Glossary of Selected HIPAA Terminology

Business associate (BA): The 2013 Omnibus Rule significantly expands the definition as follows:

"*Business associate*:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services."

Covered entity (CE): An organization (including government agencies and businesses) that is directly covered by the HIPAA Administrative Simplification rules, including the Privacy and Security Rules:

- "A health plan
- A health care clearinghouse
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter"

Providers for whom another entity (covered or not) transmits claims, remittance, referrals, etc., electronically become CEs themselves.

Disclosure: The "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the [individually identifiable health] information."

Protected health information (PHI): All individually identifiable health information (with the exception of, for example, FERPA-protected data) in any form or medium. The Omnibus Rule explicitly includes genetic information as PHI.

Use: The "sharing, employment, application, utilization, examination, or analysis of [individually identifiable health information] within an entity that maintains such information."

Workforce: All "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Workforce members are not BAs, and BAs are not workforce members. Independent contractors working substantially on-site are considered part of the workforce if there is no BA contract.

Source: Electronic Code of Federal Regulations, 45 CFR 160.103. http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=2&SID=2819d30d81ced53a03f5555703ecd405&h=L&r=PART&n=45y1.0.1.3.75#45:1.0.1.3.75.1.27.3.

HIPAA Security Rule Matrix

The most current regulation text is available at www.ecfr.gov*. Select Title 45, and then select Subtitle A and scroll down to Subchapter C for the parts listed here. This is a summary snapshot.*

Volume 45 of the Code of Federal Regulations

45 CFR Part 160 – **General Administrative Requirements,** including Administrative Simplification definitions, preemption, compliance and enforcement, and civil monetary penalties

45 CFR Part 164 – Security and Privacy

Subpart A – General provisions for subpart C [security] and subpart E [privacy], including [these are the main points]:
164.103 Definitions [applicable to Security Rule and Privacy Rule]
164.104 Applicability
164.105 Organizational requirements

Subpart C – Security Standards for the Protection of Electronic Protected Health Information
164.302 Applicability
164.304 Definitions [specific to the Security Rule]
164.**306** **Security standards: General rules**
164.**308** **Administrative** safeguards
164.**310** **Physical** safeguards
164.**312** **Technical** safeguards
164.**314** **Organizational requirements**
164.**316** **Policies and procedures and documentation requirements**
164.318 Compliance dates for the initial implementation of the security standards

Subpart D – Notification in the Case of Breach of Unsecured Protected Health Information
164.4xx

Subpart E – Privacy of Individually Identifiable Health Information
164.5xx

*Editor's note: *These documents are adapted from 45 CFR Appendix A to Subpart C of Part 164—Security Standards: Matrix.* http://www.gpo.gov/fdsys/granule/CFR-2010-title45-vol1/CFR-2010-title45-vol1-part164-subpartC-appA/content-detail.html.

Administrative Safeguards*

Standards (all required)	Citations	Implementation Specifications (R) = Required (A) = Addressable	
Security Management Process	164.308(a)(1)(i)		
	.308(a)(1)(ii)(A)	Risk Analysis	**(R)**
	.308(a)(1)(ii)(B)	Risk Management	**(R)**
	.308(a)(1)(ii)(C)	Sanction Policy	**(R)**
	.308(a)(1)(ii)(D)	Information System Activity Review	**(R)**
Assigned Security Responsibility	164.308(a)(2)		**(R)**
Workforce Security	164.308(a)(3)(i)		
	.308(a)(3)(ii)(A)	Authorization and/or Supervision	(A)
	.308(a)(3)(ii)(B)	Workforce Clearance Procedure	(A)
	.308(a)(3)(ii)(C)	Termination Procedures	(A)
Information Access Management	164.308(a)(4)(i)		
	.308(a)(4)(ii)(A)	Isolating Healthcare Clearinghouse Function	**(R)**
	.308(a)(4)(ii)(B)	Access Authorization	(A)
	.308(a)(4)(ii)(C)	Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)(i)		
	.308(a)(5)(ii)(A)	Security Reminders	(A)
	.308(a)(5)(ii)(B)	Protection from Malicious Software	(A)
	.308(a)(5)(ii)(C)	Log-in Monitoring	(A)
	.308(a)(5)(ii)(D)	Password Management	(A)
Security Incident Procedures	164.308(a)(6)(i)		
	.308(a)(6)(ii)	Response and Reporting	**(R)**
Contingency Plan	164.308(a)(7)(i)		
	.308(a)(7)(ii)(A)	Data Backup Plan	**(R)**
	.308(a)(7)(ii)(B)	Disaster Recovery Plan	**(R)**
	.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	**(R)**
	.308(a)(7)(ii)(D)	Testing and Revision Procedure	(A)
	.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		**(R)**
Business Associate Contracts and Other Arrangements	164.308(b)(1)		
	.308(b)(4)	Written Contract or Other Arrangement	**(R)**

Physical Safeguards*

Standards (all required)	Citations	Implementation Specifications **(R) = Required (A) = Addressable**	
Facility Access Controls	164.310(a)(1)		
	.310(a)(2)(i)	Contingency Operations	(A)
	.310(a)(2)(ii)	Facility Security Plan	(A)
	.310(a)(2)(iii)	Access Control and Validation Procedures	(A)
	.310(a)(2)(iv)	Maintenance Records	(A)
Workstation Use	164.310(b)		**(R)**
Workstation Security	164.310(c)		**(R)**
Device and Media Controls	164.310(d)(1)		
	.310(d)(2)(i)	Disposal	**(R)**
	.310(d)(2)(ii)	Media Re-use	**(R)**
	.310(d)(2)(iii)	Accountability	(A)
	.310(d)(2)(iv)	Data Backup and Storage	(A)

Technical Safeguards*

Standards (all required)	Citations	Implementation Specifications **(R) = Required (A) = Addressable**	
Access Control	164.312(a)(1)		
	.312(a)(2)(i)	Unique User Identification	**(R)**
	.312(a)(2)(ii)	Emergency Access Procedure	**(R)**
	.312(a)(2)(iii)	Automatic Logoff	(A)
	.312(a)(2)(iv)	Encryption and Decryption	(A)
Audit Controls	164.312(b)		**(R)**
Integrity	164.312(c)(1)		
	.312(c)(2)	Mechanism to Authenticate Electronic PHI	(A)
Person or Entity Authentication	164.312(d)		**(R)**
Transmission Security	164.312(e)(1)		
	.312(e)(2)(i)	Integrity Controls	(A)
	.312(e)(2)(ii)	Encryption	(A)

Additional Security Rule standards:

164.306 General rules [requirements … CEs "must do the following"]

(a)(1) **Ensure** the confidentiality, integrity, availability of all ePHI

(2) **Protect** against any reasonably anticipated threats or hazards to the security or integrity of ePHI

(3) **Protect** against any reasonably anticipated uses/disclosures not permitted or required by Privacy Rule

(4) **Ensure** workforce compliance

(b) **Flexibility** of approach [use any measures to reasonably and appropriately implement standards, taking into account size, complexity, capabilities, including technology, cost, and criticality of potential risks]

(c) **Standards:** Must comply with all

(d) **Implementation specifications**: Either required or addressable

(e) **Maintenance**: Security measures must be reviewed and modified as needed

164.314 Organizational requirements

(a)(1) Standard: **Business associate** contracts or other arrangements. [Parallels Privacy Rule …] Business associate (BA) will:

- Implement safeguards to protect confidentiality, integrity, and availability of ePHI
- Ensure that its agents do the same
- Report security incidents to CE
- Make its policies, procedures, and documents available to HHS for compliance determination
- Authorize CE to terminate contract if BA violates material term of contract

(b)(1) Standard: Requirements for **group health plans**. [Like Privacy Rule and like BA contract: Update plan document, require plan sponsor to ensure safeguards, ensure adequate separation, ensure agents agree, report incidents to plan]

164.316 Policies and procedures and documentation requirements

(a) Standard: Policies and procedures [must have in writing or electronic]

(b)(1) Standard: Documentation [must retain policies, RA reports, etc.]

Implementation specifications:

(b)(2)(i) Retention (R): Six-year retention (later of the date created or date last in effect)

(b)(2)(ii) Availability (R): Make available to those needing them

(b)(2)(iii) Review (R): Review periodically and update as needed in response to changes affecting security

HIPAA/HITECH Act Administrative Simplification Penalties

Civil penalties for failure to comply with Privacy, Security, Breach Notification, and other Administrative Simplification Rules

Violation Tier	Monetary Penalty
A. Person did not know (and by exercising reasonable diligence[1] would not have known) that a provision was violated	$100–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision during a calendar year
B. Violation due to reasonable cause[2] and not to willful neglect[3]	$1,000–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision during a calendar year
C. Violation due to willful neglect, but corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation	$10,000–$50,000 for each violation Up to $1,500,000 for all such violations of an identical provision during a calendar year
D. Violation due to willful neglect and not corrected within 30 days of knowing, or date when entity exercising due diligence would have known, of the violation	$50,000 for each violation $1,500,000 for all such violations of an identical provision during a calendar year

45 CFR 160.401:
[1] *Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

[2] *Reasonable cause* means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

[3] *Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

HIPAA/HITECH Act Administrative Simplification Penalties

Criminal penalties

Criminal penalties* for wrongful disclosure of individually identifiable health information knowingly and in violation of HIPAA:

(1) Using a unique health identifier OR

(2) Obtaining identifiable health information OR

(3) Disclosing identifiable health information

Offense	Fine and/or Imprisonment
Knowing misuse	Up to $50,000 and/or up to one year imprisonment
Knowing misuse under false pretenses	Up to $100,000 and/or up to five years imprisonment
Knowing misuse with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm	Up to $250,000 and/or up to 10 years imprisonment

*Refer to 42 USC 1320d–6. *http://www.gpo.gov/fdsys/granule/USCODE-2010-title42/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d-6/content-detail.html.*

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement.

These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual’s request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual’s request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either “covered entity” or “individual”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as “as necessary to perform the services set forth in Service Agreement.”]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity’s minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1.

    1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
    2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
    3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
    4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
    5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) <u>Survival</u>. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] <u>Regulatory References</u>. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] <u>Amendment</u>. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] <u>Interpretation</u>. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Active/ Inactive	Name of BA	Services Provided	Date of Signing	Legal Signature Name and Position

Questions to Ask When Selecting Business Associates

Ensure that a business associate's (BA) policies and processes are documented and comprehensive. Ask to review all security and privacy policies and workforce training materials. Review the process for identifying an incident and responding to it. For example, ask the following questions:

- What is considered an incident?
- To whom is it reported?
- How quickly must it be reported?

Ensure that both parties document this service level agreement.

Covered entities (CE) can use the following questions to assess their BAs' privacy and security controls, and BAs can use them to assess their subcontractor BAs privacy and security controls:

1. Are you also a Health Insurance Portability and Accountability Act (HIPAA) CE? (If so, the organization should be fully HIPAA compliant and should be able to answer questions readily.) Are you accredited by The Joint Commission or National Committee for Quality Assurance?
2. Have you signed HIPAA BA contracts with other organizations?
3. Do you have an information security officer and a privacy officer? If so, are they full time or part time? Where do they report within your organization? Do they have job descriptions? What are their qualifications?
4. Do you have a comprehensive, written set of security and privacy policies and procedures? How often do you review them? Who approves them?
5. Do you have a physical security policy and plan? Has an SSAE 16 (Statement on Standards for Attestation Engagements) audit been performed? If so, may we see the report?
6. How do you secure portable devices and media? How do you dispose of confidential data on all media? How do you remove data on a device or medium to prepare it for reuse?
7. Assuming you perform the same or similar service for other HIPAA CEs, how do you ensure that protected health information (PHI) from different CEs is not comingled? How do you ensure that you do not disclose one CE's PHI to another CE in error? How do you ensure that one entity cannot access another entity's PHI (unless authorized by contract)?
8. Are you disclosing PHI? If so, summarize to whom and under what circumstances you would disclose our PHI. If so, what controls have you implemented to ensure disclosure is appropriate and at the minimum necessary level?
9. Do you or do you anticipate disclosing our PHI to subcontractor(s)? If so, are they outside the United States? Have they signed your BA contract? What has your

organization done to ensure that they understand and are compliant with the HIPAA Security Rule and certain Privacy Rule requirements?

10. Describe your workforce privacy and security training program, including content, frequency, and method(s) of delivery. Does it cover the full workforce? Does it cover subcontractors?

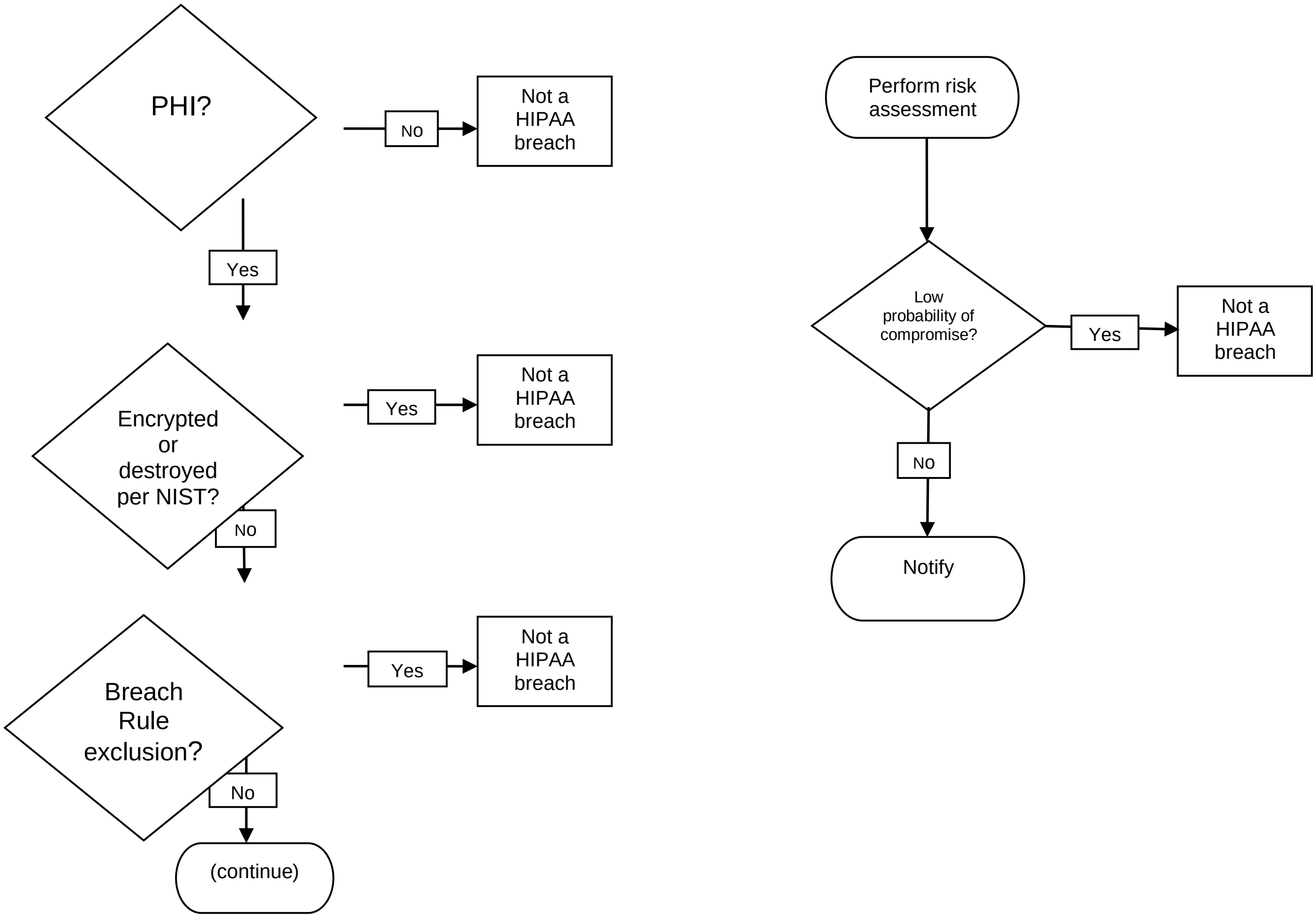
11. Do you have formal, written policies and guidelines governing privacy and security incident reporting? How do you define incidents? How would incidents be reported to our organization? Would you be informed of an incident by/under control of your subcontractor? Have you experienced an incident in the past year? Does your incident response plan include procedures for breach notification as required by the Omnibus Rule's final Breach Notification Rule?

12. Do you have formal, written policies and guidelines governing sanctions for policy violations? Do they also apply to non-employees (if you have non-employee workforce members)? How would you respond to serious violations or breaches? Do you have insurance to cover privacy and security breaches of our PHI occurring under your watch or through your subcontractors?

13. [If appropriate] How are you prepared to comply with the specific HIPAA Privacy Rule requirements for (a) inspection and copying, (b) amendment, (c) tracking and accounting of disclosures, and (d) restrictions on disclosures?

14. Upon termination of our relationship or when you no longer need certain PHI, how would you return or destroy PHI? What are your current mechanisms? How would these be affected if your company is acquired or declares bankruptcy?

15. What are your technical network perimeter controls? How will you ensure secure communication between the entities? Describe your remote authentication process (e.g., authentication on handheld devices), if appropriate. Describe how and when encryption is required. If wireless media and networks are part of the solution, describe security controls.



Courtesy of The Marblehead Group 2013

HIPAA Breach Notification Checklist

Timing

___ Discovery date: ____________________
___ Deadline for notifications (60 days post-discovery): _________________
___ Law enforcement determination of notification delay (based on hindering criminal investigation or causing damage to national security); if so:
  ___ Documentation of determination
  ___ Extended deadline for notifications: ____________

Determination of Urgency

___ Decision re: danger of imminent misuse of protected health information (PHI)/personal health record (PHR) data (if so, document decision and escalate notification procedures)

Notice

___ Public notice(s) prepared, containing organization's statement and toll-free number for inquiries, including "Am I affected?"
___ Individual notice prepared, containing:
  ___ Brief description of what occurred, date of breach, and date of discovery
  ___ Description of types of unsecured PHI involved (e.g., name, Social Security number, date of birth, home address, account number)
  ___ Steps individuals should take for protection
  ___ Brief description of what we are doing to investigate the breach, mitigate losses, and protect against further breaches
  ___ Contact information for queries and to learn additional information, including toll-free telephone number, email address, website, and/or mailing address
___ Notice to U.S. Department of Health and Human Services Secretary
  ___ If 500 or more individuals affected, immediate notice given
  ___ If fewer than 500 individuals affected, log entry made (submit no later than 60 days after end of year of breach discovery)

Contact Information and Mailings

___ Notification mailed to current address of individuals (or next of kin) as available
___ Insufficient or out-of-date information for 10 or more individuals? If so:
  ___ Public notice posted on our website
  ___ Public notice in major print or broadcast media in affected geographic regions

ABC Organization	
Policy Name: Confidential Data Protections Policy	**Effective Date:** 1/1/05
Sponsor: Information Security Officer	**Date Last Reviewed:** 1/3/11
Document Number: IS 2	**Date Obsolete:**
Revision History: Author and Description	**Revision Date:**

1. *Policy*

Information designated as confidential or highly confidential shall be protected from unauthorized access and disclosure, both intentional and unintentional, by all reasonable means and acceptable business practices.

2. *Purpose*

Information designated as confidential or highly confidential must be protected so that people and computer processes not properly authorized to access or use the information are kept from it. These protections enable this organization to maintain the privacy of our patients and plan members, our employees, and internal business matters. These protections also preserve data integrity and availability by guarding against improper or unauthorized alteration, as well as loss, of confidential and highly confidential data.

3. *Scope*

This policy applies to our confidential and highly confidential information *(hereinafter referred to as confidential),* such as protected health information (PHI), as defined by the Health Insurance Portability and Accountability Act, and other information designated by this organization or by law as confidential or highly confidential. It applies to such information in any form (written, electronic, oral). It applies to our workforce and to third parties granted access to our PHI and other confidential information.

4. *General Rules*

Confidential information shall be protected according to the following general rules. Refer to specific policies and procedures for additional details.

- When feasible for responding to a request for or providing access to data, nonconfidential data will be provided instead of confidential data. For example, de-identified data will be provided instead of personally identifiable data. This applies to any purpose, including data analysis, research, software development, testing, and training. However, whenever confidential data is required (e.g., for patient care, payment for services, or regulatory reporting), it will be provided. These rules are not intended to interfere with performance of one’s duties for this organization or with the fulfilling of this organization’s mission or legal and regulatory obligations.

ABC Organization	
Policy Name: Confidential Data Protections Policy	**Effective Date:** 1/1/05
Sponsor: Information Security Officer	**Date Last Reviewed:** 1/3/11
Document Number: IS 2	**Date Obsolete:**
Revision History: Author and Description	**Revision Date:**

- Access to confidential data is restricted to those with a business need to know, as defined by organization policy and procedure. Access to and disclosure of confidential information is permitted only when required to perform an individual's work for this organization or to satisfy an approved third-party request.
- Access to confidential data and protected resources requires written approval from an authorized source (typically the system "owner" and/or the user's management). Unauthorized access to confidential information is a violation of organization policy. (Federally defined "incidental" and unavoidable access/disclosure of PHI is an exception to this policy.) Authorization is required for network and remote access also, because confidential data resides on our interconnected network.
- Written access authorization for confidential electronic resources will be kept on file for the duration of the individual's access plus three months, at a minimum, and longer if required by this organization's retention policy. (For example, documentation of access to PHI should be retained for six years.)
- Access to and disclosure of confidential information must be role based and limited to the minimum necessary to perform an individual's job or to satisfy the purpose of a disclosure, given reasonable technical or other limitations. When access is electronic, access also will be limited to the minimum level of functionality (e.g., read-only access instead of update) required for the individual's work. The minimum-necessary principle will never be invoked to interfere with patient care or a patient's right to access his/her own information.
- Access to electronic confidential information will be granted only through a unique user ID and a form of authentication meeting organization standards (e.g., a password of the required minimum length and composition). Generic user IDs are not permitted except under very limited circumstances, and exceptions must be approved in writing by the Information Security Officer. User IDs will not be reissued. Users may not share their unique user IDs and authentication with anyone else, and users must not permit others to use their access even if the ID and authentication are not shared. Users are required to protect their IDs and authentication from accidental disclosure or use by anyone else. If and when multifactor authentication is required by organization standards, users must comply.
    - In some cases, a biometric form, such as a fingerprint, or a physical token, such as an RF ID card/badge, will serve as either a unique user ID or a form of user authentication but not both.

ABC Organization	
Policy Name: Confidential Data Protections Policy	**Effective Date:** 1/1/05
Sponsor: Information Security Officer	**Date Last Reviewed:** 1/3/11
Document Number: IS 2	**Date Obsolete:**
Revision History: Author and Description	**Revision Date:**

- Access to electronic confidential information will be reviewed (semiannually at a minimum) by management (i.e., by system "owners" and certain managers) to ensure that access by every user is currently appropriate and authorized.
- Physical and electronic access to confidential information will be halted promptly when anyone (workforce member or third party) with access no longer needs it for this organization's business purposes. This applies to job changes as well as to terminations. When the organization believes there is heightened information security risk associated with an individual's termination, removal of physical and electronic access to facilities and resources will be processed immediately upon notification.
- Unless it is a routine function of one's job, copies of confidential information in any form may not be made unless written permission is granted from an authorized source, such as the system owner or privacy officer. Permissions must be kept on file for a minimum of six years.
- Unless it is a routine function of one's job, confidential information in any form may not be removed from the organization's premises without explicit written permission and signed agreement to maintain additional security protections required off-site. (Refer to separate policies, procedures, and guidelines governing working offsite for further details.) Permissions and agreements must be retained for a minimum of six years.
- Access granted to an electronic database (typically through a system, such as an electronic health records system) or a records room shall not be construed as permitting access to all records contained in the system/database or records room. Access is permitted only to those specific records needed for performance of one's job.
- Access granted to electronic systems containing confidential information will be monitored and audited when and as technically feasible for the protection of the data and the organization's assets. Use of these systems acknowledges that activity will be monitored.
- Confidential information in any form will be physically protected through reasonable measures (e.g., locks on devices, locked server and storage rooms, private conversations).
- Confidential information in any form will be destroyed prior to disposal or as part of the disposal process (e.g., paper cross-cut shredding). Confidential information will continue to be protected while awaiting disposal. When destruction is performed by a third party, the organization will obtain certification of the destruction and/or destruction will occur on this organization's premises. Confidential information will be removed from all

- computers and magnetic and optical media used for organization business, regardless of device or media ownership, prior to reuse and prior to a workforce member's termination. Disposal and reuse techniques will follow organization procedures.
- Confidential information backup, transport, transmission, storage, and other handling processes will follow specific policies and procedures on these topics.
- Disclosure of confidential information, in any form, for other than this organization's purposes is prohibited, including following termination of an individual's business relationship with this organization. In special cases, written authorization for a particular disclosure may be granted by the CEO or designee.
- All workforce members, including senior management, are required to participate in privacy and security training on responsibilities for protecting confidential information. Training will occur prior to, or as soon as possible after, being granted access to confidential resources, and annually thereafter. Individuals will be required to sign the Security and Privacy Agreement at the conclusion of each training session. Additional specialized privacy and security training will be provided as needed (e.g., to department heads). Workforce members will have access to all information about security and privacy policies and procedures needed to perform their jobs in a privacy- and security-conscious manner.
- The organization's Sanctions for Privacy and Security Violations policy will be followed when violations of this and/or any other privacy and security policies and procedures occur.

5. *Monitoring and Enforcement*

The information security officer is responsible for monitoring and enforcement of this policy, with the assistance of the privacy officer. However, management and individuals share responsibility for understanding and following this policy and for reporting all suspected and actual breaches of this policy. Specifically, managers are responsible for monitoring workforce and, when reasonable, sponsored users' behavior in terms of information security and privacy and ensuring that wherever confidential information is accessible, all individuals are either authorized for access to that information or they are supervised.

6. *Penalties*

See Sanctions for Privacy and Security Violations policy. Note that sanctions apply to the full workforce and are not limited to employees. Sanctions may include immediate termination of work relationship and may lead to revocation of professional license and to civil and criminal legal action.

7. ***References***
   See Glossary of Terms for definitions of PHI, workforce, and confidential data.

8. ***Approval***
   General Executive Committee, December 30, 2004

9. ***Review Cycle***
   Annual

Title: Security of Portable Computers and Media

Policy: Portable computers and portable electronic media containing or used to access this organization’s confidential data will be protected from unauthorized access through this policy’s security controls. This policy is intended to supplement, not countermand, other information security policies for the special case of portable equipment and media.

Purpose: Portable computers and portable electronic media are at greater risk of loss and theft than nonportable items. Therefore, when they contain confidential information or can be used to access such information, that information could be compromised by unauthorized access. There is not only a potential loss of privacy and confidentiality of the data on the device or media, but also, if the device is used (directly or indirectly, such as when a password is stored on a PDA) to gain access to this organization’s network and other protected resources, the security of all information assets could be at greater risk. Hence, the additional security controls in this policy are appropriate and necessary to contain the risk.

Scope: This policy applies to our workforce and any third parties who are authorized to have access to any information this organization designates as confidential or highly confidential (including protected health information, employee records, etc.) and who use portable computers to access or store our confidential data and/or who remove confidential data from the facility on magnetic media.

This policy applies both when the organization owns the device or medium and when it does not, as long as the organization's confidential data are accessed through or stored on the device or medium.

Examples of portable computers include laptop computers, tablets, and handheld devices (PDAs, pager/cell phones with storage and processing capability). Examples of portable media include disks, CDs, some MP3 players, and USB drives, storage devices, and thumb drives.

General rules:

1. *Inventory of Portable Computers*

   The Information Security Department (ISD) will create and maintain an inventory of portable computing devices (including both organization owned and personally owned) used to access and/or store organization confidential data. Departments will be responsible for reporting new devices and changes to ISD promptly.

   This inventory will give the ISD information about how portable computers are being used with respect to confidential data. Based on review of that information, the ISO may mandate additional security controls and specific security software.

2. *Authorization*

Individuals must be authorized in writing (sent to the ISD) by management prior to removing confidential information on electronic media or computer and prior to accessing or storing confidential information on a portable computer.

3. *Authentication*

Access to portable computers requires at least one form of authentication, such as a password or a fingerprint. Passwords must meet organization standards for password length, composition, and expiration.

4. *Virus Protection*

Virus protection software should be installed on the portable device and routinely updated.

5. *Encryption*

Encryption software should be installed on the device and used to protect any confidential data on it. Encryption software that meets organization standards and government-endorsed algorithms should be used to encrypt data on portable media leaving the facility.

6. *Locking*

Portable devices must be kept locked (for example, in a drawer or briefcase) unless they are in use or on one's person. Portable media must be locked when unattended (other than in a locked private office) and when removed from the facility.

Off –Site User Device Inventory

Owned By	User Name	Department	Telephone	Device	How Used

ABC Organization	
Policy Name: Encryption of Confidential Information	**Effective Date:** 1/1/05
Sponsor: Information Security Officer	**Date Last Reviewed:** 1/13/11
Document Number: IS 3	**Date Obsolete:**
Revision History: Author and Description	**Revision Date:**

1. *Policy*

All organization confidential and highly confidential electronic information must be encrypted (a) when transmitted over unsecure networks, including the Internet and wireless, and (b) when at rest on portable computing devices and portable/removable electronic media.

2. *Purpose*

The Internet is an open, public communications medium. Wireless signals travel through air and cannot be entirely contained in normal business settings. Messages and data transmitted over these networks are not secure. Portable devices and media are easily lost and stolen, jeopardizing confidential data stored on them. Therefore, this organization must protect the privacy and confidentiality of our patients, our employees, and our business matters by requiring that confidential information be encrypted in these high-risk circumstances.

3. *Scope*

This policy applies to all organization electronic information designated as confidential and highly confidential (hereafter referred to as confidential) data. It applies to such data transmitted over the Internet and wireless networks. This policy applies to all users transmitting confidential data over those networks. This policy applies to any and all mechanisms by which organization data may be transmitted over wireless networks and the Internet, such as file transfer, email and email attachments, website transactions, and interactive sessions.

This policy also applies to portable computing devices, such as laptops and handheld personal digital assistants (e.g., iPhone™, BlackBerry™), and to portable electronic media, such as CDs, DVDs, MP3 players, and USB drives.

This policy sets a minimum requirement. It is not intended to prevent or discourage use of encryption under other circumstances, particularly when it has been determined that an appreciable risk exists.

ABC Organization	
Policy Name: Encryption of Confidential Information	**Effective Date:** 1/1/05
Sponsor: Information Security Officer	**Date Last Reviewed:** 1/13/11
Document Number: IS 3	**Date Obsolete:**
Revision History: Author and Description	**Revision Date:**

4. *General Rules*

The Information Security Department will specify standards, acceptable methods, and technical tools for encryption in different circumstances. For example:

- Virtual Private Network (VPN) for staff–corporate connections
- Secure FTP for file transfer
- SSH for system administration
- SSL for website transactions
- Secure email product
- WPA for wireless transmission
- Laptop hard disk encryption

The Information Security Department will choose particular tools based on government-endorsed symmetric and asymmetric algorithms and minimum keylengths. When appropriate, users will receive training in use of encryption tools.

7. *Monitoring and Enforcement*

The information security officer (ISO) is responsible for monitoring and enforcing this policy. However, managers and workforce members are responsible for ensuring compliance with this policy. If in doubt about whether an activity is subject to this policy, consult with the ISO.

8. *Penalties*

See the Sanctions for Privacy and Security Violations policy.

9. *Related Information*

8. *Approval*

9. *Review Cycle*

Annual

Disposal Policy Statement

All confidential materials, in any medium (e.g., electronic, optical, paper), must be destroyed, or in the case of non-paper media, their contents erased, when the data are no longer required for business purposes, and following the expiration of any retention period required by law, regulation, or organization policy.

Temporary suspension: Destruction will be suspended for records involved in any open audit, investigation, or legal action.

Re-use: Confidential data must also be erased from electronic or other non-paper media before the computing and/or storage device may be reused for a different purpose or by a different user.

Methods: Destruction/disposal/erasure techniques must meet organization standards and acceptable security practices. Paper, film, or other hard copy media must be shredded or destroyed such that the data cannot be read or otherwise reconstructed. Electronic media must be cleared or destroyed according to NIST Special Publication 800-88, *Guidelines for Media Sanitization*, so that the data cannot be retrieved.

ABC Healthcare Organization	
Policy Name: Off-Site Computers and Media Security	**Effective Date: 1/10/12**
Sponsor: Information Security Officer	**Date Last Reviewed: 1/10/12**
Revision History—Author and Description:	**Revision Date:**

1. Policy

Working off-site and working with portable computing devices and media carry greater information security risks than working in our facility. Therefore, when used off-site, stationary workstations, portable computing devices (e.g., laptop computers, PDAs, and smartphones), and portable electronic or other media used to store and/or access this organization's confidential data must be protected from unauthorized access, disclosure, damage, or loss through heightened administrative, physical, and technical controls.

To ensure that individuals recognize the increased risk and their responsibility, individuals who work off-site with this organization's confidential information, even occasionally, must sign a Working Off-Site Security Agreement. Further, if work is performed in a fixed location, such as a home or small office, individuals must agree to permit an on-site review, if and when this organization undertakes such reviews, with advance notice, to verify compliance with security policies and procedures.

This policy is intended to supplement other information security policies for the special case of working off-site with both portable and nonportable equipment and media.

2. Purpose

This organization is responsible for protecting the confidentiality, integrity, and availability of our confidential data wherever it is. For example, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule explicitly makes us responsible for safeguarding protected health information (PHI) wherever it is used by our workforce.

Personally owned workstations, portable computers, and portable storage media used for our business purposes off-site are subject to specific risks not present on-site. Portables are at greater risk of loss and theft than nonportable items. Personally owned workstations used for business are typically also used for personal reasons that could compromise this organization's data and systems. Either could be used in a home or public setting, where numerous physical and technical risks exist. Therefore, when they contain confidential information, that information could be compromised by unauthorized access. It could also be altered or destroyed through unauthorized actions.

There is heightened risk to the data on the device or media. Also, if the device is used to access this organization's network and other protected resources, the security of all information assets could be at greater risk. Unsecure devices can be used for unauthorized access (e.g., when a password is stored on a laptop computer or no device authentication is required) and can introduce malware. Hence, the additional security controls in this policy are appropriate and necessary to contain the risks.

ABC Healthcare Organization	
Policy Name: Off-Site Computers and Media Security	**Effective Date: 1/10/12**
Sponsor: Information Security Officer	**Date Last Reviewed: 1/10/12**
Revision History—Author and Description:	**Revision Date:**

3. *Scope*

This policy applies to our workforce and any third parties who are authorized to have or to access any information this organization designates as confidential or highly confidential (e.g., PHI employee records) and who work off-site using workstations or portable computers to access or store our confidential data and/or who remove confidential data from this organization.

This policy applies both when the organization owns the device or medium and when it does not, as long as our confidential data are accessed through or stored on the device or medium.

This policy applies to any user computing device. This includes workstations, such as personal computers, in homes. It includes portable computers, such as, but not limited to, laptop computers, tablets, and handheld devices (e.g., PDAs, pagers, and smartphones with storage and processing capability).

This policy also applies to portable media of all forms, including paper. Examples of portable electronic media include external hard drives, CDs, MP3 players, SD cards, and USB drives.

This policy (particularly the inventory, encryption, and physical security controls) also applies to portable electronic storage, including backup tapes and cartridges, and records being archived.

4. *General Rules and Procedures*

a. Inventory of Portable and Other Computing Devices and Electronic Media
The IT department will create and maintain an inventory of computing devices used to access and/or store this organization's confidential data off-site. The inventory includes both organization-owned and personally owned devices. Devices include desktop workstations, laptop computers, tablets, smartphones, and any other user-computing device. Individuals are responsible for reporting new devices, replacements, and inventory information changes promptly. IT will also track portable electronic media, such as USB drives.

The inventory will give the information security officer (ISO) information about how these devices are being used off-site with respect to confidential data. Based on review of this information, and/or on new risks, the ISO may mandate additional security controls and specific security software.

Upon termination, or when the computing device or medium is no longer needed, organization-owned devices and media must be returned to the organization, wiped clean, and returned to inventory. Upon termination, personally owned computing devices and media must be wiped clean of organization data and organization-licensed software, if any, and the user must signed a statement acknowledging that all data and software have been removed according to organization secure erase standards. Organization-issued storage media must be returned, physically destroyed, or wiped clean using acceptable secure erase software.

b. Authorization and Acknowledgement
Individuals must be authorized in writing by management prior to working off-site if doing so entails a remote connection to the organization's network or if it entails accessing and/or storing any confidential data on an off-site or portable device or media. Note that authorization is required even if there is no need for a remote connection to this organization's private network.

Individuals must sign an acknowledgement of their security responsibilities and to permit announced site visits for a security review, if and when the organization performs them. Additionally, individuals must agree to permit this organization to remotely lock and/or wipe contents from portable devices with this capability when a risk exists. This may include, but is not limited to, when the device is stolen and when there are a given number of consecutive unsuccessful logon attempts [organization-specific setting, e.g., five]. Finally, individuals must agree that computing devices used for work purposes must not be shared with others, regardless of device ownership.

c. User Identification, Authentication, and Access Control
Access to personal computing devices used for this organization's work requires a unique user ID. Exceptions may be permitted for certain devices, such as smartphones. The device may not be shared with another individual unless approved by this organization.

Access to the device requires at least one form of user authentication, such as a password, PIN, or fingerprint. Passwords and other forms of authentication must meet organization standards. Passwords that are also used as encryption keys must be longer passphrases (e.g., 20 characters) that meet organization standards. Passwords and passphrases are secret; they may not be shared and they may not be saved on the device.

Devices containing confidential data or that are used to access confidential data may not be left logged on and unattended. The user must log off or "lock" the device so that re-authentication is required to use the device.

Portable devices, such as laptop computers, tablets, and smartphones used for business purposes, must be centrally controlled by this organization to permit, for example, remote locking and/or wiping in case of loss or theft. This applies regardless of device ownership.

d. Inactivity Timeout

Devices must be configured to automatically time out or terminate the session after a short period of inactivity [to be determined by the organization]. Note that this is intended as a safety net and does not relieve the user of the responsibility to lock or log off before leaving a device unattended.

Remote access to the organization network will time out after a designated period of inactivity [determined by the organization]. This may be set in a VPN connection or SSL connection through a website where user re-authentication will be required for an application to continue.

e. Software

The IT department will develop and maintain configuration standards to be followed. Users generally are not permitted to modify organization-owned devices, and they are required to maintain personally owned devices in accordance with this policy.

Downloading software apps from the Internet should be done with great care, particularly on smartphones, and only when the source is reliable. IT will maintain a list of approved applications.

Virus protection and antimalware software must be installed on devices, updated promptly when security updates are available, and configured to scan vulnerable components. Use of a personal device firewall is also required. Security updates to operating systems, browsers, and applications must be promptly applied to devices.

File sharing software must not be installed or enabled.

f. Encryption

All portable computing devices (e.g., laptop computers) and portable electronic media (e.g., USB drives) used for organization work must be encryption-enabled to protect stored organization confidential data. Consult IT for assistance.

Only National Institute of Standards and Technology (NIST)–endorsed algorithms, such as AES, may be used. Decryption keys must be stored separately from the device or media and kept confidential. IT will provide key escrow services when appropriate.

When a device is connected to a network (wired or wireless), and any portion of the connection is over the air, the Internet, or a network not under the control of this organization, transmission must be encrypted. This can be accomplished with standard technologies (e.g., IPsec VPN, SSL/HTTPS, Secure Shell, secure FTP). Wireless networks, including home networks, must be configured with WPA2 or higher.

g. File Backup
If off-site data are unique source data that could not be recreated and are important to this organization's operations, it must be backed up to a secure file server on the network.

h. Physical Protections
Whether using a desktop computer or a portable device, it should be set up or used in a private area where access to the device is restricted. In all cases, users must be aware of their surroundings and must protect screens from view by others. Devices should have privacy screens (e.g., filters or films) unless the device is a desktop computer in a private office.
Logged-on devices must never be left unattended if anyone else is or may be in the vicinity. Note that disk encryption does not provide protection when the user is logged on.

Portable devices must be kept logged off and physically locked up (e.g., in a locked drawer or locked briefcase) unless they are in use or on one's person. Media of any type (e.g., electronic, paper) containing confidential information must be locked securely when unattended.

When transporting portable computing devices and/or media containing confidential data, the items must be on one's person or logged off, locked up, and out of sight. For example, a laptop computer and work papers left in a parked vehicle or a hotel room must be in a locked case and hidden out of sight. Locks are not foolproof, but they are an important deterrent to theft. In vulnerable circumstances, portable devices and media should be kept with the responsible individual.

When portable media in any form are transported by or for a department (e.g., for record archiving, for data backup and restore, and similar purposes), the media must be in a locked case. When media containing confidential data are stored off-site, they must be in locked containers unless an exception is authorized in writing by the privacy officer or ISO.

i. Disposal
When files containing confidential data are no longer needed, follow organization policy and procedures for safely disposing of the information. Seek assistance from IT, if necessary, to thoroughly erase or destroy electronic data. All paper containing confidential data must be cross-cut shredded.

j. Loss or Theft
Users must promptly [insert organization's standard, e.g., within one day] report the loss or theft of any device or media that may contain confidential information to [insert organization-specific system or office, e.g., the Help Desk]. This event will be treated as a privacy/security incident to be immediately triaged and investigated. If appropriate, the IT department will remotely lock and/or wipe contents from the device.

5. Monitoring and Enforcement
The ISO is responsible for monitoring and enforcing this policy. However, managers and each member of this workforce also share responsibility for ensuring compliance with this policy and reporting violations.

6. Penalties
Refer to the Sanctions for Privacy and Security Violations policy.

7. Related Information
Refer to the Off-Site User Device Inventory form. Refer to the Glossary for definition of confidential data.

8. Approval Jane Doe, CEO
9. Review Cycle
Annual

Working Off-Site
Security Agreement

I acknowledge that I have read and will abide by ABC Organization's information security policies, as applicable to me, including the Off-Site Work Security policy (a copy of which I have received). I agree to protect ABC Organization's confidential data, in any form, when I am accessing and/or using it while away from the facility. Further, I agree to a security audit of my off-site work location if and when requested by ABC Organization.

Name: ____

Signature: ____

Date: ____

Please return this form to the Information Security Officer, ABC Organization