise, when a custodian of the physical site is unavailable.

##### *Facility Security Controls*

5. Standards for protection of facilities from unauthorized physical access, tampering and theft are based in part on the kind of equipment located in a facility. Physical security controls shall include, without limitation, the following:
  - a. Mainframe computer systems and data centers must be located in an access-controlled area. Appropriate physical controls include some combination of (i) guards, (ii) multi-factor authentication (e.g. token and pin number), (iii) complete access logging via card key, and (iv) video monitoring.
  - b. File servers containing E-PHI or other sensitive information must be installed in a secure area to prevent theft, destruction or unauthorized access. Appropriate physical controls include door keys (with restricted distribution) or any combination of the controls in the previous paragraph.
  - c. Network wiring closets, computer labs and other concentrated aggregations of devices with access to E-PHI must be secured from unauthorized access. Appropriate physical controls include door keys (with restricted distribution) or one or more of the controls mentioned in requirement 5.a. above.

6. Reasonable efforts must be made to ensure that areas or equipment accessed by third-parties are physically separated from other E-PHI Systems through appropriate design or tools (e.g. cages, cabinets, rooms, etc.).
7. Environmental controls shall be appropriate for E-PHI Systems in the facility. For mainframe computer systems, areas in and around the computer facility must have protections against fire, water damage, and other environmental hazards, such as power outages and extremes in temperature.

[References: HIPAA Regs.--Section 164.310(a)]

## **B. POLICY - WORKSTATION USE AND SECURITY**

Workstations and devices with access to E-PHI shall be administered consistent with their business purposes and with appropriate physical and electronic security controls.

### **REQUIREMENTS**

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures for specifying business purposes, physical surroundings and appropriate security controls for workstations and devices.

1. For workstations and other personal computing devices (e.g. laptops, PDA's, etc.) accessing or storing E-PHI there shall be:
  - a. a process for maintaining a current inventory
  - b. appropriate controls for the secure access of E-PHI
  - c. appropriate positioning to minimize unauthorized viewing of E-PHI, i.e., not located in public walkways, hallways, waiting areas, etc. In the event that unauthorized viewing of E-PHI cannot be minimized by positioning of the workstation, it shall be secured with a screen filter.
2. Refer to Section D, Technical Security Policies (HIPAA Policy C.4) for further requirements regarding workstation and device security.

[References: HIPAA Regs.--Section 164.310(b) and (c)]

## **C. POLICY - DEVICE AND MEDIA CONTROLS**

Johns Hopkins shall control the receipt, maintenance, and removal of hardware and electronic media containing E-PHI, and the movement of such items within the facility. Back-up and disposal procedures for E-PHI and E-PHI Systems must be documented by Responsible Sites.

### **REQUIREMENTS**

Subject to the General Policy on Security Regulations (HIPAA Policy C.1), each Responsible Site shall document procedures for device and media security controls including, without limitation, the following:

#### *Accountability – Inventory, Movement and Maintenance*

1. Responsible Sites shall document procedures for movement and maintenance of equipment related to E-PHI Systems. Such procedures must address, without limitation, the following:

- a. an inventory of hardware and electronic media
- b. records supporting the movement of hardware and electronic media into and out of the facility
- c. records of those individuals who moved the hardware and electronic media
- d. records relating to equipment repairs and maintenance of hardware and electronic media
- e. records of those individuals who performed the repair or maintenance on the hardware and electronic media

*Back-up*

- 2. For purposes of accountability, data integrity, business continuity and audit, among others, Responsible Sites shall document procedures to create a retrievable, exact copy of E-PHI and appropriate information regarding system configurations.
  - a. E-PHI shall be regularly backed-up on durable media using documented handling procedures that should include a provision for off-site storage.
  - b. E-PHI stored on an external medium shall be protected from theft and unauthorized access.
  - c. E-PHI stored on an external medium shall be labeled appropriately as sensitive and confidential, and the label must include the creation date.
  - d. Disposal and re-use processes shall be followed as stated in this policy.

*Disposal*

- 3. Disposal of E-PHI must include the following:
  - a. final disposition of E-PHI and/or hardware or electronic media on which it is stored
  - b. removal of E-PHI from electronic media before the media are made available for re-use
  - c. assigning responsibility for removing E-PHI and logging removal.
- 4. Disposal or re-use of media storing E-PHI shall be rendered unreadable by one of the following:
  - a. shredding hard copies,
  - b. cleaning media through degaussing or other reliable techniques; and/or
  - c. defacing CDs.

[References: HIPAA Regs.--Section 164.310 (a) and (d)]

**D. POLICY -- RECORD, RETENTION AND DESTRUCTION**

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.