Brooklyn Community Services

Policies and Compliance Guide

relating to the

HIPAA Security Rule

June 2013

Table of Contents

Introduction

Scope The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule contains standards and implementation specifications for administrative, technical, and physical safeguards for electronic protected health information (PHI) held in any electronic device by a HIPAA covered entity. Implementation of policies and procedures to support the standards and specifications is required.

Source The HIPAA Security Rule is 45 CFR Parts 160, 162, and 164, *Health Insurance reform: Security Standards; Final Rule*, February 20, 2003, which may be downloaded as a PDF formatted file over the Internet at the Web address http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf .

Every Agency Is Unique One of the foundations of the HIPAA Security Rule is that each agency under the rule is different and will need to respond to the details of the rule differently, according to its own background and capabilities. BCS is committed to complying with the rule and developing the procedures necessary to support its security policies, based on its own business processes and characteristics.

Required and Addressable Implementation Specifications Of the implementation specifications, some are Required and some are Addressable. The Required items must be met as specified, while agencies can decide how best to meet Addressable items, based on their own context. If an Addressable item is not implemented as stated in the rule, BCS will perform the analysis and documentation necessary to justify its actions.

Risk Assessment Central to the analysis required by the Security Rule is risk assessment of information security. Decisions about what should be done to be in compliance with the HIPAA Security Rule will be supported by an assessment of the information security risks that exist at BCS. The process identified in the preamble to the HIPAA Security Rule is described by the National Institute of Standards and Technologies in their document *Risk Management Guide for Information Technology Systems* (NIST SP800-30, available at http://csrc.nist.gov/publications/nistpubs).

Flexibility As required in the flexibility provisions in Security Rule §164.306(b), BCS will take measures to manage security by considering not only risk assessment, but

also the costs of various measures, the size of the agency, and the hardware and software security capabilities.

Culture The establishment of a culture of privacy and security supported by policies and procedures is an essential step in creating a successful security program. BCS is committed to having sufficient policies and procedures in place to support a culture of privacy and security, and the workforce that works within the BCS culture.

Security Management Process The first action item listed in the Security Rule's safeguards is to establish a Security Management Process that includes risk analysis and a regular periodic assessment of security (among other requirements). Security is not a one-time event – it is a process that requires maintenance and attention for success. The policies included here will also need to be revisited on a regular basis to ensure that they meet the needs of the agency and provide the necessary protection of health information security in an environment where new threats are discovered on nearly a daily basis.

Safeguards Administrative safeguards in the Security Rule include a security management process, workforce security policies and procedures, information access management policies and procedures, training and awareness requirements, security incident procedures, contingency and disaster plans, periodic evaluation requirements, and Business Associate contract requirements. Physical safeguards include physical access controls, workstation use and security policies and procedures, and device and media (i.e., disks, tapes, etc.) controls. Technical safeguards include access controls, audit controls and mechanisms, data integrity controls, entity authentication, and transmission security. In addition, there are sections for organizational and documentation requirements.

Electronic and Non-Electronic Information While the Security Rule applies only to information that is held electronically, the rule's concepts should be used to support information security for non-electronic information wherever possible as well, since the principles involved are sound and should be considered for all kinds of protected health information.

Justification and Documentation BCS is committed to the process of thorough analysis, justification, and documentation required for compliance with the HIPAA Security Rule. Any actions taken by BCS relating to information security will be properly justified through analysis and fully documented.

This Document

This document provides a reference tool, in the compliance guide in the section following, to show how BCS meets its obligations under the HIPAA Security Regulation, by listing the requirements in the regulation and identifying which policies support those requirements.

The sections following the guide detail the policies themselves. A glossary is included, followed by sample forms for establishing and terminating access to computer systems.

Guide to BCS Compliance with the HIPAA Security Regulation

This guide is intended to assist with compliance with the Health Insurance Portability and Accountability Act Security regulation by identifying the policies and documents that ensure compliance with HIPAA Security standards. Compliance with the HIPAA Security regulation is required as of April 20, 2005.

This guide is organized using the HIPAA Security Standards Final Rule as a template. The final rule is organized by General Rules, Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Polices & Procedures and Documentation Requirements. Each section describes the HIPAA requirement as stated in the Federal Register Final Rule and describes how BCS is meeting this requirement, by the inclusion of Compliance Statements and References to policies. In addition the reference to the Federal Register section is provided and each requirement is identified as Required (R) or Addressable (A).

I. General Rules

I. **General Rules** - §164.306

(a) *General requirements*

Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information [PHI] the covered entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

References: All HIPAA Security Policies

(b) *Flexibility of approach*

(1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic PHI.

(c) *Standards*

A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications*

In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word ''Required'' appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word ''Addressable'' appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications.
(3) [printing typo in Federal Register: (1)] When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must—
(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and
(ii) As applicable to the entity—
(A) Implement the implementation specification if reasonable and appropriate; or
(B) If implementing the implementation specification is not reasonable and appropriate—
(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance*
Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.
References: Policy 2.4 and Policy 2.6

II. Administrative Safeguards

II. **<u>Administrative Safeguards</u>** - § 164.308
(a) A covered entity must, in accordance with § 164.306:
(1)
(i) *Standard*: *Security Management Process* - § 164.308(a)(1)
Implement policies and procedures to prevent, detect, contain, and correct security violations.
Reference: Policy 2
(ii) Implementation Specifications
(A) Risk Analysis (R)
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
Reference: Policy 2.2
(B) Risk Management (R)
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
Reference: Policy 2.2
(C) Sanction Policy (R)
Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
Reference: BCS Personnel Policies and Practices Manual
(D) Information System Activity Review (R)
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Reference: Policy 2.4

(2) *Standard: Assigned Security Responsibility* – 164.308(a)(2)
Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Reference: Policy 2.1

(3)

(i) *Standard: Workforce Security* – § 164.308(a)(3)
Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.
References: Policy 1 and Policy 3

(ii) Implementation Specifications

(A) Authorization and/or Supervision (A)
Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
Reference: Policy 1.1

(B) Workforce Clearance Procedure (A)
Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
References: Policy 1.1 and Policy 3.1

(C) Termination Procedures (A)
Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
Reference: Policy 3.2

(4)

(i) *Standard: Information Access Management* – § 164.308(a)(4)
Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule].
Reference: Policy 3

(ii) Implementation Specifications

(A) Isolating Health Care Clearinghouse Function (R)
If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
Compliance Statement: BCS does not engage in Clearinghouse operations. This section does not apply to BCS.

(B) Access Authorization (A)
Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
Reference: Policy 3.1

(C) Access Establishment and Modification (A)
Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
Reference: Policy 3.1

(5)

(i) *Standard: Security Awareness and Training* – § 164.308(a)(5)
Implement a security awareness and training program for all members of its workforce (including management).
Reference: Policy 1.2

(ii) Implementation Specifications

(A) Security Reminders (A)
Periodic security updates.
Reference: Policy 1.2

(B) Protection from Malicious Software (A)
Procedures for guarding against, detecting, and reporting malicious software.
Reference: Policy 1.2

(C) Log-in Monitoring (A)
Procedures for monitoring log-in attempts and reporting discrepancies.
Reference: Policy 1.2

(D) Password Management (A)
Procedures for creating, changing, and safeguarding passwords.
Reference: Policy 1.2

(6)

(i) *Standard: Security Incident Procedures* – § 164.308(a)(6)
Implement policies and procedures to address security incidents.
Reference: Policy 2.3

(ii) *Implementation Specification*: Response and Reporting (R)
Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
Reference: Policy 2.3

(7)

(i) *Standard: Contingency Plan* – § 164.308(a)(7)
Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
Reference: Policy 4

(ii) Implementation Specifications

(A) Data Backup Plan (R)
Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
Reference: Policy 4.1

(B) Disaster Recovery Plan (R)
Establish (and implement as needed) procedures to restore any loss of data.
Reference: Policy 4.2

(C) Emergency Mode Operation Plan (R)
Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
Reference: Policy 4.2

(D) Testing and Revision Procedure (A)
Implement procedures for periodic testing and revision of contingency plans.
Reference: Policy 4.2

(E) Applications and Data Criticality Analysis (A)
Assess the relative criticality of specific applications and data in support of other contingency plan components.
Reference: Policy 4.2

(8)

(i) *Standard: Evaluation* – § 164.308(a)(8)
Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
Reference: Policy 2.6

(b)

(1) *Standard: Business Associate Contracts and Other Arrangements* – § 164.308(b)(1)
A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.
Reference: Policy 3.9

(2) This standard does not apply with respect to—
(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.
(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or
(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)I, when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)I are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) *Implementation Specification:* Written Contract or Other Arrangement (R)
Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).
Reference: Policy 3.9

III. Physical Safeguards

III. **Physical Safeguards** – § 164.310
A covered entity must, in accordance with § 164.306:
(a)

(1) *Standard: Facility Access Controls* – § 164.310(a)
Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Reference: Policy 3.8

(2) Implementation Specifications

(i) Contingency Operations (A)
Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Reference: Policy 3.8

(ii) Facility Security Plan (A)
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Reference: Policy 3.8 and Policy 5

(iii) Access Control and Validation Procedures (A)
Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
Reference: Policy 3.8

(iv) Maintenance Records (A)
Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).
Reference: Policy 3.8

(b) *Standard: Workstation Use* – § 164.310(b)
Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
Reference: Policy 1.3

(c) *Standard: Workstation Security* – § 164.310(c)
Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
References: Policy 1.3 and Policy 3.8

(d)

(1) *Standard: Device and Media Controls* – § 164.310(d)
Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.
References: Policy 3 and Policy 4

(2) Implementation Specifications

(i) Disposal (R)
Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
References: Policy 3.7

(ii) Media Re-use (R)
Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
Reference: Policy 3.7

(iii) Accountability (A)
Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Reference: Policy 3.7

(iv) Data Backup and Storage (A)
Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.
Reference: Policy 4.1

IV. Technical Safeguards

IV. **Technical Safeguards** - § 164.312

A covered entity must, in accordance with § 164.306:

(a)

(1) *Standard: Access Control* – § 164.312(a)
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).
References: Policy 1.1 and Policy 3

(2) Implementation Specifications

(i) Unique User ID (R)
Assign a unique name and/ or number for identifying and tracking user identity.
Reference: Policy 3.3

(ii) Emergency Access Procedure (R)
Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
Reference: Policy 3.3

(iii) Automatic Logoff (A)
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
References: Policy 3.3

(iv) Encryption and Decryption (A)
Implement a mechanism to encrypt and decrypt electronic protected health information.
References: Policy 3.6 and Policy 3.7

(b) *Standard*: *Audit Controls* – § 164.312(b)
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
References: Policy 2.4

(c)

(1) *Standard: Integrity* – § 164.312(c)
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
References: Policies 3.3, 3.4, 3.5, and 3.6

(2) *Implementation Specification*: Mechanism to Authenticate Electronic Protected Health Information (A)
Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
Reference: Policy 3.6

(d) *Standard: Person or Entity Authentication* – § 164.312(d)
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
Reference: Policy 3.3

(e)

(1) *Standard: Transmission Security* – § 164.312(e)
Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
References: Policies 3.3, 3.4, 3.5 and 3.6

(2) Implementation Specifications

(i) Integrity Controls (A)
Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
References: Policies 3.3, 3.4, 3.5 and 3.6

(ii) Encryption (A)
Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
References: Policies 3.3, 3.4, 3.5 and 3.6

V. Organizational Requirements

V. **Organizational Requirements** - § 164.314
(a)

(1) *Standard: Business associate contracts or other arrangements*
Reference: Policy 3.9

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—
(A) Terminated the contract or arrangement, if feasible; or
(B) If termination is not feasible, reported the problem to the Secretary.

(2) Implementation Specifications

(i) *Business associate contracts*
The contract between a covered entity and a business associate must provide that the business associate will—
(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;
(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
(C) Report to the covered entity any security incident of which it becomes aware;
(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(ii) *Other Arrangements*
(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—
(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or
(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.
(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of

business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(b)

(1) *Standard: Requirements for group health plans*
Reference: None Required
Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation Specifications (R)*
The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

VI. Policies and Procedures and Documentation

VI. **Policies and Procedures and Documentation** - § 164.316
A covered entity must, in accordance with § 164.306:

(a) *Standard: Policies and Procedures* – § 164.316(a)
Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.
Reference: All HIPAA Security Policies

(b)

(1) *Standard: Documentation* – § 164.316(b)

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Reference: Policy 2.5

(2) Implementation Specifications

(i) Time Limit (R)

Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Reference: Policy 2.5

(ii) Availability (R)

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Reference: Policy 2.5

(iii) Updates (R)

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Reference: Policy 2.5

Policy 1. Workforce Compliance with HIPAA Security Provisions

Purpose

The purpose of the policy on Workforce Compliance with HIPAA Security Provisions is to ensure that the BCS workforce complies with all elements of the HIPAA Security Rule and its related policies, as called for in §164.306(a)(4). The security of protected health information is of critical importance to the agency and must be ensured at all times. All workforce members must be made aware of the importance of the confidentiality, integrity, and availability of electronic protected health information (PHI). This policy includes sections in the following topics:

1.1 Workforce Authorization and Clearance

1.2 Information Security Awareness and Training

1.3 Workstation Use

Policy

1.1 Workforce Authorization and Clearance

BCS shall adopt procedures to ensure that all members of the workforce have appropriate access to electronic PHI and do not have unnecessary or inappropriate access to electronic PHI. Procedures shall be established to ensure that all workforce members working with electronic PHI or working in areas where electronic PHI is accessible shall be authorized to do so and/or shall be supervised while doing so. For instance, contractor or service personnel needing access to areas where electronic PHI is accessible should be known to the agency and granted access and/or supervised accordingly.

1.2 Information Security Awareness and Training

BCS shall establish an Information Security Awareness and Training Program for the purpose of ensuring that all workforce members, including management, are aware of BCS's security policies and procedures and general principles of information security.

Each member of the workforce shall receive appropriate training in HIPAA and information security policies and procedures:

1. prior to being allowed to access or use electronic PHI
2. when their responsibility is increased
3. when they are promoted or reassigned
4. when systems in use change
5. when security policies and procedures change
6. On a continuing education basis at least annually.

The training program shall include:

1. Periodic security updates (such as logon reminders, periodic e-mails, newsletter entries, posters, etc.)
2. Procedures for guarding against, detecting, and reporting malicious software (such as worms, viruses, Trojan horses, etc.)
3. Procedures for monitoring log-in attempts and reporting discrepancies (such as what to do if your log-in does not work properly)
4. Procedures for creating, changing, and safeguarding passwords (such as how often to change them, good password lengths and character combinations, etc.)
5. Documentation of all training activities performed, including attendance.

1.3 Workstation Use

On-the-job e-mail and Internet access are powerful tools that can help BCS staff accomplish their work more efficiently. As with any of BCS's limited resources, Internet access and e-mail services are made available to staff primarily for business use. However we recognize that from time to time, staff may need to use these resources for personal reasons to balance demands between their work and personal lives. As such, employees may use BCS e-mail and Internet resources for both business and certain non-business purposes subject to the following:

1. BCS e-mail and Internet services are the property of BCS. Use of these resources whether in the office or from a remote dial-up location, is not private.
2. Non-business use of these resources must be governed by good judgment and restraint, and must be limited to non-work time, i.e. before or after work or during lunch hour.
3. BCS network and computing resources must be available for business use at all times. Management will limit non-business use if it interferes with the

overall availability or cost of the services or with the productivity of individual employees.

4. BCS can and will monitor individual use of network services including visits to specific websites. Those who use BCS resources to access web sites containing sexually explicit material or content that could be construed as hostile or inconsistent with BCS policies and values, may be subject to disciplinary action, up to and including dismissal. Employees who question whether a particular site is prohibited should check with their supervisor.
5. BCS e-mail and Internet services are business tools. They must not be used to send or forward threatening or harassing messages or chain letters, or to express personal opinions on behalf of the Bureau in on-line forums.
6. Staff must obtain the approval of the BCS Systems Administrator before downloading pictures, screensavers, messenger software from websites such as AOL, Yahoo, Lycos and MSN, or any other software.
7. Users may not share their log-in or access codes or passwords with others and may not allow others to use their workstations except as allowed in an approved business process.
8. Protected health information may not be sent, copied, or removed from a workstation by any method except as part of an approved business process.
9. Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate business or healthcare reason to access that information, to the extent practicable.

Policy 2. Information Security Management Process

Purpose

The purpose of the Information Security Management Process policy is to establish requirements for an Information Security Management Process for BCS. Such a process is required by the HIPAA Security Rule §164.308(a)(1) as a means of managing the security of PHI now and over time. The process includes the following topics:

2.1 Assigned Security Responsibility

2.2 Risk Analysis and Management

2.3 Information Security Incident Procedures

2.4 Information Systems Usage Audits and Activity Reviews

2.5 Documentation for HIPAA

2.6 Information Security and Compliance Evaluation

Policy

2.1 Assigned Security Responsibility

BCS will assign responsibility for all matters relating to the safeguarding of health information to a HIPAA Security Officer. This individual will be responsible for ensuring that all PHI in electronic form is protected against reasonably anticipated threats or hazards to the security and integrity of PHI, and against reasonably anticipated improper uses and disclosures under the Privacy Rule.

The Security Officer will:

1. Ensure that all policies and procedures required by the HIPAA Security Rule are established and maintained over time.
2. Be responsible for monitoring the appropriate and consistent implementation of policies and procedures.
3. Ensure that all members of the workforce, contractors, and business associates are aware of and abide by the policies and procedures.
4. Be responsible for the investigation of information security incidents and/or breaches.

5. Ensure that any security weaknesses discovered in the course of security incidents or security evaluations will be prioritized for correction and corrected.
6. Ensure that analyses and documentation required by the HIPAA Security Rule and/or BCS's security policies and procedures are carried out fully and completely.

2.2 Risk Analysis and Management

BCS shall establish procedures for risk analysis and assessment according to HIPAA Security Rule §164.308(a)(1). Such procedures shall include the conduct of an accurate and thorough assessment of the potential risks and vulnerabilities to PHI held by the agency. Risk analysis and assessment shall be carried out using a process that substantially conforms to the process defined in the National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information technology Systems" (document available at http://csrc.nist.gov/publications/nistpubs).

Risks shall be mitigated and managed by BCS to the best of its abilities within reasonable constraints of cost, staff ability, and hardware and software capabilities.

IT Committee with IT staff and other program staff meets at least twice a year to discuss risk analysis and other IT concerns.

2.3 Information Security Incident Procedures

BCS shall develop procedures for the reporting, processing, and response to suspected or known information security incidents, in order to investigate, mitigate, and report such incidents, so that security violations may be reported and handled promptly, using a known, orderly process. Such procedures will be made known to all workforce members.

Procedures shall follow the agency's usual incident handling procedures and, as practicable, incorporate recommendations described in National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide" (document available at http://csrc.nist.gov/publications/nistpubs).

2.4 Information Systems Usage Audits and Activity Reviews

It is the policy of BCS to use, to the extent practicable, procedures and available technologies to record and examine activity in information systems holding PHI in order to discover and facilitate investigations into information security incidents, and provide information for input to the agency's security management process. The level of detail to be audited will be set as part of the overall information systems risk management program.

As systems are modified and expanded, abilities to audit access in greater detail shall be pursued where practicable and according to any risk mitigation plan in place.

BCS shall establish procedures to conduct the periodic review of the agency's internal security controls. Such controls may include, for example:

1. Logs produced by firewall or system monitoring applications
2. Access reports and other documentation provided by application programs in use
3. System security status reports
4. Incident tracking systems and procedures
5. Sign-in logs for service personnel.

Such reviews of information system activity shall be sufficient to determine the effectiveness of security procedures and controls, and discover any security issues that may not be addressed by the procedures or controls in place.

2.5 Documentation for HIPAA

It is the policy of BCS to document any policies and procedures implemented under the requirements of the HIPAA Security Rule.

The agency shall also document any actions, activities, and assessments required to be performed under the Rule, or under the requirements of agency policies enacted in support off the HIPAA Security Rule.

Documentation may be in electronic or paper format.

Documentation under this policy shall be maintained for at least six years from the date of issue or the date of last effect, which ever is later.

Relevant documentation shall be made available to the people responsible for implementing policies and procedures enacted under the HIPAA Security Rule.

Documentation shall be periodically reviewed and updated as needed or in response to environmental or operational changes affecting the security of electronic PHI.

2.6 Information Security and Compliance Evaluation

BCS shall perform regular, periodic evaluations of the information security-related policies and procedures in place at the agency to ensure that they continue to meet the requirements of the HIPAA Security Rule. The period of review shall be determined according to the agency's information systems risk analysis and consideration of best practices.

Evaluations shall also be performed whenever there is a change in environmental or operational conditions that may affect the security of electronic protected health information. For example, such changes would include (but not be limited to):

1. The emergence of a significant new threat such as
    a) terrorist attacks of facilities
    b) the emergence of new type of computer virus
2. Significant change in information systems such as
    a) the installation of a new computer system or
    b) Installation of new services such as wireless or remote access.

Evaluations shall include the review of relevant information security-related policies and procedures, and shall be documented for compliance with the HIPAA Security Rule and to provide direction to the agency in the execution of its security plans.

Policy 3. Information Access Management and Control

Purpose

The purpose of the Information Access Management and Control policy is to ensure that all members of the workforce have access to the systems and information appropriate to their job functions, and to ensure that inappropriate access is prevented. The policy includes the following topics:

3.1 Information Access Management

3.2 Termination Procedures

3.3 Technical Access Control and Authentication

3.4 Technical Perimeter Security

3.5 Remote Access

3.6 Data Encryption and Integrity

3.7 Electronic Information Device and Media Controls

3.8 Physical Access Controls

3.9 Contracts and Memoranda of Understanding and PHI

Policy

3.1 Information Access Management

BCS shall institute procedures for granting access to electronic PHI (for example, through access to a workstation, transaction, program, process or other mechanism) to authorized persons. Such access shall be granted only within the bounds of the "minimum necessary" requirements of the HIPAA Privacy Rule.

The agency shall institute procedures to establish, document, review, and modify a user's right of access to a workstation, transaction, program, process or other mechanism. Access lists will be reviewed regularly.

Supervisors are required to complete the following information and submit it by e-mail to the BCS MIS department (helpdesk@wearebcs.org) in order to establish or modify access:

1. First Name
2. Middle Name
3. Last Name

4. Title or New Title
5. Phone Number of Extension
6. Department
7. Location
8. Is a PC in the location desired? (If not please request via the Director of Administrative Services or his designee.)
9. Specify Software to be Used (for example: GroupWise, Internet Access, Microsoft Office, Financial Edge, Raiser's Edge, Accumed, etc.)
10. Justification for Internet Access, if desired

3.2 Termination Procedures

BCS shall adopt procedures to ensure that terminated workforce members or workforce members whose access to electronic PHI is restricted shall have physical and/or system access privileges removed and shall surrender any keys, tokens, or other objects that allow access. In addition, combination locks and alarm system codes known by such workforce members shall have their combinations or codes changed.

Procedures shall identify:

1. The parties to be involved in termination activities
2. The steps to be taken in the process of termination
3. The timing of termination activities, such as coordination of notice of termination with removal of access to systems and networks.

Supervisors are required to complete the following information and submit it by e-mail to the BCS MIS department as soon as termination information is available:

1. First Name
2. Middle Name
3. Last Name
4. Title
5. Phone Number of Extension
6. Department
7. Location
8. Termination Date and Time
9. Are electronic files needed from the terminated user's accounts?
10. Specify Needed Files (Note that files will not be available after deletion so please describe here any and all files desired for retention)

3.3 Technical Access Control and Authentication

It is the policy of BCS to limit, through technical means as practicable, access to electronic protected health information (PHI) to only those persons or software programs that have been properly granted access rights.

Authentication Procedures shall be established to verify the identity of the person or entity seeking access to electronic PHI. Persons may be authenticated by the use of passwords, cards, tokens, keys, biometrics, or other means of personal identification. System authentication shall be required for system access of PHI.

Unique Log-In Every user of systems holding or using electronic PHI shall have a unique user name or number, to enable the identification and tracking of user access. Users may not share their log-in or access codes or passwords with others.

Group Log-Ins Group log-ins shall not be used, except in situations where it is necessary to use such procedures to maintain quality of care, where permitted by an approved business process. Where group log-ins are used, there shall be procedural methods for recording the members of a group that have access under a single log-in.

Password Policy Passwords must be changed at least every 90 days and must be at least five characters, with a combination of letters and numbers. Users' GroupWise passwords should not be the same as their network passwords.

Emergency Access Procedures shall be developed to ensure that electronic PHI shall be accessible by approved personnel in an emergency situation in which normal access is not available.

Automatic Log-Off Electronic procedures shall be established to terminate an electronic session after a predetermined period of inactivity. Procedures may include password-protected screen savers or forced logouts of systems and/or applications.

3.4 Technical Perimeter Security

It is the policy of BCS to establish technical perimeter security controls, such as properly configured routers and firewalls and any other devices related to BCS's computer network security, in order to protect the electronic protected health information (PHI) held within the agency's systems and allow access where appropriate.

Wireless network hubs shall be allowed only in approved locations and shall be configured so as to protect the security of the agency's perimeter and its electronic PHI.

3.5 Remote Access

BCS does not allow staff remote access to electronic networks or PCs containing protected health information (PHI).

Staff e-mail may be accessed remotely via GroupWise Web Access according to a defined procedure and must be kept confidential. Any PHI remaining on remote computers must be secured.

Any remote access requests must be approved by the MIS manager and the BCS HIPAA Committee. All requests must show the need for remote access. The MIS manager will ensure that adequate authentication and safeguards in place.

Vendor remote access to systems must be approved by the accounts department and may be performed only by a defined procedure and under the supervision of the MIS manager. As of June 2013, the Deputy Executive Director, the Chief Financial Officer, the Director of External Relations and Advancement, and the Hurricane Sandy Relief staff have laptops with VPN client remote access.

3.6 Data Encryption and Integrity

It is the policy of BCS to encrypt electronic PHI at rest or in transmission where a risk analysis indicates that such encryption is necessary to protect the security of PHI. Such risk analysis shall consider the probability and criticality of risks to security.

1. Technical procedures shall be instituted to provide encryption and decryption capabilities where deemed necessary by the risk analysis.
2. Unencrypted e-mail or e-mail attachments to outside of BCS must not contain any PHI unless required by a city or state agency requesting specific information as part of a regular BCS process.
3. Electronic transmission of PHI outside of BCS by other than e-mail may only be as part of regular BCS processes, such as claims submission, and must be secured through encryption.
4. Portable devices such as Palm Pilots, laptop computers, “USB memory sticks”, and other devices that are easily lost or stolen shall use encryption technologies to protect PHI resident on those devices.
5. Data Backup devices and programs shall encrypt the contents of files containing any PHI, if feasible with the technologies in use at BCS.
6. Procedures shall be developed to ensure that encrypted electronic PHI at rest shall be accessible by approved personnel in an emergency situation.

It is the policy of BCS to use, to the extent practicable, available technologies to corroborate that electronic protected health information held by BCS has not been altered or destroyed in an unauthorized manner. New systems procured should ensure the integrity of the information stored on them to the extent practicable, using readily available technologies.

3.7 Electronic Information Device and Media Controls

It is the policy of BCS that the movement of hardware and electronic media which contain electronic PHI into and out of agency facilities shall be controlled.

There shall be procedures to record the movement, and the person responsible for the movement, of hardware and electronic media containing electronic PHI into, out of, and within agency facilities.

The disposal or reuse for another purpose of any hardware or electronic media containing electronic protected health information (PHI) shall include the destruction of any such PHI before ultimate disposal or reallocation to a new use. The destruction of electronic PHI shall be carried out by physical or electronic means that ensures the actual destruction of the information. Simply "dragging files to the trash" is not sufficient to destroy PHI. Procedures shall be defined in order to ensure the destruction of information in systems that are de-commissioned, reused, or sold.

The use of portable memory devices, such as "USB memory sticks", for the purpose of removing PHI from BCS facilities is prohibited without prior approval from the HIPAA Security Officer. Any such approved devices must encrypt any PHI stored thereon.

3.8 Physical Access Controls

Equipment should be protected from fire, flood, and other natural disasters. Computers in open areas accessible to the public should be locked to desks where feasible. Servers should be in locked rooms or closets with access restricted to the MIS department and maintenance staff only.

Security procedures shall be employed to safeguard facilities and the equipment therein from unauthorized physical access, tampering, and theft, while ensuring that properly authorized access is allowed. Such plans and procedures may include security guards at entrances enforcing sign-in by visitors, employee awareness of personnel authorized to be in areas where client information is present, access control during

emergencies, staff monitoring of information system vendor personnel, and documentation of physical security modifications and maintenance.

3.9 Contracts and Memoranda of Understanding and PHI

BCS shall enter into written agreements with any entities that use or disclose electronic protected health information on behalf of the agency, in order to require the protection of the security of any and all such information. Such agreements shall be Business Associate Contracts or Memorandums of Understanding designed to meet the requirements of HIPAA Security Rule §164.308(b) and §164.314(a).

This policy shall not apply in the following situations:

1. When electronic PHI is transmitted to a provider for purposes of treatment
2. When electronic PHI is transmitted by a group health plan (or an HMO or health insurance issuer on behalf of a group health plan) to the plan sponsor (provided the recipient provides assurances it will safeguard the PHI)

Policy 4. Data Backup and Contingency Planning

Purpose

The purpose of the Data Backup and Contingency Planning policy is to ensure that BCS has a usable copy of electronically held PHI and can properly respond to emergencies or other occurrences that may damage systems containing electronic PHI, as required by HIPAA Security Rule §164.308(a)(7). The policy includes the following topics:

4.1 Data Backup

4.2 Contingency Planning

Policy

4.1 Data Backup

BCS shall develop procedures for the regular and periodic backup of electronically held health information. Backups shall be sufficient to restore damaged data with a useful duplicate.

Backup procedures shall include the following elements:

1. Definition of which file systems to back up
2. Definition of frequency of backups
3. Definition of frequency of media rotation
4. Definition of off-site storage requirements and frequency
5. Documentation and labeling of storage media
6. Regular testing of backed up data to ensure adequacy.
7. Performing backups before the movement of systems.

4.2 Contingency Planning

BCS shall develop procedures for the development and execution of contingency plans in order to properly respond to emergencies or other occurrences that may damage systems that contain electronic PHI, resulting in the loss of confidentiality, integrity, or availability of PHI.

Contingency plans must provide for the continued operation of essential or strategic activities and their critical systems in the event of an interruption or degradation

of service. Contingency plans should take into account the effects of short-term interruptions (such as brief power failures) and long-term interruptions (such as a loss of facilities to fire or contamination of some kind).

Contingency plans shall include the following required elements:

1. Disaster Recovery plans and procedures, to ensure the restoration of lost data and system access, including a full range of information and activities needed to assure that the Plan will be effective and its operation will be as smooth as possible
2. Emergency Mode Operation plans and procedures, as described in the agency's Disaster Preparedness Plan
3. Plans and Procedures for the testing and revision of contingency plans, as described in the agency's Disaster Preparedness Plan
4. Assessment of the criticality of applications/systems and data, in support of the other contingency plan components and information system backup policies and procedures.

Policy 5. Use of Photographic or Video Recording Devices

Purpose

The purpose of the policy on the Use of Photographic or Video Recording Devices is to ensure that BCS establishes procedures, such as signs prohibiting such use, to limit the use of image recording devices at agency facilities in order to limit the collection of unauthorized electronic protected health information (PHI) and protect the privacy of agency clients.

Policy

It shall be the policy of BCS that photographic and video recording devices not be used to capture the image, voice, or other PHI of any client except as part of an approved business process. The agency shall post notices in areas open to clients to the effect that cameras and video recorders of any type should not be used on the premises except for designated purposes in designated areas.

Appendix 1: Glossary of Terms

Primary Source: CMS Information Systems Security Policy, Standards and Guidelines Handbook, version 1.0, February 19, 2002.

ACCESS CONTROL A security mechanism used to grant users access to a system, based upon the identity of the user, and prevent access to unauthorized users. The user is commonly pre-defined to the system by the systems administrator with a User-id and password.

ACCESS TO INFORMATION The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

APPLICATION SYSTEM Computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system.

ASSETS These include information, software, personnel, hardware, and physical resources (such as the computer facility).

ASSET VALUATION The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

AUDIT CONTROL is two-fold in that it is:
1. An independent review and examination of system records, operational procedures, and system activities to ensure compliance with established policies, procedures, and
2. A record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction, from its inception to output of final results.

AUTHENTICATION is:

1. The corroboration that an entity (User, Process, etc.,) is the one claimed.
2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs, and processes.

AVAILABILITY Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.

BACKUP The process of creating exact copies of data in storage that can be used to restore lost data in contingency circumstances. Also, the information so copied.

BIOMETRICS identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).

CERTIFICATION A technical evaluation with system owner's concurrence of a sensitive application and/or system to see how well it meets security requirements.

CHECKSUM is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can determine whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

COMPUTER SECURITY The concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss.

COMPUTER SYSTEM Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

CONFIDENTIALITY Assurance that data is protected against unauthorized disclosure to individuals, entities or processes.

CONSEQUENCE (or IMPACT) ASSESSMENT An estimation of the degree of overall, aggregate harm or loss that could occur, e.g., lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury, or loss of life.

CONTINGENCY PLAN A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan.

CONTINGENCY PLANNING A planned response to high impact events to maintain a minimum acceptable level of operation.

DATA INTEGRITY ASSURANCE TECHNOLOGIES The technological means of assuring that information stored in electronic systems has not been altered or destroyed

in an unauthorized fashion. For example, hardware-based data integrity assurance technologies may include error-correcting memory or duplicated storage systems; software-based data integrity assurance technologies may include mathematical checksums or other programmatic means of detecting anomalies in stored information.

DATABASE A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; data is stored so that it can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data.

DIGITAL SIGNATURE An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters, such that the identity of a signer and the integrity of the data can be verified.

DISASTER RECOVERY A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.

ENCRYPTION The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium.

FIREWALLS Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

GUIDELINES General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.

HACKER A person who secretively invades others' computers, inspecting or tampering with the programs or data stored on them.

HIPAA The Health Insurance Portability and Accountability Act of 1996, under which the HIPAA Security Rule (and other HIPAA rules) is created.

HIPAA SECURITY RULE Published in the United States Federal Register as 45 CFR Parts 160, 162, and 164. Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. Washington, DC.

INFORMATION SYSTEMS FACILITY An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. IS Facilities range from large centralized computer centers to individual standalone workstations.

ILLEGAL ACCESS AND DISCLOSURE Activities of employees that involve improper systems access and sometimes disclosure of information found thereon, but not serious enough to warrant criminal prosecution.

INFORMATION Any communication or reception of knowledge, such as facts, data, or opinions; including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape.

INFORMATION SYSTEMS SECURITY (INFOSEC) The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. Protection results from the application of a combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.

INTEGRITY Assurance that data is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.

INTERNET A worldwide electronic system of computer networks which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.

LOCAL AREA NETWORK (LAN) A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. Local area networks commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.

MAJOR APPLICATION (MA) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. Note: All applications holding electronic protected health information require some level of protection. Certain

applications, because of the information in them, however require special management oversight and should be treated as major.

MALICIOUS SOFTWARE The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms.

MEDIA Hard copy (including paper), PC/ workstation diskettes, and other electronic forms by which CMS data is stored, transported, and exchanged. The need to protection information confidentiality, integrity, and availability applies regardless of the medium used to store the information. However, the risk exposure is considerably greater when the data is in an electronically readable or transmittable form compared to when the same data is in paper or other hard copy form.

MISUSE OF ORGANIZATION PROPERTY The use of computer systems for other than official business that does not involve a criminal violation, but is not permissible under organization policies.

MITIGATION See Risk Mitigation.

MODEM Modem is short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line. Modems convert digital computer signals into analog telephone signals (modulate) and the reverse (demodulate).

NETWORK A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A network can be as small as a LAN consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer network exists to provide computer users with the means of communicating and transferring information electronically.

NIST The National Institute of Standards and Technology, which (among many duties) creates standards and guides to be used in meeting various Federal requirements such as HIPAA. NIST documents are frequently cited in the preamble to the HIPAA Security Rule.

PASSWORDS A confidential character string used to authenticate an identity or prevent unauthorized access. Passwords are most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).

PERSONNEL SECURITY Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of information resources which the individual will be able to access.

PHI An abbreviation for Protected Health Information (see below).

PHYSICAL SECURITY The application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information.

POLICY A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

PROCEDURES Define the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.

PROTECTED HEALTH INFORMATION (PHI) The health information concerning health treatment of an individual and payment for such services. Virtually all health information held by a HIPAA covered entity is protected by HIPAA in some manner.

RISK The potential for harm or loss. Risk is best expressed as the answers to these four questions:

1. What could happen? (What is the threat?)
2. How bad could it be? (What is the impact or consequence?)
3. How often might it happen? (What is the frequency?)
4. How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" *per se*.

RISK ANALYSIS A process whereby cost-effective security / control measures may be selected by balancing costs of various security control measures against the losses that would be expected if these measures were not in place.

RISK ASSESSMENT The identification and study of the vulnerability of a system and the possible threats to its security.

RISK MANAGEMENT The total process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk, including identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost/benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review. It encompasses the incorporation of the processes and results from both risk analysis and risk mitigation.

RISK MITIGATION The process of reducing the probability and / or consequences of an adverse risk event to an acceptable threshold.

SAFEGUARD ANALYSIS An examination of the effectiveness of the existing security measures, actions, devices, procedures, techniques, or other measures that reduce a system's vulnerability to a threat and identification of appropriate new security measures that could be implemented on the system.

SECURITY All of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data.

SECURITY-RELATED EVENT An attempt to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also included are attempts to violate the security policy of the system (e.g., too many attempts to log on, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).

SECURITY VIOLATION An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. This includes, but is not limited to, unusual or apparently

malicious break-in attempts (either local or over a network), virus or network worm attacks, or file or data tampering, or any incident in which a user, either directly or by using a program, performs unauthorized functions.

SENSITIVE APPLICATION An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, or delivery interruption of the application.

SENSITIVE DATA Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an organization to accomplish its mission, proprietary data, and records about individuals requiring protection under HIPAA.

SIGNIFICANT CHANGE A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation.

STANDARDS Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to meaningful and effective.

SYSTEM OWNER/MANAGER The official who is responsible for the operation and use of an application system.

SYSTEM SECURITY PLAN A basic overview of the security and privacy requirements of the subject system and the organization's plan for meeting those requirements.

TELECOMMUNICATIONS A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such as telephone lines, microwave relay, satellite link, or physical cable.

THREAT An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.

THREAT IDENTIFICATION The analysis of recognized threats to determine the likelihood of their occurrence and their potential to harm assets.

TROJAN HORSE A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. Also a destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful.

USER The person who uses a computer system and its application programs to perform tasks and produce results.

VIRUS A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. May be a self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component.

VULNERABILITY A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.

WIDE AREA NETWORK (WAN) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. A WAN is a communications network that connects geographically separated areas.

WORKFORCE The collection of employees, trainees, contractors, and volunteers whose conduct, in the performance of work or services for a HIPAA-covered organization, is under the direct control of such entity, whether or not they are paid by the covered entity.

WORKSTATION A workstation is a computer built around a single-chip microprocessor. Less powerful than minicomputers and mainframe computers, workstations have nevertheless evolved into very powerful machines capable of complex tasks. Technology is progressing so quickly that state-of- the-art workstations are as powerful as mainframes of only a few years ago, at a fraction of the cost.

WORLD-WIDE WEB (WWW or WEB) The collection of electronic pages, (documents) that are developed in accordance with the HTML (hyper text markup language) Web format standard and may be accessed via Internet connections.

WORM A worm is a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information.

Appendix 2: Form for Notification of New Hire or Promotion

Brooklyn Community Services
Computer Services Request for New Hire or Promotion

Supervisors are required to complete the following information for all their new hires or promoted staff and submit this form by e-mail to the MIS department.

First Name:

Middle Name:

Last Name:

Title or New Title:

Phone Number of Extension:

Department:

Location:

Is a PC in the location desired? (If not please request via the Director of Administrative Services or his designee.)

Specify Software to be Used (for example: GroupWise, Internet Access, Microsoft Office, MS Access, MS Publisher, Echo, Raiser's Edge, Accumed, etc.):

Justification for Internet Access, if desired:

Appendix 3: Form for Notification of Termination

Brooklyn Community Services
Notice to MIS of Termination of Computer Services

Supervisors are required to complete the following information as soon as termination information is available. This form should be submitted by e-mail to the MIS department.

First Name:

Middle Name:

Last Name:

Title:

Phone Number of Extension:

Department:

Location:

Termination Date and Time:

Are electronic files needed from the terminated user's accounts?

Specify Needed Files (Note that files will **not** be available after deletion so please describe here **any and all files** desired for retention)