Template for a Comprehensive Health Care Information Protection Agreement

Date: May 25, 2001
Author: John R. Christiansen
Stoel Rives LLP
206.233.5930
jrchristiansen@stoel.com

NOTE: THIS PREPUBLICATION DRAFT HAS BEEN LICENSED FOR LIMITED DISTRIBUTION PENDING PUBLICATION OF THE FINAL VERSION BY HEALTHKEY IN JUNE 2001. PLEASE CONTACT THE AUTHOR TO RECEIVE THE FINAL VERSION.

Introduction

This Agreement was developed to provide a contractual framework for the protection of private information in the course of electronic transactions among health care organizations, as part of the HealthKey program. The HealthKey program was funded in 1999 by the Robert Wood Johnson Foundation, to encourage privacy practices and market-based pilots focussed implementing information security infrastructures for the health care market.

In the course of pilot activities in the State of Washington, it became apparent that one of the obstacles to private and secure exchange of patient identifiable health information was the lack of generally acceptable contract forms. Emerging laws for the protection of information and good risk management principles call for such contracts where parties are exchanging private or other sensitive information, especially when using electronic transactions. This Agreement was therefore commissioned to support health care infrastructure pilot activities, and circulated to a number of parties involved for their review. The Agreement which follows incorporates insights and suggestions which arose during this process.

While this Agreement is intended to suggest provisions or strategies which may be useful for most health care organizations, in most if not all transactions involving protected information, it should not be adopted without prudent analysis of its applicability to parties' actual needs and intention. Many provisions presume the implementation of information protection policies and procedures which are required by law or are good risk management practice, and it is important to ensure that provisions which are adopted will in fact be followed.

The comments included with this Agreement are intended to support legal analysis, but are not legal advice. It is strongly recommended that any organization considering adopting this Agreement or any of its provisions conduct an independent legal review and assessment of its application before adoption.

Scope of the Agreement

The primary purpose of this Agreement for Disclosure and Protection of Information is use as a template for standardized terms, where one or more parties to a transaction involving the exchange of individually identifiable health information is required to comply with the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1] as a "Covered Entity."[2] However, HIPAA is only one of a number of overlapping laws concerning the privacy and protection of personal information, at both the federal and state levels. This Agreement is therefore also intended to allow the parties to take other such laws into account as they may be applicable.

In particular, this document is intended to comply or allow for compliance with the following requirements:

- The Agreement includes all provisions the HIPAA Privacy Rule requires a Covered Entity to obtain before disclosing Protected Health Information[3] to a "Business Associate,"[4] as a "satisfactory assurance that the Business

---

[1] As used in this document, "HIPAA" refers to Title II subtitle F ("Administrative Simplification") of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (August 21, 1996), enacting sections 1171 – 1179 of the Social Security Act, as well as implementing regulations adopted by HHS pursuant to HIPAA.

[2] A "Covered Entity" is any health plan or health care clearinghouse, and any health care provider "who transmits any health information in electronic form in connection with a transaction covered by" HIPAA. See United States Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information; Final Rule," 65 Fed.Reg. 82,462 (December 28, 2000)(publishing final regulations codified as sections of 45 CFR Parts 160 and 164)("Privacy Rule"), at 82,798 – 799, 45 CFR sec. 160.102(a), .103 (definition of "covered entity"). See also United States Department of Health and Human Services, "Security and Electronic Signature Standards; Proposed Rule," 63 Fed.Reg. 43,242 (August 12, 1998)(publishing proposed regulations to be codified as sections of 45 CFR Part 142)("Draft Security Rule"), at 43,264, proposed 45 CFR sec. 142.102(a), .103 (definitions of "health care clearinghouse," "health care provider" and "health plan"), and United States Department of Health and Human Services, "Health Insurance Reform: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organizations; Final Rule and Notice," 65 Fed.Reg. 50,312 (August 17, 2000)(publishing final regulations codified as sections of 45 CFR Parts 160 and 162)("Transactions Rule"), at 50,365, 45 CFR sec. 160.102, .103 (definition of "covered entity").

[3] "Protected Health Information" is defined as "individually identifiable health information" which is "transmitted or maintained" in any oral, written or electronic medium, excluding only certain educational and college student mental health records. See Privacy Rule at 82,805, 45 CFR sec. 164.501 (definition of "protected health information"). "Individually identifiable health information" is defined by HIPAA as "any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present, or future physical mental health of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and identifies the individual[,] or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." See HIPAA sec. 1171(6).

[4] A "Business Associate" is "a person or entity" which is not an employee, trainee or volunteer under direct supervision of a Covered Entity, which "performs, or assists in the performance of" any "function or

Associate will appropriately safeguard the information" ("Business Associate Contract)."[5]

- The Agreement includes the provisions required for the "chain of trust partner agreement" required of Covered Entities as an "appropriate security measure" to "manage the selection and execution of security measures to protect data" in the Draft HIPAA Security Rule ("Chain of Trust Agreement").[6]

- The Specifications Addendum to this Agreement is intended to serve as the "trading partner agreement" contemplated for use by Covered Entities under the Transactions Rule, which "may specify, among other things, the duties and responsibilities of each party to the agreement in conducting standard transaction [sic]." ("Trading Partner Agreement").[7]

- The Agreement can be used to establish compliance with the Health Care Financing Administration ("HCFA") Internet Security Policy. This policy establishes requirements for the encryption and authentication of federal Privacy Act-protected information transmitted by HCFA agents, contractors, Medicare and Medicaid beneficiaries and other HCFA-related parties.[8]

---

activity" on behalf of the Covered Entity. See Privacy Rule at 82,798 and 82,800, 45 CFR sec. 160.103 (definitions of "Business Associate" and "workforce").

[5] Privacy Rule at 82,806, 45 CFR sec. 164.502(e)(1)(i). This agreement is not required for disclosures to health care providers "concerning the treatment of [an] individual[,]" to health plan disclosures to plan sponsors under certain conditions, or to certain government program health plan transactions. Id. At 45 CFR sec. 164.502(e)(1)(ii). The Privacy Rule requires a number of specific kinds of provisions, described in the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2) – (3). See Privacy Rule at 82,806, 45 CFR sec. 164.502(e)(2).

[6] The Draft Security Rule defines this as "a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged." Draft Security Rule at 43,266, proposed 45 CFR sec. 142.308(a)(2). A Chain of Trust Agreement therefore overlaps but is not coextensive with the Business Associate Contract, since (a) a Covered Entity must have a Chain of Trust Agreement to protect data being disclosed, whether or not the receiving party fits the definition of a Business Associate, while (b) the Chain of Trust Agreement, at least as set forth in the Draft Security Regulation, is required only in the context of electronic data exchanges, while Business Associate Contracts are required regardless of the medium in which Protected Health Information is disclosed.

[7] Transactions Rule at 50,366, 45 CFR sec. 160.103 (definition of "trading partner agreement"). The only specific requirements stated for Trading Partner Agreements in the Transactions Rule is a prohibition on Covered Entities agreeing to materially deviate from the required transactions standards. See Transactions Rule at 50,369, 45 CFR sec. 162.915.

[8] Bulletin, "Internet Communications Security and Appropriate Use Policy and Guidelines for HCFA Privacy Act-protected and Other Sensitive HCFA Information, Health Care Financing Administration (November 24, 1998)("HCFA Internet Security Policy"). Presumably, the requirements of this policy will be subsumed under and superseded by the final HIPAA security rule. The policy will remain in effect until superseded by that final rule, or by a subsequent HCFA publication.

- One or more parties may be required to comply with the Gramm-Leach-Bliley Act ("G-L-B") because it is a "financial institution," a category which in some states includes health plans.[9] G-L-B compliance includes a requirement that a financial institution may only "provide nonpublic personal information to a nonaffiliated third party to perform services" on its behalf if it has (a) provided an appropriate notice to its customers, and (b) entered into "a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which [the financial institution] disclosed the information[.]"[10] ("G-L-B Agreement").

- Parties may also use this Agreement to support their compliance with state privacy and confidentiality laws which may apply. However, the Agreement has been drafted to account for generally accepted privacy principles which state laws tend to follow. These may vary in material details from the general principles, and so need to be checked against this Agreement to ensure it is appropriate in all applicable state jurisdictions.[11]

- This Agreement will support the use of electronic signatures and electronic records if the parties wish to use them. It incorporates optional provisions consistent with both federal and state laws covering these areas.

The Agreement also includes provisions concerning information ownership and certain customary contract provisions, so that it can serve as a comprehensive resource for health information transaction contracting.

---

[9] The Gramm-Leach-Bliley Act, Pub.L. No. 106-102 (1999) imposes a number of privacy requirements on "financial institutions," to be implemented by regulations promulgated by federal banking authorities, the Federal Trade Commission and state insurance regulators. See United States Department of the Treasury, "Privacy of Consumer Financial Information; Proposed Rule," 65 Fed.Reg. 8,771 (February 22, 2000) at 8,789 – 8,796 (Office of the Comptroller of the Currency, proposed provisions of 12 CFR secs. 40.1 – 40.16), 8,796 – 8,802 (Board of Governors of the Federal Reserve System, proposed Regulation P, proposed provisions of 12 CFR secs. 216.1 – 216.6), 8,802 – 8,809 (proposed provisions of 12 CFR secs. 332.1 – 332.16) and 8,809 – 8,816 (proposed provisions of 12 CFR 573.1 – 573.16); and United States Federal Trade Commission, "Privacy of Consumer Financial Information; Final Rule," 65 Fed.Reg. 33,646 (May 24, 2000)("FTC Rule"). The various federal rules are materially the same, so for the sake of simplicity only the FTC Rule will be cited or discussed below. A number of states have been implementing Gramm-Leach-Bliley by passing legislation or promulgating regulations which apply to health plans as well as other insurers. See e.g. Washington Administrative Code ("WAC") 284-04, "Privacy of Consumer Financial and Health Information".

[10] FTC Rule 313(a)(1)(ii); and WAC 284-04-400(1)(a)(ii).

[11] This Agreement was drafted in contemplation of the Uniform Health Care Information Act of the State of Washington, Revised Code of Washington ("RCW") 70.02. This act is generally consistent with common law principles adopted by caselaw and with statutes enacted in most other states, as well as ethical confidentiality and other information protection requirements applicable to physicians, health care providers and health plans in general.

Crosswalk of Provisions

This Agreement is accompanied by a "crosswalk," a matrix mapping the various provisions to relevant legal sources. This crosswalk is intended to assist users in determining the purposes and uses of various provisions.

Structure of the Agreement

The Agreement is based on a distinction between the roles of "Disclosing Party" and "Receiving Party." Each role has a different set of obligations derived from their different relationship to Protected Information in an exchange. Covered Entities may be in either or both roles. However, it is not required that any party be a Covered Entity.

The Agreement is intended to identify relationships to Protected Information and allocate privacy and security obligations at a general enough level that it is neutral as to the specific solutions adopted by the parties. As with the HIPAA Privacy and Draft Security Rules, the Agreement identifies obligations which must be met but leaves the specific policies, processes, procedures and technologies used to the parties' informed judgment. It does require that each party communicate and coordinate with the other about elements of its Privacy and Security systems and processes which might affect the other party's own contractual performance.

The effect of the allocation of privacy and security obligations should be both to clarify what each party is responsible for, and allocate liability if Protected Information is improperly used or disclosed. The Agreement incorporates warranty and indemnification provisions, based on standard provisions, which enforce the allocation of liability.

The Agreement includes provisions specifying ownership rights in Protected Information that are not required by HIPAA, but are intended to avoid situations in which a party might be able to place information beyond its privacy protections. For example, a party which is legally considered the "owner" of information may be entitled, or even required to disclose or sell such information in some kinds of court proceedings.[12]

The format of the Agreement calls for two cross-referential documents, the Agreement itself and a "Specifications Addendum." The Specifications Addendum is the operational core of the Agreement. Where the Agreement is essentially general, the Specifications Addendum provides specifics about the Information to be exchanged; the Purposes, Uses and Disclosures which may be made of it; Formats and methods for Transmission of information; and any additional protective standards the parties may wish to incorporate. This format allows parties to adopt the Agreement, and amend or modify operational terms in the Specifications Addendum without renegotiating the Privacy and Security provisions of the Agreement. The Agreement nonetheless provides a mechanism for initiating renegotiations if necessary or desirable.

Outline of Agreement

The Agreement is divided into the following sections:

- *Recitals*.   This section formally identifies the parties and states their intent to protect information.

- *Interpretation of this Agreement*. This section includes definitions of key terms, and other principles for interpretation of the Agreement.

- *Standards for Transactions*.   This section states the requirements for Specifications Addenda and Transactions.

- *Information Protection Obligations of Disclosing Parties*.   This section identifies the information protection obligations of Disclosing Parties *under this Agreement only*. This section is not intended to be a comprehensive guide to HIPAA or other information privacy or protection compliance by such parties, but only to specify their obligations as they affect Receiving Parties. A Disclosing Party which is a Covered Entity will be subject to many more obligations than those identified in this Agreement.

- *Information Protection Obligations of Receiving Parties.*   As in the section pertaining to Information Protection Obligations of Disclosing Parties, this section identifies obligations *under this Agreement only*. These obligations are more detailed and specific than those applicable to Disclosing Parties, principally because of the need to address specific Business Associate contracting requirements imposed by HIPAA.

- *Privacy Practices.* As used in this document, "privacy practices" are policies, procedures and documentation adopted for interaction with the individuals who are the subjects of Protected Information. These principally include notices specifying how information may be used or disclosed, forms for consent to and authorization of information use or disclosure, and procedures for review, copying and amendment of information. Because various kinds of parties may have different kinds of relationship to individuals, their legal privacy practice obligations may vary. In order to accommodate the diversity of obligations, this section does not impose mandatory practices, but requires parties to share their materials and ensure that their own are consistent with their obligations under the Agreement.

---

[12] See Winn and Wrathall, "Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data," 56 **The Business Lawyer** 213 (November 2000) at 256-59.

- *Information Ownership.* This section presumes that Protected Information is owned by the Disclosing Party, while giving the Receiving Party limited rights to possess, use and disclose it.

- *Return, Archiving and Destruction of Information.* This section controls what happens to Protected Information when the Receiving Party is no longer entitled to use or disclose it.

- *General Warranties and Indemnification.* This is intended to provide for standard warranties of performance and allocate risk.

- *Dispute Resolution.* This section pertains only to judicial dispute resolution. It is recommended that the parties include less formal alternatives, but no specific process is provided.

- *Term and Termination.* This section provides for the termination of the Agreement. Since more than two parties may participate, the provisions allow one party to opt out of the Agreement, while keeping it effective as to those who remain.

Use of the Agreement

Health care organizations frequently need to both Disclose Protected Information to their business partners, and Receive such information from them. This may entail a return of information previously disclosed by the organization but processed into a different format or commingled with information from other sources, the transfer of Protected Information never before disclosed to the party, and so on.

In this context the Agreement itself functions to define consistent information protection obligations based upon the role each party plays with respect to any given Disclosure of Protected Information, while the Specifications Addendum lets the parties differentiate such matters as Formats and means of Transmission and Authentication if necessary. This may be clarified by examples.

Example 1:   Two Parties, Multiple Types of Information

In an example demonstrating the use of this Agreement between only two parties exchanging more than one kind of information, consider a hospital which needs to exchange both clinical and claims-related information with a clinic. For operational reasons the data may be created and transmitted by different systems, and customized security precautions may be desirable for some kinds of clinical data such as mental health records.

The parties could initially establish one set of Specifications Addenda for exchange of claims information (one addendum for each party, pertaining to the different

roles each plays with respect to information). Subsequently, they may decide to exchange clinical data which for operational reasons cannot be Transmitted by the same means or in the same Formats as the claims data. The parties could either amend the existing addenda to include the new specifications, or preferably enter into new addenda specific to the clinical information.

<u>Example 2:   Multiple Parties, Single Data Type.</u>

For an example demonstrating the use of this Agreement among multiple parties exchanging the same type of data, consider a hospital which needs to Transmit claims data to health plans and affiliated physicians by means of a network established by a health care clearinghouse. The hospital, health plans, health care clearinghouse and physicians could all adopt the Agreement by incorporating it by reference in the various Specifications Addenda they establish. The hospital would then have a separate Specifications Addendum with each health plan and physician, each physician would have a separate addendum with each plan with which she exchanged information, any party using the health care clearinghouse would have a separate addendum with it, and so on.

In this situation all the parties in the network would accept a standard set of obligations. Since this acceptance would be effective only in connection with an exchange of information pursuant to a Specifications Addendum, a party's obligations and liability for performance would only be triggered if and to the extent that it Disclosed Protected Information to or Received it from the other party to a Specifications Addendum. In other words, the Agreement would not function as a contract under which each party might be liable to all others, or might be liable for acts of other parties, but would instead create a network of standardized contracts following the paths along which the parties agreed to exchange information. Each party might be thought of as a node in an information exchange network, with a contractual relationship only to those other nodes with which it actually exchanged information.

Electronic Signatures Provisions

In order to accommodate electronic document usage the Agreement includes provisions allowing the use of Electronic Records and Electronic Signatures. While the Agreement does not specify the types of solution to be used for these purposes, published HHS standards strongly suggest digital signatures should be the signature solution.[13]

Electronic Records pose additional problems of archiving and proof of originals, which are solved by providing for use of an Electronic Records Warehouse. Such a facility could be hosted in a data warehouse operated by one of the parties to the Agreement, if trusted, or by a trustworthy third party. These features are not necessary for the use of the balance of the Agreement, but are available for use if desired.

---

[13] See Draft Security Rule at 43,268-268, 45 CFR sec. 142.310.

The adaptability to a network and usability of electronic documentation strongly suggests that the Agreement could be used to manage privacy and security compliance in a large enterprise or community information network in ways analogous to the management of certificate policies and certification practices statements in a PKI.[14] Unlike a PKI, there would be no central management authority comparable to a certificate authority. Like a PKI there would need to be a central, readily available on-line repository for the Agreement.

Adaptation of Agreement.

The Agreement enables parties to create a draft by globally replacing the following capitalized place-holders:

NAME1	Replace with the organizational or individual name of one of the parties. The template is formatted to make NAME1 the Disclosing Party in the Specifications Addendum, but this is not necessary.
NAME2	Replace with the organizational or individual name of the other party. The template is formatted to make NAME2 the Receiving party in the Specifications Addendum, but this is not necessary.
TYPE1	Replace with the type of organization or individual which identifies NAME1; for example, hospital or health plan.
TYPE2	Replace with the type of organization or individual which identifies NAME2; for example, physician or health care clearinghouse.
DESC1	Replace with a brief description of the business done by NAME1.
DESC2	Replace with a brief description of the business done by NAME2.
STATE1	Replace with the names of the state(s) in which NAME1 does business which will be subject to the Agreement.
STATE2	Replace with the names of the state(s) in which NAME2 does business which will be subject to the Agreement.
AUDITRET	Replace with the period of time for which Audit Trail records will be retained.
JURISD	Replace with the name of the state whose laws will apply to interpretation of the Agreement.

---

[14] See e.g. Greenwood, "Risk and Trust Management for an 'Open But Bounded' Public Key Infrastructure," 38 **Jurimetrics** 277 (Spring 1998).

VENUE	Replace with the name of the court which will have jurisdiction over and venue for any dispute arising under the Agreement.
EFFDATE	Replace with the Effective Date of the Agreement.

Most of these terms appear only in the Recitals, which are Sections I and II. The Recitals are primarily for identification of parties. While the template is formatted for two parties, more parties can be added by copying Recitals I and II and adding their names, descriptions, etc. in place of NAME1, TYPE1, etc. as applicable in the copied Recitals. If this is done, there should be a separate Specifications Addendum for each set of two parties where one will be Disclosing Protected Health Information to the other.

AGREEMENT FOR PROTECTION OF INFORMATION

This Agreement for Protection of Information ("Agreement") is entered into between [NAME1] and [NAME2], effective as of the Effective Date stated below.

I.   NAME1 is TYPE1. NAME1 does DESC1 in the State(s) of STAT1. NAME1 wishes to conduct transactions involving the disclosure of information to NAME2 for the purposes described in the attached NAME1 Specifications Addendum. NAME2 wishes to conduct transactions and receive information from NAME1 for these purposes.

II.   Some or all of the information to be disclosed is required by law to be protected against unauthorized use, disclosure, modification or loss. A violation of such a legal requirement may lead to criminal or civil penalties or other harm or damages. In order to comply with applicable legal requirements for the protection of information, the parties agree as follows.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties therefore agree as follows:

A   Interpretation of this Agreement.

    1   *Definitions*.

Capitalized terms in this Agreement are defined in the text or as follows:

a   "Access" means the ability, means or act of reading, writing, modifying or otherwise communicating data or information or making use of any computer system resource.[15]

b   "Aggregate" means to combine information from a Disclosing Party with information Received from another source.[16]

c   "Agreement" means this Agreement and any Specifications Addendum incorporated into this Agreement by reference.

d   "Anonymize" means to remove, encode, encrypt, or otherwise eliminate or conceal data which identifies an individual, or modifies information so that there is no reasonable basis to believe that the information can be used to identify an individual.[17]

---

[15] Draft Security Rule at 43,265, 45 CFR sec.142.304 (definition of "access").

[16] See Privacy Rule at 82,803, 45 CFR sec. 164.501 (definition of "data aggregation").

[17] Privacy Rule at 82,818, 45 CFR 164.514(a) – (c).

e   "Audit Trail" means a chronological record of the events occurring when a computer system user Accesses and/or Uses Information in the system.[18]

f   "Authenticate" and "Authentication" mean (i) in the case of physical delivery and Receipt, a formalized and recorded process for establishing the Authorization of the Receiving individual, and (ii) in the case of an electronic Transmission, a formalized and recorded process for establishing the Authorization of a communications partner or recipient over a data communications channel.[19]

g   "Authorization" means having or the process of giving an individual or entity the power or right to act on behalf of a party, and to have Access to, Use or Disclose PHI on behalf of the party, including the use of specific written policies and procedures for the granting, documentation and revocation of such power or right, including a specification of the purpose(s) for which such Authorization has been given.[20]

h   "Authorized Person" means an individual or entity to which a party to this Agreement has given prior Authorization to have Access to, Use or Disclose PHI.

i   "Authorized Purpose" means a specified purpose for which an Authorized Person has been given an Authorization to have Access to, Use or Disclose PHI on behalf of a party to this Agreement.

j   "Copy" or "Copying" means the replication or reproduction of information.

k   "Criminal Conviction" means (i) a judgment of conviction entered against the entity or individual by a federal, state or local court, regardless of whether an appeal is pending or the judgment of conviction or other record relating to criminal conduct has been expunged; (b) a finding of guilt against the individual or entity that has been accepted by a federal, state or local court; (c) a plea of guilty or nolo contendere by the individual or entity that has been accepted by a federal, state or local court; or (d) the entering into participation in a first offender, deferred adjudication, or other arrangement or program where judgment of conviction has been withheld.

---

[18] Draft Security Rule 43,267, 45 CFR sec. 142.308(c)(ii); see Newton's Telecom Dictionary at 79.

[19] See Draft Security Rule at 43,265, 45 CFR sec. 142.304 (definition of "authentication") and HCFA Internet Security Policy at 8. Cf. Privacy Rule at 82,820, 45 CFR sec. 164.514(h) (procedures for verification of identity and authority of persons requesting protected health information).

[20] See Privacy Rule at 82,805, 45 CFR sec. 164.502(b)(Covered Entity must ensure only "minimum necessary" protected health information is used or disclosed) and at 82,819, 45 CFR sec. 164.514(d)(implementation specifications for "minimum necessary" standard); Draft Security Rule at 43,266, 45 CFR sec. 142.308(a)(5), (7)(required security features include information access controls and personnel security clearances, policies and training); and HCFA Internet Security Policy at 8.

l   "Disclose," "Disclosing" or "Disclosure" mean the release, transfer, provision of Access to, or divulging in any manner of Information outside the entity holding the Information.[21]

m   "Disclosed Information" means Information which one party has Disclosed to another pursuant to this Agreement.

n   "Disclosing Party" means the party which is Disclosing Information to another party pursuant to this Agreement.

o   "Disclosure Accounting" means an accounting to an Individual of all Disclosures made of PHI pertaining to that Individual.[22]

p   "Effective Date" means the date on which this Agreement becomes effective.

q   "Electronic Record" means any combination of text, graphics, data, audio, pictorial or other information representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system.[23]

r   "Electronic Records Warehouse" means a facility using Security consistent with the requirements of this Agreement, at which Electronic Documents may be stored, and from which non-repudiable copies may be readily retrieved by any party agreeing to use the facility pursuant to this Agreement.

s   "Electronic Signature" means any logical process by which parties manifest adoption of or consent to an Electronic Record.[24]

t   "HHS" means the United States Department of Health and Human Services.

u   "Individual" means a natural person who is the subject of Protected Information.[25]

v   "Information Privacy and Protection Laws" mean (i) the Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations ("HIPAA"); (ii) the Gramm-Leach-Bliley Act, as amended and including any implementing regulations; (iii) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy or security of information pertaining to the health or medical status or condition of an

---

[21] See Privacy Rule at 82,803, 45 CFR sec. 164.501 (definition of "disclosure").
[22] See Privacy Rule at 82,826, 45 CFR sec. 164.528 (requirements for provision of accounting of disclosures to individuals).
[23] See Electronic Signatures in Global and National Commerce Act ("E-SIGN"), 15 USC sec. 7006(4) and 21 CFR sec. 11.3(b)(6) (U.S. Food and Drug Administration regulation defining "electronic records").
[24] See E-SIGN, 15 USC sec. 7006(5) and 21 CFR sec. 11.3(b)(7) (U.S. Food and Drug Administration regulation defining "electronic signature").
[25] See Privacy Rule at 82,804, 45 CFR sec. 164.501 (definition of "individual").

individual, and/or the payment for health or medical care for an individual; (iv) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy of information pertaining to the financial or credit status or condition of an individual; (v) any statute, regulation, administrative or judicial ruling requiring a party to protect information pertaining to Individuals based upon the Individuals' status as consumers; and (vi) any other statute, regulation, administrative or judicial ruling requiring a party to protect the confidentiality, privacy and/or security of information pertaining to Individuals; all to the extent that such Information Privacy and Protection Laws have been enacted, promulgated, issued or published by any federal or state governmental authority with jurisdiction over that party.

w   "Intermediary" means any Third Party which Transmits Information from a Disclosing Party to a Receiving Party, including but not limited to a health care clearinghouse.

x   "Minimum Necessary Information" means (i) in the case of routine and recurring types of Disclosures, the set of data or records which the Disclosing Party's policies and procedures have established as reasonably necessary to achieve the purpose of such Disclosures; (ii) in the case of non-routine or non-recurring Disclosures, the set of data or records which the Disclosing Party determines is reasonably necessary to accomplish the purpose of the Disclosure, upon review of each Disclosure according to criteria developed by the Disclosing Party; provided that (iii) in the case of a Disclosure (A) to a Covered Entity, (B) to a professional for purposes of providing professional services to the Disclosing Party, or (C) to a public official for Disclosures which are permitted by law without Individual consent, the Minimum Necessary Information shall be the set of data or records requested by that party, upon the party's reasonable representation that the request is for the minimum necessary given the purpose of the Disclosure(s). [26]

y   "Process" and "Processing" mean a computer operation or sequence of computer operations applied to Information to produce a specified result. As used in this Agreement, Process specifically includes but is not limited to Information storage, copying, transmission, commingling or combining with other information, application of algorithms, and any other computer operation which affects the availability, accessibility, integrity, structure, format or content of Information.

---

[26] See Privacy Rule at 82,805, 45 CFR sec. 164.502(b) and at 82,819, 45 CFR sec. 164.514(d).

z   "Protect," "Protected" and "Protection" refer to the implementation and use of appropriate administrative, technical and physical safeguards to protect the privacy of Protected Information.[27]

aa "Protected Information" means any information which identifies or could reasonably be believed could identify an individual, which in any way concerns that individual's health status, healthcare, or payments for his or her healthcare,[28] or which a party is otherwise legally required to protect under an Information Privacy and Protection Law applicable to that party, and includes as well any information derived by the Processing of such information which is not Anonymized with respect to any Individual who is the subject of the information.

bb "Receive," Receiving" and "Receipt" means (i) to take physical delivery of media containing information, or (ii) in the case of electronic delivery, for information to come into existence in a party's information processing system in a form capable of being processed by or perceived from a system of that type by the Receiving Party, if the Receiving Party has designated that system or address as a place for Receipt of Information to a Disclosing Party and the Disclosing Party does not know that the information cannot be Accessed from the particular system.

cc "Receiving Party" means a party which is Receiving Information from another party pursuant to this Agreement.

dd "Security" means that set of policies, processes and procedures adopted by a party to ensure the Protection of Information.[29]

ee "Specifications Addendum" means an addendum to this Agreement which defines the specifications and procedures for Disclosure of information by a party to this Agreement. In the event that more than one party is Disclosing information to another party to this Agreement, the parties may agree to establish Specifications Addenda for each party. Each Specifications Addendum shall be identified by the name of the Disclosing Party to which it applies. All Specifications Addenda shall be incorporated into this Agreement by reference. Specifications Addenda may be amended by the parties from time to time as provided below.

ff   "Subcontractor" means a Third Party providing services to a Receiving Party in connection with the Receiving Party's obligations under this Agreement.[30]

---

[27] See Privacy Rule at 82,827, 45 CFR sec. 164.530(c).
[28] Privacy Rule at 82,805, 45 CFR sec. 164.501 (definition of "protected health information").
[29] Draft Security Rule at 43,249-250.
[30] See Privacy Rule at 82,808 45 CFR sec. 164.504(e)(2)((ii)(D).

gg "Term" means the period of time from the Effective Date through Termination of this Agreement..

hh "Third Party" means any individual, person or organization which is not a party to this Agreement.

ii "Transaction" means the Transmission of information between parties to this Agreement.[31]

jj "Transmit," "Transmitted" or "Transmission" means the transfer of information by one party to another, including (i) telephone voice and "faxback" systems, (ii) the transfer by mail or courier of information stored in portable electronic media or printed on paper or other "hard copy" medium, and (iii) electronic transmission by a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, and private networks.[32]

kk "Unauthorized" means (i) an individual or entity who has not been Authorized to act on behalf of a party, or (ii) an action by an Authorized individual or entity which is not within the scope of the Authorization.

ll "Use" means the sharing, employment, application, utilization, examination, analysis, anonymization, or commingling with other information, of information by a party which holds that information.[33]

mm "Workforce" means an party's employees, volunteers, trainees, and other persons under direct control of the party, including persons providing labor on an unpaid basis.[34]

nn "Writing" or "Written" means text created or recorded on paper or created or recorded in an electronic medium; provided that a copy of any electronic Writing must be recorded and archived in a trustworthy system of records in which its integrity and usability will be maintained and from which non-repudiable copies will be readily available for a period of no less than six (6) years from the date the copy is deposited.[35]

---

[31] See Privacy Rule at 82,800, 45 CFR sec. 160.103 (definition of "transaction").

[32] See Transactions Rule at 50,367, 45 CFR sec. 162.103 (definition of "electronic media").

[33] See Privacy Rule at 82,805, 45 CFR sec. 164.501 (definition of "use")

[34] See Privacy Regulations at 82,800, 45 CFR sec. 164.103 (definition of "workforce")

[35] See Privacy Rule at 82,828, 45 CFR sec. 164.530(j)(requiring that a Covered Entity must retain Electronic Records of its required privacy policies and procedures for at least six (6) years from the later of the date of its creation or the date it was last effective). See generally *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* (National Archives and Records Administration,

2 *Application of Provisions to Multiple Parties*.   Any party to this Agreement may either Disclose Protected Information and other information to or Receive Protected Information and other information from any other party to this Agreement. The provisions applicable to a party will vary depending upon whether the party is a Receiving Party or a Disclosing Party in any given Transaction.

3 *Incorporation of Specifications Agreements*. This Agreement incorporates by reference any Specifications Addendum which any two or more parties to this Agreement have agreed shall incorporate this Agreement by reference. Any such Specifications Addendum must include the provisions set forth in Section B(2) below.

4 *Intent to Comply with Laws*.   This Agreement shall be interpreted consistently with all applicable Information Privacy and Protection Laws, and shall be construed and interpreted liberally in favor of the protection of Protected and confidential Information. In the event of a conflict between applicable laws, the more stringent law shall be applied.[36]

B Standards for Transactions.

1 *Minimum Necessary Information*.   Prior to conducting any Transaction in which Protected Information is Disclosed, the parties shall establish the Minimum Necessary Information for purposes of that Transaction.

2 *Specifications Addenda*.   Prior to conducting any Transaction subject to this Agreement the parties shall enter into a Specifications Addendum applicable to that Transaction. Any Specifications Addendum shall include the following provisions:

a   An identification of the parties.

b   A statement incorporating this Agreement by reference.

c   A description of the purpose(s) for which Protected Information will be Disclosed in the Transaction.[37]

d   A description of the scope of the Protected Information which will be Disclosed.[38]

October 18, 2000). The actual records retention period should probably be tied to the expected Term of the Agreement, plus the statute of limitations applicable to written contract actions under applicable state law.

[36] In the event of a conflict between the Privacy Rule and state law, the "more stringent" standard applies. See Privacy Rule at 82,800 – 801, 45 CFR Subpart B. The same approach should be applied in the event two federal laws apply to the same Transaction or party, since compliance with the "more stringent" of the two laws would necessarily entail compliance with the less stringent as well.

[37] This statement is required in order both to document the authority for the Disclosing Party's Disclosure, as required by the Privacy Rule at 82,805, 45 CFR sec. 164.502(a), and to define and limit the Receiving Party's authority to Use or further Disclose Protected Information, as required in the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)2)(i).

e   A description of the Uses and Disclosures permitted with respect to Protected Information Received.[39]

f   A description of the format(s) in which information will be disclosed.

g   A description of the method(s) by which information will be Transmitted, including encryption or other technical security mechanisms implemented if using electronic communications network.

h   If an Intermediary will be used, it must be identified.

i   A description of the means used to Authenticate person(s) Authorized to Receive Protected Information.

j   The parties may elect to state additional or more detailed requirements for the Protection of information.

k   If the purposes for the Disclosure include Anonymizing or Aggregation of Protected Information, that must be stated.

l   If the parties wish to implement Electronic Signatures and/or Electronic Records, the applicable procedures and processes for Electronic Signatures must be specified and the Electronic Records Warehouse must be identified.

m   While not required, it may be desirable to include terms for payment of fees or other applicable sums payable in connection with Transactions under this Agreement.

3   *Disclosing Party Transmission.*   A Disclosing Party shall Transmit information to the Receiving Party according to the processes and procedures agreed in the applicable Specifications Addendum.

4   *Receiving Party Receipt.*   A Receiving Party shall Receive information from the Disclosing Party according to the processes and procedures agreed in the applicable Specifications Addendum.

5   *Use of Intermediaries.*The parties may use Intermediaries to Transmit Information, provided that:

---

[38] This description is intended to document that the Disclosure is of the "Minimum Necessary" information, as required in the Privacy Rule.

[39] This is a required element of a Business Associate Contract under the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(i).

a   Any Intermediary to which Protected Information is Disclosed must enter into a Written agreement requiring the Intermediary to Protect such Information which is consistent with and provides at least as much Protection for Protected Information as this Agreement;

a   The Intermediary has been identified in the applicable Specifications Addendum; and

b   The use of an Intermediary shall not relieve any party of any obligation stated in this Agreement, unless the parties expressly agree otherwise in Writing.

C   Information Protection Obligations of Disclosing Parties.

1   *General Obligations*. When Disclosing information under this Agreement, the Disclosing Party shall:

b   Maintain the policies, procedures and documentation necessary to establish the Disclosing Party's right and authority to Disclose that information. [40]

c   Provide the Minimum Necessary Information as shown or stored in records or systems owned or operated by or subject to the Disclosing Party's control.

d   If the information is provided in electronic form, the information must be subjected to a virus check prior to Transmission.[41]

---

[40] The basis for a Disclosing Party's authority to Disclose Protected Information will depend upon the status of the parties to the transaction and the purposes for the disclosure. For example, the Disclosing Party will be required to have an individual's written, signed "consent" to support a disclosure for "payment" purposes, such as claims submission. See Privacy Rule at 82,810, 45 CFR sec. 164.506(a)(1). Other purposes will have to be supported by a written, signed "authorization," see Privacy Rule at 82,812 – 813, 45 CFR sec. 164.510, while disclosures marketing purposes are subject to a requirement that individuals be permitted to "opt out," see Privacy Rule at 82,812 – 813, 45 CFR sec. 164.510, and disclosures for a range of purposes as public health and health oversight are not required to be supported by any individual consent or authorization. See Privacy Rule at 82,813 – 818, 45 CFR sec. 164.512. Some uses or disclosures must also be disclosed in the Disclosing Party's notice of its privacy practices. See Privacy Rule at 82,8221, 45 CFR sec. 164.520(b)(1)(iii). Since it is a criminal offense to "knowingly obtain" protected health information in violation of HIPAA, see HIPAA sec. 1177(a)(2), the Receiving Party has an incentive to hold the Disclosing Party to a warranty that its Disclosure does not violate the regulations. See generally Christiansen, **Electronic Health Information: Privacy and Security Compliance Under HIPAA** (2000) at 29 – 36.
[41] Virus checking is required under the Draft Security Regulation at 43,266, 45 CFR sec. 142.308(a)(8)(v).

e   If the information is Transmitted electronically, the Disclosing Party shall use or maintain technological systems and procedures to guard against unauthorized access to information that is Transmitted electronically, including encryption and/or appropriate technical security mechanisms;[42]

2   *Computer System Administration.*   In the event the parties have implemented Transmission procedures under which the Disclosing Party has the capacity to directly access a computer or computer systems of the Receiving Party, the Disclosing Party shall:[43]

a   Maintain a designated individual or individuals to serve as security officer(s) responsible for supervising the security of the Disclosing Party's applications permitting access to the Receiving Party's systems, who shall further be responsible for communicating with the Receiving Party with respect to matters affecting the security of the Receiving Party's computer or computer systems;[44]

b   Maintain such policies, procedures and systems as may be necessary to prevent Unauthorized parties from having Access to, Using, Disclosing, Processing, Copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the availability, accessibility, integrity, structure, format or content of information which may be Transmitted to the Receiving Party;[45]

c   Notify the Receiving Party immediately in the event of any proven or suspected incident in which the Disclosing Party has reason to believe any Unauthorized person may have had Access to the computer or computer systems of the Receiving Party; and

d   Conduct assessments of the policies, procedures and systems used by the Receiving Party to fulfill the obligations of this Section, (i) no less frequently than once each year, [46] and (ii) in response to any material breach of security within the scope of this Section.

---

[42] See Draft Security Regulation at 43,268, 45 CFR sec. 142.308(d); and HCFA Internet Security Policy. Note that the systems used to Transmit information must be compatible with Receiving Party systems used to Receive such information.

[43] The following provisions are intended to establish "chain of trust" obligations applicable to a Disclosing Party under the Draft Security Rule. A Covered Entity will in any case have to comply with all the HIPAA security requirements.

[44] While a security officer is not specifically required, security management processes including oversight and accountability are required under the Draft Security Rule at 43,267, 45 CFR 142.308(a)(10) and .308(b)(1).

[45] Such controls are required for electronic Transmissions over a network under the Draft Security Rule at 43, 268, 45 CFR sec. 142.308(d).

[46] Such assessments are prudent practice, and also required under the Draft Security Rule at 43,266-267, 45 CFR sec. 142.308

D   Information Protection Obligations of Receiving Parties.

1   *General Obligations*. At all times following the Receipt of Protected Information, until such time as the Protected Information is no longer in the Receiving Party's possession or subject to its control:[47]

   a   The Receiving Party shall not Use, Disclose or Process Protected Information for any Purpose not stated in the applicable Specifications Addendum, excepting only as necessary for the proper management and administration or in order to carry out the legal responsibilities of the Receiving Party.[48]

   b   The Receiving Party shall implement appropriate safeguards to prevent any Use or Disclosure of the Protected Information other than those permitted under this Agreement.[49]

   c   The Receiving Party shall promptly notify the Disclosing Party of any Use or Disclosure of the Protected Information contrary to the terms of this Agreement of which the Receiving Party becomes aware.[50]

   d   The Receiving Party may only Disclose Protected Information to Third Parties under the following conditions:[51]

      i   The Disclosure is of the Minimum Necessary Information for the purposes of the Disclosure; and

      ii   The Disclosure

      A   Is necessary to accomplish a Purpose for which the Protected Information was Disclosed to the Receiving Party, and

      B   Is to a Subcontractor who has entered into a Written agreement which

         I   Requires the Subcontractor to Protect such Information under conditions consistent with and providing at least as much Protection for the Protected Information as this Agreement, including but not limited to provisions requiring the Subcontractor to promptly notify the Receiving Party of any Use or Disclosure of the Protected Information contrary to the

---

[47] These obligations correspond to general requirements for a Business Associate Contract, see Privacy Rule at 82,808, 45 CFR sec. 164.504(e)2).
[48] See Privacy Rule at 82,808 - 8, 45 CFR sec. 164.504(e)(2)(i)(A), .504(e)(2)(ii)(A) and .504(e)(4)(i).
[49] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(B).
[50] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(C).
[51] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(D).

terms of the Written agreement under which the Receiving Party Disclosed the information;[52] and

II Includes provisions stating that the Subcontractor shall not be deemed to have an ownership interest in the Protected Information, and requiring the Subcontractor to return, destroy or archive all such information under terms consistent with Section G of this Agreement, upon the termination of the Receiving Party's agreement with the Subcontractor; or

iii The Disclosure is required by law, provided that the Receiving Party shall give the Disclosing Party prior Written notice and an opportunity to intervene (unless the Receiving Party is prohibited from giving such notice by order of a court of competent jurisdiction);[53] or

iv The Disclosure is to the Individual who is the subject of the Protected Information;[54] or

v The Disclosure is otherwise permitted under applicable Information Privacy and Protection Laws.[55]

e The Receiving Party shall at all times Protect information Received from the Disclosing Party in compliance with all applicable Information Privacy and Protection Laws.

f The Receiving Party shall make its internal practices, books and records relating to its Uses and Disclosures of Protected Information Received from the Disclosing Party available to HHS, upon HHS's request, for purposes of determining the Disclosing Party's compliance with the Information Privacy and Protection Laws.[56]

---

[52] See Privacy Rule at 82,808 - 809, 45 CFR sec. 164.504(e)(2)(ii)(D), .504(e)(4)(ii)(B).

[53] See Privacy Rule at 82,809, 45 CFR sec. 164.504(e)(4)(ii). The Privacy Rule does not require notification of a Covered Entity in the event of a Business Associate Disclosure required by law, but it is in the interest of such entities to be aware of governmental information gathering activities which may pertain to them.

[54] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(E) and 82,823 – 824, 45 CFR sec. 164.524.

[55] This provision is necessary to permit a Business Associate which is also a Covered Entity to Use or Disclose Protected Information Received under this Agreement in connection with health care operations such as accreditation, for example, as permitted under the Privacy Rule at 82,803, 45 CFR sec. 164.501 (definition of "health care operations"), presuming that the required consent has been obtained. See Privacy Rule at 82,810 - 811, 45 CFR sec. 164.508.

[56] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(H), .504(e)(4)(i)(ii)(B).

g   The Receiving Party shall notify the Disclosing Party promptly in the event that it becomes aware of any Use or Disclosure of Protected Information Received under this Agreement, which is not provided for in this Agreement.[57]

2   *Computer System Administration.*   In the event the Receiving Party Receives, Discloses, stores or Processes Protected Information using a computer or computer systems, the Receiving Party shall:[58]

a   Maintain a designated individual or individuals to serve as security officer(s) responsible for supervising the security of the Receiving Party's computer systems, who shall further be responsible for communicating with the Disclosing Party with respect to matters affecting the security of the Disclosing Party's computer or computer systems;

b   Maintain technological systems and procedures to guard against unauthorized access to information that is Transmitted electronically, including encryption and/or appropriate technical security mechanisms;[59]

c   Maintain such policies, procedures and systems as may be necessary to prevent Unauthorized parties from having Access to, Using, Disclosing, Processing, Copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the privacy, availability, accessibility, integrity, structure, format or content of information which may be Transmitted to the Receiving Party;[60]

d   Notify the Disclosing Party immediately in the event of any proven or suspected incident in which the Receiving Party has reason to believe any Unauthorized person may have had Access to the computer or computer systems of the Receiving Party; [61]

e   Maintain such policies, procedures and systems as may be reasonably necessary to ensure the Protection of information against Disclosure, corruption or destruction caused by modification of, harm or damage to computer systems components and storage media pertaining to such information, including but not limited to appropriate backup procedures and contingency plans;[62] and

---

[57] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(C)..

[58] These obligations correspond to the Disclosing Party's "chain of trust" obligations.

[59] See Draft Security Regulation at 43,268, 45 CFR sec. 142.308(d); and HCFA Internet Security Policy. Note that the systems used to Receive information must be compatible with Disclosing Party systems used to Transmit to the Receiving Party.

[60] See Draft Security Regulation, 45 CFR sec. 142.308(a) – (c).

[61] This provision is also required to comply with the Business Associate Contract provisions of the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(B), in the context of computerized transactions.

[62] A Receiving Party will only be required to comply with the final HIPAA security rule if it is also a Covered Entity. This Agreement does not attempt to specify that such compliance is required, but Covered

    f   Conduct assessments of the policies, procedures and systems used by the Receiving Party to fulfill the obligations of this Section, (i) no less frequently than once each year and (ii) in response to any material breach of security within the scope of this Section. [63]

E   <u>Privacy Practices</u>.

    During the Term of this Agreement the parties shall at all times coordinate any policies, processes and procedures they maintain under which Individuals are permitted to inspect, copy and amend or seek amendment of Protected Information which pertains to them. The parties shall therefore at all times:

    1   *Privacy Officers.*   Maintain a designated individual or individual(s) who shall be responsible (a) for ensuring the compliance of the party with the privacy requirements of all applicable Information Privacy and Protection Laws, and (b) for communicating with the other party with respect to matters concerning the inspection, copying and amendment of Protected Information by Individuals.[64]

    2   *Policies, Consents and Authorizations.*   If a party is required or elects to publish a consent and/or authorization forms, and/or a privacy policy or policies, the party shall (a) ensure that such documentation and/or the policy does not conflict with the party's ability to perform its obligations under this Agreement, and (b) provide copies of such documentation to all other parties to this Agreement on or before their publication to Individuals. [65]

    3   *Additional Privacy Protections at Individual Request.*   In the event a Disclosing Party has agreed to provide additional privacy protections to information pertaining to an individual, the Disclosing Party shall notify the Receiving Party on the date such information is Transmitted to the Receiving Party or the date on which the Disclosing Party makes such an agreement, whichever is later.[66] In the event or an individual has revoked an authorization or consent to disclosure of information previously given to the Disclosing Party, which pertains to information Disclosed to a Receiving Party, the Disclosing Party shall promptly notify the Receiving Party of

---

Entities entering into this Agreement as Disclosing Parties may wish to add such a specification applicable to Receiving Parties which are not Covered Entities.

[63] Such assessments are prudent practice, and also required under the Draft Security Rule at 43,266-267, 45 CFR sec. 142.308

[64] The privacy officer called for under the Privacy Rule might be the appropriate individual to fulfill this function.

[65] This Agreement does not attempt to establish joint privacy procedures, something which would probably not be possible in a document of this general applicability since different standards will apply to different kinds of parties. Rather, it requires the parties to establish processes to coordinate and support each others' practices.

[66] See Privacy Rule at 82,822- 823, 45 CFR sec. 164.522;

such revocation, and the Receiving Party shall implement such processes and procedures as may be necessary to implement such revocation.[67]

4   *Inspection, Copying and Amendment of Records.*   If a party is required or elects to maintain policies and procedures for the inspection, copying, amendment or request for amendment by Individuals of Protected Information, the party shall (a) ensure that these policies and procedures do not conflict with the party's ability to perform its obligations under this Agreement, and (b) provide copies of such documentation to all other parties to this Agreement on or before their publication to Individuals.[68]

5   *Notification of Record Amendment.*   In the event a record pertaining to an individual is amended or statements pertaining to a proposed amendment of the record have been prepared for inclusion in the record, the party responsible for responding to the individual's request for amendment shall promptly provide all other parties to which it has Disclosed copies of that record with copies of the amendments or statements, as applicable. A party Receiving a copy of such amendment or statement shall promptly include it in the records maintained by that party with respect to that individual.[69]

6   *Disclosure Records.*   Maintain a record of all Disclosures made of Protected Information, including (a) the date of the Disclosure, (b) the name and address of the organization and/or individual Receiving the Information; (c) a brief description of the information Disclosed; (d) if the Disclosure was not to the Individual, the Purpose for the Disclosure; and (e) a copy of all requests for Disclosures ("Disclosure Accounting").[70]

7   *Provision of Information and Amendment of Records.*   Maintain procedures for the:

    a   Providing Disclosure Accountings directly to Individuals, or to Disclosing Parties who have been requested to provide a Disclosure Accounting;[71]

    b   Communication of amendments or information pertaining to amendments of Protected Information by Individuals from Disclosing Parties to Receiving Parties;[72] and

---

[67] See Privacy Rule at 82,811, 45 CFR sec. 164.508(b)(5); RCW 70.02.030
[68] See Privacy Rule at 82,823 – 826, 45 CFR sec. 164.524, 526.
[69] See Privacy Rule at 82, 825, 45 CFR sec. 164.526((b)(3), (e).
[70] See Privacy Rule at 82,826, 45 CFR sec. 164.528.
[71] Id.
[72] See Privacy Rule at 82,825, 45 CFR sec. 164.526(c)(3).

c   Including amendments or information pertaining to amendments of Protected Information Received from Individuals or Disclosing Parties, into record sets of Protected Information.[73]

F   Information Ownership.

The following provisions control the ownership of information Disclosed under this Agreement. These provisions shall not apply to information which (a) is readily available or can be readily ascertained through public sources, (b) a party has previously Received from a source or sources legally entitled to Disclose such Information to the party, or (c) can be demonstrated by documentation to have been independently developed by the Receiving Party without reference to any information provided by the Disclosing Party.

1   *Information Presumed Owned by Disclosing Party.* All information shall be deemed to be the exclusive property of the Disclosing Party, unless (a) otherwise expressly agreed in Writing or (b) the information was previously Received by the Disclosing Party from another party to this Agreement, who did not disclaim ownership in Writing.[74]

2   *No Transfer of Ownership by Disclosure.*   A Disclosure of Information shall not transfer legal title to information to the Receiving Party, unless otherwise expressly agreed in Writing.

3   *Receiving Party Limited Right of Possession.*   The Receiving Party shall be entitled to have non-exclusive possession of Disclosed information subject to the provisions of this Agreement. The right to possession of such information shall be automatically terminated upon the termination of this Agreement, unless (a) otherwise agreed in Writing, or (b) return or destruction of the Information is not feasible, in which event the right of possession shall be limited to possession for the Purpose(s) which make return or destruction of the information not feasible.

3   *Receiving Party Limited Right of Use and Disclosure.*   The Receiving Party shall have a non-exclusive right to Use and Process Disclosed information for the Purposes stated in the applicable Specifications Addendum. This right shall be revoked immediately upon the termination of this Agreement.

4   *No Right to Anonymize or Aggregate.*   The rights to Use and Process information shall not include rights to Process information to produce Anonymized Information or produce Aggregated Information, unless otherwise expressly agreed in Writing.

---

[73] See Privacy Rule at 82,825, 45 CFR sec. 164.526(a)(1). .526(c)(5).

[74] This provision does not account for the possibility that information may be owned by a party not privy to this Agreement, who provided it to the Disclosing Party without transferring ownership.

5   *No Liens.*   The Receiving Party shall not have a lien or security interest in any Disclosed information, unless otherwise expressly agreed in Writing.

G   Return, Archiving or Destruction of Information.

Upon the Termination of this Agreement: [75]

1   *Return of Information.*   The Receiving Party shall provide the Disclosing Party with originals, or if originals are not available a copy of all information Disclosed to the Receiving Party by the Disclosing Party under this Agreement; and

2   *Destruction of Information.*   Any information subject to this Agreement which the Receiving Party does not or cannot return, the Receiving Party shall permanently destroy by shredding or otherwise destroying all paper or other hard copy media on which it is recorded, and/or wiping it from any hard drive, tape, diskette, compact disk or other electronic medium on which it has been stored using utilities or processes which render the information unrecoverable, and/or by otherwise destroying the medium on which the Information is stored so that the Information is not recoverable, unless otherwise agreed in Writing; provided that

3   *Archiving of Information.*   If it is not feasible for the Receiving Party to return or destroy such information, the Receiving Party shall continue all protections provided to Protected Information under this Agreement, and shall limit future Uses or Disclosures of such information to those Purposes which make the return or destruction of the information infeasible.

4   *Subcontractor Information.*   The provisions of this Section G shall also apply to any Subcontractors to whom the Receiving Party has Disclosed Protected Information.

H   General Warranties and Indemnification.

1   *Mutual Warranties*:   Each party to this Agreement represents and warrants to all other parties that, at all times during the Term and at such other times as may be indicated, he, she or it:

a   Is duly organized or incorporated and validly existing under the laws of the jurisdiction of its organization, unless the party is an individual;

b   Has all requisite powers, licenses and permits;

c   Has undertaken all actions and has fulfilled all conditions to Disclose or Receive Protected Information and to enter into, perform under and comply with its obligations under this Agreement;

---

[75] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(ii)(i).

d   Shall comply with, and as applicable shall require its directors, officers and employees with, all applicable Information Privacy and Protection Laws;

e   Is not and has not ever been excluded, barred or otherwise ineligible from participation in any government health care program, including but not limited to Medicare, Medicaid, CHAMPUS or Tricare;

f   Has not ever received, and if applicable has taken appropriate steps to ensure that its directors, officers and employees have never received, a Criminal Conviction related to health care; and

g   Shall comply with, and as applicable shall require its directors, officers and employees to comply with its duties and obligations pursuant to this Agreement, including but not limited to duties and obligations which survive the termination of this Agreement.

2   *Indemnification.* Each party will indemnify, hold harmless and defend the other parties to this Agreement from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this Agreement; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with the party's performance under this Agreement.

I   Dispute Resolution.

1   *Applicable Law.* This Agreement and any disputes arising under it shall be exclusively governed by and interpreted under the laws of the State of JURIS in the United States as though the parties were located in the State of JURIS.

2   *Alternative Dispute Resolution.* {This Section reserved.}

3   *Jurisdiction and Venue for Judicial Proceedings.* Jurisdiction and venue for any dispute arising out of or in connection with this Agreement shall be at VENUE.

4   *Legal Fees and Costs.* In the event of legal proceedings arising from or pertaining to this Agreement the substantially prevailing party shall be awarded its reasonable attorneys fees and costs of litigation, including any on appeal or in bankruptcy proceedings.

J   Term and Termination.

1   *Effective Date.* The Effective Date of this Agreement shall be EFDAT.

2   *Termination of Specifications Addenda.*   The Termination of this Agreement with respect to a party shall simultaneously terminate any Specifications Addendum in effect with respect to that party under this Agreement.

3   *Effect of Multiple Parties*.   In the event there are more than two parties to this Agreement, the termination of this Agreement with respect to any one party shall not terminate this Agreement with respect to the remaining parties.

4   *Effect of Termination on Obligations.*   The Termination of this Agreement shall not affect any provision of this Agreement which by its wording or its nature is intended to remain effective and to continue to operate in the event of termination of this Agreement, and shall not prejudice or affect the rights of any party against another in respect of any breach of the terms and conditions of this Agreement.

5   *Term.* Except as otherwise agreed, this Agreement shall be in effect for an initial Term of one (1) year, commencing on the Effective Date ("Minimum Term"). This Agreement will be automatically renewed for a Renewal Term of an additional one (1) year at the end of the Minimum Term and the end of each automatic Renewal Term thereafter, provided that any party may elect not to renew its coverage by and participation under this Agreement by giving Written notice of such election to all other parties no later than thirty (30) days prior to the end of the Minimum or any Renewal Term.

6   *Conditions Allowing Immediate Termination.*   Notwithstanding anything to the contrary in this Agreement, any party may terminate its coverage by and participation under this Agreement immediately upon Written notice to all other parties, without any term of notice and/or judicial intervention being required, and without liability for such termination, in the event that:

a   The terminating party determines that any other party has violated a material provision of this Agreement pertaining to the Protection, Use or Disclosure of Protected Information;[76]

b   Any other party receives (i) a Criminal Conviction, (ii) is excluded, barred or otherwise ineligible to participate in any government health care program, including but not limited to Medicare, Medicaid, CHAMPUS or Tricare; (iii) is named as a defendant in a criminal proceeding for a violation of any Information Privacy and Protection Law; or (iv) is found to have or stipulates that the party has violated any privacy, security or confidentiality protection requirements under any applicable Information Privacy and Protection Law in any administrative or civil proceeding in which the party has been joined;

---

[76] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(iii).

c   A trustee or receiver is appointed for any or all property of a party to which is in possession of Protected Information Disclosed by the terminating party;

d   A party which is in possession of Protected Information Disclosed by the terminating party becomes insolvent or unable to pay debts as they mature, or ceases to so pay, or makes an assignment for benefit of creditors;

e   Bankruptcy or insolvency proceedings under bankruptcy or insolvency code or similar law, whether voluntary or involuntary, are properly commenced by or against a party which is in the possession of Protected Information Disclosed by the terminating party; or

f   A party which is in the possession of Protected Information Disclosed by the terminating party is dissolved or liquidated.

7   *Termination for Curable Breach.*   A party may terminate may terminate its coverage by and participation in this Agreement upon Written notice in the event that another party materially breaches one or more of the requirements or conditions of this Agreement or the applicable Specifications Addendum and, if curable, fails to reasonably cure such breach within thirty (30) days from the date of the notice. Notwithstanding the foregoing, the non-breaching party, at the non-breaching party's sole discretion, may elect to cure any breach which in the non-breaching party's sole determination may constitute or cause a violation of any Information Privacy and Protection Law by the non-breaching party, in which event the costs and expenses of such cure shall be borne by the breaching party.[77]

8   *Termination for Good Cause.* Any party may terminate its coverage by and participation in this Agreement for good cause by providing sixty (60) days Written notice to all other parties; provided, however, that the party may not enter into an agreement for substantially the same services provided for in a Specifications Addendum terminated by such notice with another party or parties to that addendum during a period equal to the remainder of the then-current Minimum or Renewal Term.

9   *Termination Due to Change in Law.* Any party may terminate its coverage by and participation in this Agreement upon reasonable Written notice to all other parties in the event that it has sought amendment of this Agreement pursuant to Section K(1)(iii) and no amendment has been agreed upon, by Written notice of termination no later than thirty (30) days after the date required for agreement upon amendment.

---

[77] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(ii).

K   Miscellaneous.

1   *Amendment of Agreement*.

a   A Specifications Addendum may be modified or amended by mutual agreement of the parties at any time without amendment to this Agreement.

b   A modification by a party of its policies, procedures, processes and/or systems used in connection with its obligations under this Agreement shall not be deemed a breach of or amendment to this Agreement, unless (i) such modification unreasonably interferes with another party's ability to fulfill its obligations under this Agreement, or (ii) such modification is contrary to or interferes with a specific obligation stated in the applicable Specifications Addendum.

c   Any party may seek to amend this Agreement in order to accommodate any new legislation, regulation, case holding, or legal order issued or proposed to be issued by a federal or state agency of competent jurisdiction which, in the reasonable judgment of the party, (i) invalidates or is materially inconsistent with this Agreement; (ii) would cause a party to be in violation of the law by its continued performance under this Agreement; (iii) would jeopardize the tax-exempt status of the party (if applicable) by its continued performance under this Agreement; or (iv) would jeopardize the licensure, accreditation or participation in good standing in a federal health benefit plan of the party by its continued performance under this Agreement. A party wishing to seek such an amendment shall notify all other parties in writing, including any proposed terms of amendment, no later than ninety (90) days prior to the proposed effective date of the amendment. The parties shall then negotiate in good faith to agree upon an amendment. In the event no agreement is reached, no amendment shall be effective, and the party seeking amendment may elect to terminate by written notice pursuant to Section J(7).

2   *Entire Agreement.* This Agreement, including any Specification Addenda incorporating this Agreement by reference, and as amended from time to time pursuant to Section K(1), constitutes the entire agreement and understanding between the parties with respect to the services specified and agreed upon in this Agreement and supersedes all prior oral or written agreements and understandings between them with respect to such services.

3   *Assignment*. No party may assign or transfer any or all of its rights and/or obligations under this Agreement or any part of it, nor any benefit or interest in or under it, to any Third Party without the prior written consent of all other party/ies, which shall not be unreasonably withheld.

4   *No Agency or Partnership*.   This Agreement does not create a joint venture, partnership or employer-employee relationship between the parties. In performing

under this Agreement, each party is at all times acting and performing as an independent contractor and is not authorized to act as an agent or representative of any other party.

5   *Notices*. Any notice which may be or is required to be given under this Agreement shall be Written and shall be sent by first class mail, fax, courier or as an Electronic Record attached to an e-mail. All notices shall be effective upon receipt at the addresses stated in the applicable Specifications Addendum, which may be changed from time to time upon thirty (30) days notice.

6   *Use of Electronic Signatures and Electronic Records*. The parties may elect to establish processes for the use of Electronic Records in the management of and compliance with this Agreement. Such documents may include published policies, procedural information, notices, and any other document arising from or pertaining to this Agreement, including this Agreement itself. Any such process must include:

   a   Designation of a mutually acceptable, secure Electronic Records Warehouse for the archiving and retrieval of Electronic Records, which must meet or exceed all security regulations applicable to Protected Information, and be operated consistently with all applicable Information Privacy and Protection Laws; and

   b   Establishment of a mutually acceptable Electronic Signature process, which must include all features and meet or exceed all standards required to comply with all applicable federal and state laws.

No Electronic Document shall be deemed effective until it has Electronically Signed and fully signed counterparts have been received by all parties required to execute or receive the document and a counterpart as been deposited in the documentation warehouse facility. Any electronic or printed counterpart of an Electronic Document shall be deemed an original of that document, provided that in the event of a dispute the counterpart deposited in the documentation warehouse facility shall be deemed the binding version.

   NAME1   NAME2

   _____   _____
   _____   _____
   (Print Name)   (Print Name)

   _____   _____
   (Print Title)   (Print Title)

   _____   _____
   Date   Date

Sample Form: Specifications Addendum

This Specifications Addendum is entered into between NAME1 and NAME2 pursuant to that certain Agreement for Protection of Information dated effective EFDAT ("Agreement"). The Agreement is hereby incorporated by reference as if repeated in its entirety. This Specifications Addendum may be amended from time to time as provided in Section K of the Agreement. As provided in the Agreement, the parties hereby specify as follows:

A.   Purpose(s) for Disclosure.

The Purpose(s) for which NAME1 shall Disclose Information to NAME2 are the following:

B.   Information to be Disclosed.

The scope of the Information to be Disclosed is as follows:

C.   Permitted Uses and Disclosures of Information.

The Receiving Party shall be limited to the following Uses and/or Disclosures of PHI:

D.   Disclosure Format(s).

Information shall be Disclosed in the following format(s):

E.   Method of Transmission.

Information shall be Transmitted as follows:

F.   Use of Intermediary.

The parties elect to use the following Intermediary to Transmit Information:

G.   Authentication.

Authorized individuals Receiving Information on behalf of the Receiving Party shall be Authenticated by use of the following:

H.   Supplemental Security and/or Privacy Specifications.

The parties elect to implement the following additional Security and/or Privacy Protections:

I.   <u>Anonymization and Aggregation of Information</u>.

The Disclosing Party authorizes the Receiving Party to Anonymize and/or Aggregate PHI for the following Purpose(s), subject to the following limitations on Use and Disclosure of the Anonymized or Aggregated Information:

J.   <u>Electronic Records and Signatures</u>.

The parties elect to establish the following procedures for Electronic Records:

1.   This Specifications Addendum incorporates by reference the electronic counterpart of the Agreement for Protection of Information published as of the Effective Date at the following URL:

2.   Documents shall be stored in the following Electronic Records Warehouse:

3.   Electronic Records shall be Electronically Signed by the following process(es):

K.   <u>Contract Consideration/Payment Terms</u>.

NAME1   NAME2

_____   _____
_____   _____
(Print Name)   (Print Name)

_____   _____
(Print Title)   (Print Title)

_____   _____
Date   Date

Address for Notices: Address for Notices:

_____   _____
_____   _____
_____   _____

Crosswalk of Provisions
Agreement for Protection of Information

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
Intro	Identify Agreement, parties and effective date	Necessary to orient interpretation				
Recital I	Describe parties and intent to disclose information	Identify party and relationship between parties governed by the Agreement	Suggested to indicate applicability of HIPAA by specification of party status as Covered Entity (health plan, health care provider, health care clearinghouse). HIPAA 1171(2), (3), (5); HIPAA 117 2(a); Privacy Rule 160.102(a), .103; Security Rule 142.102, .103; Transactions Rule 160.102, .103	Suggested to indicate applicability of G-L-B to parties as "financial institution" or "affiliate." G-L-B 509(3), (5), (6) FTC Rule 313.3(a), (k), (m)	Suggested to indicate regulated status as "health care provider," "third party payor" under RCW 70.02.010(7), (13); or "financial institution," "affiliate," "health care provider" or insurance company "licensee" under WAC 284-04-120(1), (11), (14), (18), (19), (20)	Note that this Recital can be copied or expanded to accommodate more than two parties
Recital II	Acknowledge that some information to be disclosed is protected by law and state intention to comply with protection laws	Used to support interpretation of Agreement	Suggested to demonstrate intent to comply with HIPAA	Supports G-L-B compliance intent	Supports state law compliance intent	
Text	Consideration recital	Necessary				
Sec. A	Definitions and principles for interpretation of Agreement	Desirable to help direct interpretation of Agreement				
Sec. A(1)	Definitions of material terms	Suggested to direct interpretation of	Suggested to specifically incorporate terms defined in	Terms intended to encompass G-L-B	Terms intended to encompass state law	

Section	Contents		General and Miscellaneous Legal Practice		Health Insurance Portability and Accountability Act of 1996 (HIPAA)		Gramm-Leach-Bliley (G-L-B)		State Law (WASH)		Comments
			Agreement		HIPAA and implementing regulations		defined terms		defined terms		
A.(1)	a	Access	a		a	Security Rule 142.304	a		a		
	b	Aggregate	b		b	Privacy Rule 164.501	b		b		
	c	Agreement	c		c		c		c		
	d	Anonymize	d		d	Security Rule 142.304	d		d		
	e	Audit Trail	e		e	Security Rule 142.308(c)	e		e		
	f	Authenticate	f	HCFA Internet Policy	f	Security Rule 142.304	f		f		
	g	Authorization	g	Identified processes for authorization to control who is or is may be claimed as party's agent	g	Privacy Rule 164.502(b), .514(d); Security Rule 142.308(a)(5), (7)	g		g		
	h	Authorized Person	h		h		h		h		
	i	Authorized Purpose	i		i		i		i		
	j	Copy	j		j		j		j		
	k	Criminal Conviction	k	Best practice to support avoidance of liability	k		k		k		
	l	Disclose	l		l	Privacy Rule 164.501			l		
	m	Disclosing Party	m		m		l		m		
	n	Disclosure Accounting	n		n	Privacy Rule 164.508	m		n		
	o	Effective Date	o		o		n		o		
	p	Electronic Record	p	21 CFR 11.3(b)(6)	p		o		p	RCW 19.34.020(13)	
							p				
	q	Electronic Records	q		q	Security Rule 142.310			q		
							q				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
	Warehouse					
	r Electronic Signature	r 15 USC 7006(4)	r Security Rule 142.310	r	r RCW 19.34.020(14)	
	s	s	s	s	s	
	t HHS	t	t	s	t	
	u HIPAA	u	u	t	u	
	v Individual	v	v Privacy Rule 164.501	u	v	
	w Information Privacy and Protection Laws	w	w	v w	w	
	x Minimum Necessary Information	x	x Privacy Rule 164.502(b), .514(d)	x G-L-B 509(7) [	x RCW 70.02.050	
	y Process	y	y	y	y	
	z Protect	z	z Privacy Rule 164.530(c)	z	z	
	aa Protected Information	aa	aa Privacy Rule 164.501, HIPAA 1171(4), (6)	aa G-L-B 509(4), FTC Rule 313.3(n)	aa RCW 70.02.010(6), WAC 284-04-120(21)	
	bb Receive	bb	bb	bb	bb	
	cc Receiving Party	cc	cc	cc	cc	
	dd Security	dd	dd Security Rule at 43,249		dd	
	ee Specification Addendum	ee	ee	dd ee	ee	
	ff Subcontractor	ff	ff	ff	ff	
	gg Term	gg	gg	gg	gg	
	hh Third Party	hh	hh	hh	hh	
	ii Transaction	ii	ii Transactions Rule 162.103	ii	ii	
	jj Transmit	jj	jj Transactions Rule 162.103	jj	jj	
	kk Unauthorized	kk	kk	kk	kk	
	ll Use	ll	ll Privacy Rule 164.501	ll	ll	
	mm Workforce	mm	mm Privacy Rule 164.103	mm	mm	
	nn Writing	nn Suggested	nn	nn	nn	

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
A.2	Parties can be either Disclosing or Receiving parties	Suggested to clarify that the provisions of the Agreement apply to any party depending on the circumstances of disclosure				Suggested to clarify that the provisions of the Agreement, specifically those regarding compliance with privacy laws, apply to any party depending on the circumstances of disclosure
A.3	Allows incorporation of specifications addenda into the Agreement	Required to make the addenda binding and enforceable under this Agreement				
A.4	Agreement shall be interpreted consistently with privacy laws, etc.	Suggested to clarify interpretation	Suggested	Suggested	Suggested	
B	Standards for Transactions	Intended to establish framework for developing specific implementations				
B.1	Minimum Necessary Information		Privacy Rule 164.502(b), .514(d)	FTC Rule 313.10 – 313.12	RCW 70.020.050; WAC 284-04-300, -305, -310	This provision will require analysis when privacy laws overlap.
B.2	Specifications Addenda	Defines contents and incorporation of ancillary agreement				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
		for transaction implementations				
B.3	Disclosing Party Transmission	States obligation to comply with addenda				
B.4	Receiving Party Receipt	States obligation to comply with addenda				
B.5	Intermediaries	Permits use of identified intermediaries without release of obligations		FTC Rule 313.14	WAC 284-04-045	Functions to be performed by Intermediary need analysis if privacy laws overlap
B.6	Encryption	HCFA Internet Policy				
C.	Information Protection by Disclosing Parties	States information protection conditions Disclosing Party must maintain		G-L-B 501(b) (authority to promulgate financial institution information safeguard rules)	RCW 70.02.150 ("reasonable safeguards for security"), WAC 284-04-500 (health information privacy policies and procedures)	
C.1.a	Maintain conditions to establish right to disclose	Allocates responsibility to Disclosing Party	Right to disclose generally depends on Disclosing Party fulfillment of documentation, procedural requirements Receiving Party cannot verify	Right to disclose generally depends on Disclosing Party fulfillment of documentation, procedural requirements Receiving Party cannot verify	Right to disclose generally depends on Disclosing Party fulfillment of documentation, procedural requirements Receiving Party cannot verify	
C.1.b	Disclose minimum	Defines scope of	Tie in to analysis for Section	Tie in to analysis for	Tie in to analysis for	

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
	necessary information in party's possession or control	information obliged to disclose; no obligation to seek data beyond control	B(1).	Section B(1).	Section B(1).	
C.1.c	Virus check electronic data	Becoming standard practice	Virus check systems required under Security Rule 142.308			Suggested Chain of Trust Agreement provision
C.2	Computer system administration	Access to computer system creates risk of intrusion	Use of computer access systems creates Security Rule compliance obligations.			Chain of Trust Agreement provision
C.2.a	Security officer		Implied under Security Rule			
C.2.b	Security procedures, etc.	Allocates responsibility for management of own systems to Disclosing Party	Necessary to create "chain of trust" as implied in Security Rule requirement of chain of trust agreement. Security Rule 142.308			Chain of Trust Agreement provision
C.2.c	Security incident notification	Allows (and implicitly requires) Receiving Party to mitigate damage	Best security practice probably implicit in Security Rule			
C.2.d	Security assessments	Emerging "best practice"	Security Rule 142.308			
D.	Information Protection Obligations of Receiving Party	States information protection conditions Receiving Party must maintain	Primary section intended to comply with Business Associate Contract and Chain of Trust Agreement requirements of Privacy and Security Rules	Primary section intended to comply with G-L-B disclosure and use limitation contract requirements. See FTC Rule 313.13(a)(ii)	Primary section intended to comply with WAC 284-04-400(1)(a)(ii)	G-L-B Contract provisions
D.1	General obligations					Obligations follow information, so apply until Protected Information no longer in party's

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						control
D.1.a	Use limitations		Privacy Rule 164.504(e)(2)(i)(A), .504(e)(2)(ii)(A), .504(e)(4)(I).	FTC Rule 313.10 - .15	See WAC 284-04-300 - 410	Business Associate Contract provision; G-L-B Disclosure contract provision
D.1.b	Safeguards required		Privacy Rule 164.504(e)(2)(ii)(B)			Business Associate Contract provision
D.1.c	Unauthorized disclosure/use notification		Privacy Rule 164.504(e)(2)(ii)(C)			Business Associate Contract provision
D.1.d	Disclosure to third parties		Privacy Rule 164.504(e)(2)(ii)(D)			Business Associate Contract provision
D.1.d.i	Minimum necessary disclosure		Incorporates Privacy Rule standard			
D.1.d.2	Disclosure to subcontractors		Privacy Rule 164.504(e)(2)(ii)(D), .504(e)(2)(ii)(D), .504(e)(4)(i)(B).			Business Associate Contract provision. Note includes terms precluding transfer of ownership of information and requiring return/destruction of information
D.1.d.iii	Disclosure required by law		Privacy Rule 164.504(e)(4)(ii)		RCW 70.02.050(2)	Business Associate Contract provision. Note includes Disclosing Party notice provision, protecting Disclosing Party interest in knowing in case of investigation, etc.

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
D.1.d.iv	Disclosure to individual		Privacy Rule 164.504(e)(2)(ii)(E)		RCW 70.02.080	Business Associate Contract provision. It may be desirable to require such disclosure be according to procedures agreed under Section E.
D.1.d.v	Other permitted disclosures		See Privacy Rule 164.501 (health care operations)			Note that some permitted disclosures are not subject to Business Associate Contracts
D.2	Computer system administration					Chain of Trust Agreement provisions
D.2.a	Security officer		Implied under Security Rule, so should be required under contract			Chain of Trust Agreement provision
D.2.b	System access controls.		Required under Security Rule 142.308, so should be required under contract			Chain of Trust Agreement provision
D.2.c	Notification of security incidents		System intrusion incident creates risk of Unauthorized Access to Protected Information. If so notification would be required under Privacy Rule 164.504(e)(2)(ii)(B)			Business Associate Contract provision, if computer systems used. Chain of Trust Agreement provision
D.2.d	System security policies, etc.		Required under Security Rule 142.308, so should be required by contract			
D.2.e	System assessments,		Required under Security Rule			

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
	etc.		142.308, so should be required by contract			
E	Privacy practices			FTC Rule 313.4 – 313.9	WAC 284-04-200 - -225	Note that different types of entities may have different privacy practices obligations. This section is structured for coordination of practices and documentation, not uniformity
E.1	Privacy officers		Privacy Rule 164.520(b)(1)(vii), .524(e)(2)			Privacy management may be complex for many Covered Entities, including the assignment of mandatory duties to identified individuals as privacy officers, who would be the appropriate coordinate with other parties.
E.2	Privacy policies, consents, notices, etc.		Privacy Rule 164.506, .164.508, .520,	FTC Rule 313.4 – 313.9	RCW 70.02.030 - .040WAC 284-04-200 - -225	Not all parties will be required to obtain consents or authorizations, or publish privacy notices. Those which must or choose to do so

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						must provide them to other parties and ensure they are consistent with their obligations under the Agreement
E.3	Additional individual privacy protections, revocation of authorization		Privacy Rule 164.522	Compare G-L-B "opt out" requirements, FTC Rule 313.7	Compare "revocation of authorization," RCW 70.02.040; "opt out" requirements of WAC 284-04-215	
E.4	Inspection, copying, amendment of records		Privacy Rule 164.524, .526		RCW 70.02.080 - .110	
E.5	Party receiving amendment of record must notify other parties of change		Privacy Rule 164.524(c)(3)(ii)			
F	Information ownership	Preferred to clarify relationship to information. Applies to all information, protected or otherwise, received under the Agreement, except information also available through legitimate sources. The language of the provision is standard in trade secrets contracting.				Information management systems vendors and processing companies may claim ownership in or attempt to sell information as secondary line of business. This may be especially problematic with companies in bankruptcy, where information may be

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						considered one of the few valuable assets of a company
F.1	Disclosing party presumed to own information	Consistent with standard if not universal practice				
F.2	Transfer of information does not transfer ownership	Good practice to clarify intent not to transfer ownership				
F.3	Receiving party right of possession	Possession is limited ownership interest				Clarifies that Receiving party has e.g. no right to sell information
F.4	Receiving party rights to use and disclose	Limits rights of receiving party				
F.5	No right to anonymize or aggregate					Receiving party should not profit from anonymization or aggregation of information without disclosing party consent
F.6	No liens on information	Protects against ownership claims and may protect against receiving party creditor claims				
G	Return, archiving or destruction of information		Privacy Rule 164.504(e)(2)(ii)(I)			
G.1	Return originals or copies on termination	Good practice to maintain records for				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
		future dispute resolution				
G.2	Destruction of information by receiving party					Business Associate contract provision. Consider adequacy of methods of destruction given media
G.3	Archiving of information	Consistent with right of possession. Receiving party may have many legitimate reasons to want copies available	Privacy Rule 164.(e)(2)(ii)(I).			Business Associate contract provision. Third party escrow may be desirable if available
G.4	Application to subcontractors		Not spelled out but necessary to ensure full compliance			
H.	Warranties	Clarifies responsibilities and so allocates risk and liabilities				
H.1	Mutual warranties	Standard				
H.1.a	Legal status	Standard				
H.1.b	Legal powers	Standard				
H.1.c	Fulfilled conditions to agreement	Standard				Presumes compliance with all necessary consent, authorization, notice documentation, etc.
H.1.d	Will comply with privacy laws	Good practice				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
H.1.e	Not barred from federal health programs	Federal program prohibition comes with proven violation of federal laws, e.g. fraud and abuse or anti-kickback				Helpful to avoid contracting with untrustworthy parties, and inviting governmental scrutiny and possible legal violation
H.1.f	No criminal convictions	See H.1.e				Helpful to avoid contracting with untrustworthy parties, and inviting governmental scrutiny and possible legal violation
H.1.g	Will comply with Agreement	Good practice				
H.2	Indemnification	Standard provision requiring party in breach of Agreement to assume financial risk and burdens of breach				
I	Dispute resolution					
I.2	Applicable law	Standard. Note that even with a specification of state law, law of state where Individuals reside may apply				Consider jurisdiction(s) which might apply in case of multi-state transactions
I.2	Alternative dispute	None are				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
	resolution procedures	specifically suggested, but careful consideration of alternatives is strongly recommended due to costs, length of normal judicial processes				
I.3	Jurisdiction and venue	Standard. Usually chosen for convenience to administrative or operational offices of parties				
I.4	Legal fees and costs	Standard. Note that in absence of provision for payment of attorneys fees by losing party, each party usually pays own fees.				
J.	Term and termination					
J.1	Effective date	Standard				
J.2	Termination of Specifications Addenda	Clarifies relationship between documents				
J.3	Effect of multiple parties					Allows for termination between two parties with agreement effective

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						between any remaining parties
J.4	Effect on obligations	Standard				Not all obligations will terminate upon termination of Agreement; e.g., protection of archived information
J.5	Term	One of a number of standard approaches				Note minimum one year term may be desirable for anti-kickback, fraud and abuse compliance in some cases
J.6	Conditions allowing immediate termination	Desirable where some kinds of material failure by other party may put terminating party at serious risk				
J.6.a	Termination for material breach of privacy protections	Desirable	Privacy Rule 164.504(e)(iii)			Business Associate Contract provision
J.6.b	Termination for criminal or health care malfeasance finding	Desirable				
J.6.c	Insolvency	Standard				Insolvency raises questions of both ability to perform under Agreement, and possible

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						incentive to sell or otherwise misuse information for profit
J.6.d	Trustee appointed	Standard				Trustee raises questions of both ability to perform under Agreement, and possible court intervention leading to sale or other loss of information
J.6.e	Bankruptcy	Standard				Bankruptcy raises questions of both ability to perform under Agreement and possible court intervention leading to sale or other loss of information
J.6.f	Dissolution or liquidation	Standard				Loss of legal entity status destroys enforceability of Agreement
J.7	Termination for curable breach	One of a number of standard approaches				
J.8	Termination for good cause	Alternative available where neither grounds for immediate termination nor curable breach exists, but other				

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
		"good cause" exists. Based on standard provisions in health care contracting				
J.9	Termination due to change in law	Desirable given emerging nature of information protection laws				Termination cannot proceed without attempt to amend Agreement to come into compliance with changed law.
K	Miscellaneous					
K.1	Amendment of Agreement	Desirable				
K.1.a	Specifications Addendum	Allows amendment of addenda without amendment of Agreement				
K.1.b	Unilateral modification internal policies, processes, etc.		Desirable to permit internal changes to accommodate HIPAA compliance needs			
K.1.c	Amendment to accommodate change in law	Desirable given emerging nature of information protection laws				Process must be followed as condition to termination due to change in law, to allow parties to attempt to adapt
K.2	Integration clause	Standard				
K.3	Limitation on assignment	Standard				
K.4	No agency, etc.	Standard				
K.5	Notices	Standard				Note this clause

Section	Contents	General and Miscellaneous Legal Practice	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Gramm-Leach-Bliley (G-L-B)	State Law (WASH)	Comments
						provides for electronic notices, These should not be used without implementing an electronic records strategy
K.6	Use of Electronic Signatures, Records	Emerging practices in implementation of federal Electronic Signatures in Global and National Commerce Act ("E-SIGN"), Uniform Electronic Transactions Act ("UETA"), etc.			RCW 19.34 privileges digital signatures based on certificates issued by state-licensed certificate authorities as valid for all but a few legal purposes.	