



North Carolina Healthcare Information
and Communications Alliance, Inc.

Briefing Packet to Support the Expected Changes to Business Associate Agreements Mandated by the American Recovery and Reinvestment Act of 2009 (“ARRA”)

- **Notice to Covered Entities Under HIPAA Regarding New Requirements under the ARRA HITECH Act**
- **Template for Business Associate Alert and New Breach Notification Requirements**
- **Summary of Selected ARRA and HITECH Act (HIPAA 2) Provisions Related to Business Associates**

**Prepared by the NCHICA Business Associate
Agreement Task Force**

December 8, 2009

Prepared by the NCHICA Business Associate Agreement Task Force

NOTICE TO COVERED ENTITIES UNDER HIPAA REGARDING NEW REQUIREMENTS UNDER THE ARRA HITECH ACT

As many of you may be aware, the American Recovery and Reinvestment Act of 2009 (“ARRA”) creates a variety of incentives for health care providers to develop and utilize electronic medical records. However, many may not realize that its provisions, commonly known as the “HITECH Act,” make significant changes to HIPAA in three broad categories: business associate requirements, breach notification, and penalties. The breach notification requirements became effective September 23, 2009. Other requirements become effective in February, 2010. More details about the new requirements will be provided to the health care community through regulations expected before February, 2010.

Some of the changes extend the reach of the HIPAA security rules and certain privacy requirements to business associates of covered entities. NCHICA is revising its model Business Associate Agreement to incorporate updated provisions. The new revised version will be available as soon as the upcoming regulations are finalized. It is unclear in the ARRA whether existing Business Associate Agreements must be amended in order to comply with the new requirements, however, there may be business reasons for revising these agreements regardless of the ultimate regulatory determination on whether amendments are required. You may choose to wait until the new regulations are available before amending your Business Associate Agreements. However, if new Business Associate Agreements are required, or you determine that existing Business Associate Agreements must be amended, prior to the issuance of the new regulations, one approach which may be used is to include in the new or revised Business Associate Agreement some sort of “placeholder” indicating amendments may be required following issuance of the new regulations. An example of such a placeholder might be:

“The parties acknowledge that the American Recovery and Reinvestment Act of 2009 (“ARRA”) requires the Secretary of Health and Human Services to promulgate regulations and interpretative guidance that are not available at the time of executing this Business Associate Agreement. In the event Covered Entity determines in good faith that any such regulation or guidance adopted or amended after the execution of this Business Associate Agreement shall cause any paragraph or provision of this Business Associate Agreement to be invalid, void or in any manner unlawful or subject either party to penalty, then the parties agree to renegotiate in good faith to amend this Business Associate Agreement to comply with the change in law, regulation or interpretative guidance.”

In addition, a covered entity may want to insert a “placeholder” indicating that the provisions of the Business Associate Agreement are deemed to be amended if HIPAA is amended. The current NCHICA draft modified Business Associate Agreement contains such provisions.

NCHICA is providing the attached Business Associate Alert as a sample document which might be sent to existing business associates to notify them of the upcoming changes and the current applicability of the breach notification requirements. Covered entities may want to reference in the Business Associate Alert any existing Business Associate Agreement with the Business Associates to which the Alert is sent. NCHICA has also prepared the attached informational document to provide some background information on ARRA and HITECH.

NCHICA does not intend to provide you with legal advice regarding ARRA or HITECH, and you should contact your legal council to discuss these new requirements.

[COVERED ENTITY LETTERHEAD]

BUSINESS ASSOCIATE ALERT AND NEW BREACH NOTIFICATION REQUIREMENTS

As our business associate under HIPAA, please be aware that the American Recovery and Reinvestment Act of 2009 (“ARRA”), including its provisions commonly known as the “HITECH Act,” could have a significant impact on the duties, responsibilities and liabilities of your organization. The breach notification requirements under ARRA described below became effective September 23, 2009. Other requirements become effective in February, 2010. The ARRA’s changes extend the reach of the HIPAA security rules to business associates of covered entities. In addition, new privacy requirements of covered entities under the HITECH Act will also apply to business associates. Business associates now face civil and criminal penalties for non-compliance with duties previously imposed on Covered Entities only.

Additional regulations are expected soon that will provide more details about your new obligations under the HITECH Act. Such regulations may require amendments to our current Business Associate Agreement.

Under the HITECH Act, business associates must notify the covered entity about breaches or suspected breaches of the privacy or security of protected health information that are discovered by the business associate. The notification should be made to us as soon as you discover the breach.

We recommend that you consult with your legal counsel to address your new and modified requirements under HIPAA and HITECH.

Prepared by the NCHICA Business Associate Agreement Task Force

Nothing in this document or the revised Business Associate Agreement template are intended to provide legal advice, and the reader is directed to consult with an attorney regarding legal advice with respect to these requirements and to answer all questions.

Summary of Selected ARRA and HITECH Act (HIPAA 2) Provisions Related to Business Associates

As part of the American Recovery and Reinvestment Act of 2009 (ARRA), Congress created a wide range of incentives for health care providers to develop and utilize electronic medical records. As part of this legislation, in the section called the HITECH Act (parts of which are sometimes known as “HIPAA 2”), significant changes have been made to HIPAA in three broad categories: business associates, breach notification, and penalties. Specifically, these changes, which take effect February 2010, extend the effective reach of HIPAA coverage to business associates of HIPAA Covered Entities. Prior to this new statute, business associates were not directly required to meet the obligations by statute with respect to Administrative Safeguards (45 CFR §164.308), Physical Safeguards (45 CFR §164.310), Technical Safeguards (45 CFR §164.312), and Procedure and Documentation Requirements (45 CFR §164.316) and certain of the privacy requirements. Business Associates were required to comply with these and other requirements through Business Associate Agreements. Now, however, Business Associate Agreements should be revised by the HIPAA Covered Entity to require their Business Associates to comply with these additional requirements as well. Especially, Business Associates should be made aware that penalties for wrongful disclosure of protected health information (PHI) now apply to Business Associates to the same extent as for HIPAA Covered Entities. These penalties include significant civil fines and possible imprisonment.

Security Requirements Summary and Links to Regulations

The following are links and references to guidance, presentations, and other information regarding the HIPAA Security Rule which we attach for your information only, and not in any way as advice or opinions regarding compliance with the HIPAA Security Rule.

A complete list of the papers available can be found at:

http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage

CMS has a series of papers, including the one found at the following link, which seem to provide a good overview of the Security Rule:

<http://www.epcc.edu/Portals/62/documents/SecurityFiles/HIPAA-1996-CMS%20Security%20101.pdf>

Business Associate and PHR Vendor Modifications

The American Recovery and Reinvestment Act of 2009 (“ARRA”) extends the reach of HIPAA coverage to Business Associates (“BAs”) of HIPAA Covered Entities (“CEs”). The reach of HIPAA coverage is extended as follows:

- ARRA makes the security provisions of HIPAA, including the new security requirements that are added by ARRA, directly applicable to BAs. Thus, rather than simply being obligated to comply through their business associate agreements, BAs now are directly obligated to comply, and
- ARRA also mandates disclosures of any Protected Health Information (“PHI”) that is not secured through the use of a technology or methodology specified by the Secretary in guidance posted within 60 days of enactment of ARRA and annual updates. CEs must disclose any breach of Unsecured PHI (“UPHI”), with the deadlines and mode of the notices staged based on the scope of the breach. BAs are required to notify their CEs.

A. EXTENSION OF HIPAA PRIVACY AND SECURITY TO BUSINESS ASSOCIATES

Part 1, Section 13401:

- Subsection (a) states that the security provisions of HIPAA shall apply to BAs of CEs in the same manner that such sections apply to CEs. Also, the additional security requirements imposed in the ARRA on CEs shall apply equally to BAs.
 - See 45 CFR 164.308 – Administrative Safeguards
 - See 45 CFR 164.310 – Physical Safeguards
 - See 45 CFR 164.312 – Technical Safeguards
 - See 45 CFR 164.316 – Policies and Procedures and Documentation Requirements
- Subsection (b) makes all potential civil and criminal penalties under 42 U.S.C. 1320d-5 and 42 U.S.C. 1320d-6 for CEs in violation of a security provision applicable equally to BAs.

Part 1, Section 13404:

- Subsection (a) states that BAs of CEs that obtain or create PHI pursuant to a written contract or arrangement as described in 45 CFR 164.502(e)(2) are subject to all of the privacy provisions in 45 CFR 164.504(e) that govern CEs. Also, the additional privacy requirements imposed in the ARRA on CEs shall apply equally to BAs (and shall be incorporated in the business associate agreement between CEs and BAs).
- Subsection (b) imposes all of the requirements of 45 CFR 164.504(e) and 45 CFR 164.502(e) on BAs just as they are imposed on CEs.

- Subsection (c) makes all potential civil and criminal penalties under 42 U.S.C. 1320d-5 and 42 U.S.C. 1320d-6 for CEs in violation of a privacy provision applicable equally to BAs.

Part 1, Section 13405:

- Subsection (a) imposes a duty on a CE to comply with a restriction on disclosure of PHI that is requested by an individual pursuant to 45 CFR 164.522(a)(1)(i)(A), except as otherwise required by law or pursuant to 45 CFR 164.522(a)(1)(ii) if the disclosure is to a health plan for purposes of carrying out payment or health care operations (non-treatment), and the PHI pertains solely to a health care item or service for which the provider has been paid out of pocket in full.
- Subsection (b) mandates that disclosures be limited to the limited data set or the minimum necessary disclosure, with all current exceptions remaining applicable. Said limited data set is defined in 45 CFR 164.514(e)(2) and if that standard is followed, then the CE will be deemed to be in compliance with 45 CFR 164.502(b)(1). No later than 18 months after the date of enactment of this section, the Secretary shall issue guidance on the interpretation of what constitutes a minimum necessary disclosure, and once that guidance is issued, then it will control over the limited data set standard, as defined therein. The BA or CE disclosing such information is the appropriate party for determining what constitutes a minimum necessary disclosure. Nothing in Subsection (b) shall apply to the restriction of de-identified PHI.
- Subsection (c) governs the accounting of certain PHI disclosures if CEs are using electronic health records. CEs that use electronic health records with respect to PHI, as governed under 45 CFR 164.528, shall not have the benefit of the exception in paragraph (a)(1)(i) of that section and individuals that request an accounting of disclosures described in such paragraph shall have a right to the accounting for a period of up to three years prior to their request. The subsection goes on to place the duty on the Secretary to promulgate regulations to set up the boundaries for disclosures and information that is to be included, taking into consideration the individuals' rights and the administrative burden on the accounting. When a request for an accounting is received, a CE shall elect to provide either an accounting of the disclosures made by the CE and any BAs acting on behalf of the CE, or an account of the disclosures made by the CE and a list of all BAs and the contact information for any BA acting on behalf of the CE. Then the BA shall provide their own accounting upon request by an individual directly to the BA. The effective dates are any disclosure made on or after January 1, 2014 for CEs that acquire electronic health records prior to January 1, 2009. For those acquiring electronic health records after January 1, 2009, any disclosure made on and after January 1, 2011, or the date that the CE acquires electronic health records, shall be covered by this paragraph. The Secretary can set a later date for the applicable time periods above if deemed necessary, but that date shall not be later than 2016 in the first scenario or 2013 in the second.

- Subsection (d) places a prohibition on the receipt of any remuneration in exchange for any PHI of an individual, unless the CE obtains a valid, specified authorization in accordance with 45 CFR 164.508. Exceptions to the rule stated herein are in cases where the purpose for the exchange is for public health activities (see 45 CFR 164.512(b)), research with a valid price exchange (see 45 CFR 164.501 and 164.512(i), treatment of the individual (subject to regulations by the Secretary), health care operation (see definition in 45 CFR 164.501(6)(iv), activities between a CE and BA pursuant to a request covered under their business associate agreement, to provide an individual with a copy of the individual's PHI (see 45 CFR 164.524), or as otherwise determined by the Secretary to be similarly necessary and appropriate as said exceptions hereinabove. Not later than 18 months the Secretary shall promulgate regulations to carry out this subsection and in doing so, shall consider the price of preparation and transmittal in determining the impact of restricting remuneration for the exception covering public health activities as to not impede those activities or research. These shall become effective and apply to exchanges occurring on or after the date that is 6 months after the date of promulgation of final regulations implementing this subsection.
- Subsection (e) covers access to certain information in electronic format and states that in applying 45 CFR 164.524, a CE that maintains an electronic health record must provide that to an individual in electronic format if the individual requests such. In addition, the individual can request it be transmitted directly to an entity or person of their choice so long as that entity or person is clear, conspicuous and specific. Any fee that a CE may charge for an electronic form transmittal may not exceed their actual labor cost in responding to the request, notwithstanding 45 CFR 164.524(c)(4).

Part 1, Section 13406:

- Subsection (a) provides that a communication by a CE or BA about a product or service and that encourages recipients of the communication to purchase or use the product or service will not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations, unless the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of such title.
- Subsection (b) provides, that, even if the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501, it will not be considered "health care operations" unless the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment received by the CE for making such communication is reasonable in amount and each of the following apply: the communication is made by the CE, the CE obtains a valid authorization from the recipient, or the communication is made by a BA on behalf of the CE and the communication is consistent with the Business Associate Agreement.

B. BREACH NOTIFICATION REQUIREMENTS

The ARRA also imposes more stringent breach notification requirements on CEs and BAs when there is a discovery of a breach of UPHI. The requirements for notification of a breach to various parties are as follows:

Part 1, Section 13402:

- Subsection (a) imposes a duty on CEs that discover a breach of UPHI to notify each individual whose UPHI has been, or is reasonably believed by the CEs to have been, accessed, acquired, or disclosed as a result of such breach.
- Subsection (b) imposes a duty on BAs that discover a breach as discussed in (a) above to notify the CEs with the identification of the each individual whose UPHI has been, or is reasonably believed to have been accessed, acquired, or discovered during the breach.
- Subsection (c) indicates that a breach shall be treated as discovered on the first day such breach is known to the CEs or BAs or should reasonably have been known to have occurred.
- Subsection (d) imposes certain timelines on notification, as follows:
 - Unless there is a delay for law enforcement purposes, as defined in subsection (g), notice shall be without unreasonable delay, not to exceed 60 calendar days from discovery of the breach.
 - The CEs and BAs have the duty to prove all timelines were met, as well as duty to prove the necessity of any delay
- Subsection (e) lays out the requirement for and methods of notice required in situations where a breach is discovered:
 - Notice to an individual shall be provided promptly and in the following form:
 - Written notification to the individual (or next of kin if individual is deceased) sent via first-class mail to the last known address of whichever is applicable
 - Notice can be sent via electronic mail if individual specified such as a preference
 - Notice can come in one or more mailings when information is available
 - If no sufficient or up-to-date contact information is available, then a substitute form of notice shall be provided by Secretary
 - In the case where there are 10 or more individuals for which there is insufficient information, a conspicuous posting for a period determined by the Secretary of Health and Human Services (“the Secretary”) on the home page of the website of the CEs, or notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside
 - Notice in media or web postings shall include a toll free phone number for inquiries by individuals regarding

whether or not their UPHI is included in the possible breach

- If it is discovered that the UPHI of more than 500 residents of a State or jurisdiction has been, or is reasonably believed to have been, breached, then notice shall be provided to prominent media outlets serving the State or jurisdiction.
- Notice shall be provided to the Secretary by CEs involved in breach situations
 - If breach of 500 or more individuals' UPHI, then notice shall be provided immediately
 - If breach of less than 500, CEs may keep a log and submit the breach notices to the Secretary annually
- The Secretary shall post breaches of 500 or more individuals' UPHI on the Department of Health and Human Services' public website

The Department of Health and Human Services' public website contains more information on breach notification at:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

The Guidance published in the Federal Register can be found at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>

C. PHR VENDOR REQUIREMENTS

Part 1, Section 13407:

- Subsection (a) places a duty on vendors of PHR, following discovery of a breach of security of unsecured PHR identifiable health information in a PHR maintained or offered by said vendor to notify each individual whose unsecured PHR identifiable health information was acquired by an unauthorized person and the Federal Trade Commission.
- Subsection (b) places a duty of notification on third party service providers of vendors in the case of a breach to notify the vendor or entity, respectively, and such notification shall include the identification of each individual affected.
- Subsection (c) incorporates, by reference, Subsections (c), (d), (e) and (f) of section 13402 (each is outlined hereinabove) and states that those shall apply to vendors under this section.
- Subsection (e) indicates that a violation of (a) or (b) of section 13407 shall be treated as an unfair or deceptive act or practice under 15 U.S.C. 57a(a)(1)(B).

Glossary:

1) **Breach** –

(A) In General – The term “breach” means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(B) Exceptions – The term “breach” does not include—

(i) any unintentional acquisition, access, or use of protected health information by any employee or individual acting under the authority of a covered entity or business associate if—

(a) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

(b) such information is not further acquired, accessed, used, or disclosed by any person; or

(c) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at some facility; and

(ii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

HITECH Act Sec. 13400(1)

2) **Business Associate** -

(A) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in Sec. 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(a) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(b) Any other function or activity regulated by this subchapter; or

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

- from another business associate of such covered entity or arrangement, to the person.
- (B) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
- (C) A covered entity may be a business associate of another covered entity. *45 CFR 160.103*
- 3) **Electronic Health Record (EHR)** – The term “electronic health record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. *HITECH Act Sec. 13400(5)*
- 4) **Electronic Protected Health Information (ePHI)** - Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section. *45 CFR 160.103*
- 5) **E-prescribing gateway (EPG)** – an internet configuration allowing access to EHRs and providing physicians the ability to prescribe over the internet.
- 6) **Health Information Exchange (HIE)*** – The electronic movement of health-related information among organizations according to nationally recognized standards.
- 7) **Health Information Organization (HIO)*** – An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.
- 8) **Personal Health Record (PHR)** – The term “personal health record” means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. *HITECH Act Sec. 13400(11)*
- 9) **Personal Health Record (PHR) vendor** – any entity, other than a covered entity that offers or maintains a personal health record. *HITECH Act Sec. 13400(18)*
- 10) **Protected Health Information (PHI)** - Protected health information means individually identifiable health information:
- (A) Except as provided in paragraph (2) of this definition, that is:
- (i) Transmitted by electronic media;
 - (ii) Maintained in electronic media; or
 - (iii) Transmitted or maintained in any other form or medium.

(B) Protected health information excludes individually identifiable health information in:

- (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
- (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
- (iii) Employment records held by a covered entity in its role as employer. *45 CFR 160.103*

11) **Regional Health Information Organization (RHIO)*** – A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.