



**Franklin J. Hickman  
Janet L. Lowder  
David A. Myers  
Elena A. Lidrbauch  
Sandra J. Buzney  
Judith C. Saltzman  
Mary B. McKee  
Amanda M. Buzo  
Lisa M. Garvin**

**Penton Building  
1300 East Ninth Street  
Suite 1020  
Cleveland, OH 44114  
Telephone (216) 861-0360  
Fax (216) 861-3113**

**5062 Waterford Dr.  
Sheffield Village, OH 44035  
Telephone (440) 323-1111  
Fax (440)323-4284**

**OVERVIEW OF RECENT CHANGES IN  
HIPAA AND OHIO PRIVACY LAWS**

**with sample Notice and BA Agreement**

**and**

**Guidance from Secretary of HHS**

Elena A. Lidrbauch  
Franklin J. Hickman  
December 3, 2009

This is a summary only and is not intended to provide legal advice.  
For individual issues, you should consult your attorney.

**TABLE OF CONTENTS**

Overview of Recent Changes in HIPAA and Ohio Privacy Laws.....1

Table of Effective Dates .....10

Sample Notice of Privacy Practices for DD Boards .....11

Sample BA Agreement .....16

Guidance from Secretary of HHS on secured PHI .....21

## **OVERVIEW OF RECENT CHANGES IN HIPAA AND OHIO PRIVACY LAWS**

There have been two major sets of changes during 2009 which affect privacy and confidentiality rules for DD Boards.

Ohio law has been amended to permit disclosure of the identity of an individual served by a DD Board if the individual's identity is needed for treatment or payment for services provided to the individual.<sup>1</sup> The same bill removed the duty to provide accountings for all disclosures of an eligible individual's identity.

The American Recovery and Reinvestment Act of 2009 (ARRA) enacted on February 17, 2009 adds additional requirements to HIPAA privacy and security rules.<sup>2</sup> DD Boards, COGs and Providers are subject to these new regulations, whether they function as a Covered Entity or a Business Associate<sup>3</sup>. The ARRA changes include enhanced notice requirements in the event of a breach and expanded civil sanctions for violations of HIPAA requirements. The ARRA imposes significant new requirements for Business Associates.

In response to the ARRA directive, the Department of Health and Human Services (HHS) recently issued two sets of interim final rules:

- Rules governing notification of breaches of unsecured protected health information. This rule went into effect on September 23, 2009;
- Rules explaining the enhanced penalties for breach of HIPAA requirements. These rules are effective on November 30, 2009.

There are a number of additional HIPAA requirements enacted through the ARRA which will become effective in future years. Further information will be provided as regulations regarding these requirements are enacted.

---

<sup>1</sup> Ohio Rev. Code ("RC") 5126.044(B)(4) as amended by H.B. 1, effective 10/16/09.

<sup>2</sup> These requirements were part of the Health Information Technology for Economic and Clinical Health (HITECH) Act which is a section of the ARRA.

<sup>3</sup> DD Boards are Covered Entities subject to HIPAA requirements as both Health Plans and Health Care Providers. In some situations, DD Boards may also function as Business Associates. Most Providers are Covered Entities as Health Care Providers. To the extent that COGs are doing specific tasks for each DD Board, the COG is acting as a Business Associate.

## **I. Changes in Ohio Law**

HB 1 made two significant changes in the confidentiality rules applicable to DD Boards, effective October 16, 2009. RC 5126.044.

The identity of an eligible individual may be disclosed without the individual's consent, if the identity of the individual is necessary for treatment or payment. RC 5126.044(B)(4). Treatment is defined as "provision, coordination, or management of services provided to an eligible person." Payment is defined as "activities undertaken by a service provider or governmental entity to obtain or provide reimbursement for services to an eligible person." RC 5126.044(A).

A strict construction of the language of statute as amended permits disclosure only of the identity of an individual for treatment or payment purposes; the language as currently enacted does not clearly permit release of records or reports on an individual without a written consent for the release.<sup>4</sup>

### **Summary of the New HIPAA Regulations on Notice of Breach**

Effective September 23, 2009, all HIPAA Covered Entities and their Business Associates are required to provide notice in the event of a breach of unsecured protected health information (PHI). Covered Entities must notify the affected individual, the Secretary of HHS and under some circumstances even the media. Business Associates must provide notice of a breach to the Covered Entity. Failure to comply may lead civil penalties which have been significantly increased under the ARRA revisions. Additionally civil penalties for HIPAA violations are being extended to Business Associates as well as Covered Entities.

#### **A. Breaches Subject to Notification**

Under the new regulations, notification requirements apply to breaches of unsecured PHI. To determine whether notification is required, the Covered Entity or Business Associate must first determine (1) whether there is a breach, and (2) whether the breach includes unsecured PHI. If the answer to both is yes, then notification is required.

---

<sup>4</sup> There may be an amendment in the future which will specifically permit release of reports and records on eligible individuals for treatment or payment purposes. Until the statute is changed, however, we believe that the current practice of obtaining consent for release of all information should continue, except for the explicit exceptions in RC 5126.044 (info needed for direct services contracts and for placement on waiting list).

## **B. Definition of a Breach**

A breach is the acquisition, access, use, or disclosure of PHI in an unauthorized manner which compromises the security or privacy of the PHI<sup>5</sup>. The following types of breaches are expressly excluded from this definition:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner prohibited by HIPAA;
2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same Covered Entity or Business Associate and the information is not further disclosed in a manner prohibited by HIPAA; or
3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.<sup>6</sup>

## **C. Definition of Unsecured PHI**

Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued and made available at <http://www.hhs.gov/ocr/privacy/>.<sup>7</sup> The regulations require this guidance to be updated annually. PHI which is secured as specified by the guidance will not be subject to notification in the event there is a breach of the secured PHI.

---

<sup>5</sup> 45 CFR §164.402

(1)(i) For purposes of this definition, compromises the security or privacy of the PHI means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of PHI that is part of a limited data set as defined by § 164.514(e)(2), does not compromise the security or privacy of the PHI.

<sup>6</sup> 45 CFR §164.402(2)

<sup>7</sup> 45 CFR §164.402; The commentary notes that “unsecured PHI can include information in any form or medium, including electronic, paper, or oral form.” 74 Fed. Reg. 42748

**D. Notification Requirements Applicable to the Covered Entity**

1. Notice of Breach to Individuals.

A covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach<sup>8</sup>. The notice must be written in plain language and to the extent possible, must include all of the following:

- (a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- (b) A description of the types of unsecured PHI involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- (c) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- (d) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- (e) Contact procedures for individuals to ask questions or learn additional information, which shall include a tollfree telephone number, an e-mail address, Web site, or postal address.<sup>9</sup>

---

<sup>8</sup> 45 CFR §164.404(a)(1); A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity. 45 CFR §164.404(a)(2)

<sup>9</sup> 45 CFR §164.404(c)

## 2. Method of Notice

The Covered Entity must provide notice in one of the following three formats, depending on circumstances<sup>10</sup>:

- (a) Written notice.
  - (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.
  - (ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or personal representative of the individual.
- (b) Substitute notice.

In the case that contact information is not available, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in where the individual is deceased.

- (i) In the case in which contact information is not available for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
- (ii) In the case in which contact information is not available for 10 or more individuals, then such substitute notice shall:
  - (A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
  - (B) Include a toll-free phone number that remains active for at least 90 days that an individual can call to learn whether the individual's unsecured PHI may be included in the breach.

---

<sup>10</sup> 45 CFR §164.404(d)

3. Additional notice in urgent situations.

In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may, in addition to providing written notice, contact individuals by telephone or other means, as appropriate.

**E. Other Parties Required to Receive Notice**

In addition to providing notice to the individual, the Covered Entity must notify the following entities:

1. Notification to the media<sup>11</sup>

For a breach of unsecured PHI involving more than 500 residents, a covered entity shall, notify prominent media outlets serving the State or jurisdiction. The content of the notice shall be the same as the notice provided to the individual.

2. Notification to the Secretary of HHS<sup>12</sup>.

For a breach of unsecured PHI involving more than 500 residents, a covered entity shall, notify the Secretary of HHS in the manner specified on the HHS Web site. For breaches of unsecured PHI involving less than 500 individuals, the covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notice to the Secretary of HHS of breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

**F. Timeliness of Notification**

In general, a Covered Entity must provide the required notice without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.<sup>13</sup>

The Covered Entity must delay providing notice if a law enforcement official states to the Covered Entity or Business Associate that providing notice would impede a criminal investigation or cause damage to national security. If such statement is in writing and specifies the time for which a delay is required, the Covered Entity or Business Associate shall delay such notice for the time period specified by the official. If the statement is made orally, the Covered Entity or Business Associate shall document the statement, including the identity of the official

---

<sup>11</sup> 45 CFR §164.406

<sup>12</sup> 45 CFR §164.408

<sup>13</sup> 45 CFR §164.404(b); 406(b); 410(b)

making the statement, and delay the notice temporarily and no longer than 30 days from the date of the oral statement, unless the law enforcement official submits a written statement during that time<sup>14</sup>.

## **II. Changes Affecting Business Associates**

### **A. General Changes**

The ARRA § 13401(a), 13404(a) now explicitly requires a business associate to meet the privacy standards applicable to covered entities, and following standards for PHI as well as security and management of PHI. These requirements formerly only applied to covered entities and now cover BAs as well.

- Administrative Safeguards in § 164.308
- Physical Safeguards in §164.310
- Technical Safeguards in §164.312
- Policies, procedures and documentation requirements in §164.316

Under the ARRA, If the BA determines that the covered entity has violated HIPAA privacy or security requirements, the BA has an affirmative duty to either terminate the BA agreement or to report violations to the Secretary. ARRA § 13404(b).

### **B. Notice of Breach**

A Business Associate must, following the discovery of a breach of unsecured protected health information, notify the Covered Entity of such breach.<sup>15</sup> The Business Associate is subject to the requirements applicable to a Covered Entity for timeliness of notification including requirements for a delayed notification.<sup>16</sup>

---

<sup>14</sup> 45 CFR §164.412

<sup>15</sup> ARRA 13404(b); 45 CFR §164.410; A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate. 45 CFR §164.410(a)(2)

<sup>16</sup> 164.410(b).

The notification provided by the Business Associate shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach.

A Business Associate must provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

### **III. Compliance with Minimum Necessary Requirements**

The ARRA states that, effective February 17, 2010, a covered entity complies with the minimum necessary requirement if the covered entity releases a limited data set or the minimum information necessary to accomplish the purpose of the disclosure. ARRA § 13405(b)(1)(A). The Secretary of HHS is required to issue guidance on what constitutes minimum necessary by August, 2010. ARRA § 13405(b)(1)(B). Once the guidance is issued, the guidance will be definitive.

### **IV. Accountings**

While Ohio law no longer requires accountings.

HIPAA requires accounting of disclosures from electronic health records for treatment, payment, health care operations for three years prior to the request. Other disclosures, such as breaches, must also be accounted for a period of six years prior to the request.

If the record exists on or before January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after January 1, 2014.

If the record exists after January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after the later of January 1, 2011 or the date the covered entity acquires the electronic health record.

BA agreements must include provisions on how accounting requirements will be met.<sup>17</sup>

The Secretary may delay the implementation dates for accountings.

---

<sup>17</sup> ARRA § 13405 (c)(3).

**V. Sanctions**

The ARRA has strengthened the civil sanctions which apply to violations of HIPAA. There were no changes to the criminal penalties.

The following table shows categories of violations and respective penalty amounts available:

<b>Violation category—Section 1176(a)(1)</b>	<b>Each violation</b>	<b>All such violations of an identical provision in a calendar year</b>
(A) Did Not Know.....	\$100–\$50,000	\$1,500,000
(B) Reasonable Cause.....	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected.....	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected.....	50,000	1,500,000

For violations occurring on or after February 18, 2009, the following affirmative defenses are available:

1. The violation is subject to criminal penalties, or
2. The covered entity establishes that the violation is
  - (a) Not due to willful neglect and
  - (b) Corrected during either:
    - (i) The 30 day period on which the covered entity knew or reasonably should have known, that the violation occurred; or
    - (ii) Such additional time as the Secretary of HHS determines to be appropriate.

**VI. Enforcement Procedures**

The ARRA has given State Attorney Generals the authority to file civil actions on behalf of individuals harmed by breaches of HIPAA requirements. The Attorney General may seek injunctive relief and damages on behalf of the individual. The maximum penalty amounts are substantially lower: \$100 per violation with a maximum of \$25,000 per year for identical violations. The Attorney General can collect attorney fees.

There are provisions for individuals to receive a portion of penalties received by HHS after the GAO conducts and study and HHS adopts rules for such distributions..

**SUMMARY OF EFFECTIVE DATES FOR ARRA RULES AND REGULATIONS**

<u>TITLE</u>	<u>EFFECTIVE DATE</u>	<u>CITE</u>
General ARRA privacy and related provisions	<b>02/17/2010</b> Except as shown below:	ARRA §13423
Duty of HIPAA-Covered Entities to notify Individual in the Case of Breach of Unsecured PHI	<b>09/23/2009</b>	§ 13402
Presumptive compliance with standards for minimum necessary requirement.	<b>02/17/2010</b> until Secretary issues guidance on standards for “minimum necessary” by Aug. 2010. Guidance will then govern.	§ 13405(b)(1)(A)
Accounting of Certain PHI Disclosures Required if Covered Entity Uses Electronic Health Record.	If the record exists on or before January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after <b>January 1, 2014</b> . If the record exists after January 1, 2009, the new accounting requirements will apply to disclosures made from that record on or after the later of <b>January 1, 2011</b> or the date the covered entity acquires the electronic health record.	§ 13405(c)(4)
Prohibition on Sale of Electronic Health Records or PHI	<b>At least 6 months after sub-§(d) regs promulgated</b> – regs by 08/17/2010	§ 13405(d)(1)
Temporary Breach Notification Requirement For Vendors of PHI and Other Non-HIPAA Covered Entities.	<b>05/29/2009</b> [See Sunset: §13407(g)(2)]	§ 13407
Civil penalties for willful neglect	<b>02/17/2011</b> (for penalties imposed on/after this date)	§ 13410(a)
Tiered Increase in Civil Monetary Penalties	<b>02/17/2009</b> (for violations occurring after this date)	§ 13410(d)
Enforcement of Provisions Through Civil Suit By State Attorneys General.	<b>02/17/2009</b> (for violations occurring after this date)	§ 13410(e)
Rules governing notification of breach of unsecured protected health information	<b>09/23/2009</b>	74 FR 42740
Rules on sanctions	<b>11/30/2009</b>	74 FR 56123
FTC - health breach notification rule for entities not covered by HIPAA	<b>09/18/2009</b> (for breaches of security discovered on/after this date)	74 FR 17914 – Implements 16 CFR Part 318

---

**BOARD OF DEVELOPMENTAL DISABILITIES  
NOTICE OF PRIVACY PRACTICES**

Effective: December 3, 2009

**This notice describes how personal information about you may be used and disclosed and how you can get access to this information. Please review it carefully.**

**Our Organization**

This notice describes the privacy practices of the \_\_\_\_\_ Board of Developmental Disabilities (the DD Board). This notice also describes the privacy practices of persons or entities which have signed a contract with the DD Board and which are acting as business associates, and have promised to follow the same rules of confidentiality.

The DD Board includes \_\_\_\_\_ *insert names of facilities operated by the DD Board*, as well as the DD Board employees and volunteers at those facilities.

If you want to know about the privacy practices of service providers who are not employed by the DD Board and who are not business associates, you should contact them directly.

**Privacy Promise**

The DD Board understands that your personal information needs to be kept private. Protecting your personal information is important. We follow strict federal and state laws that require us to keep your personal information confidential.

**How We Use Your Personal Information**

When you receive services from the DD Board, we may use your personal information for such activities as providing you with services, billing for services, and conducting our normal board business known as health care operations.

If you have chosen a personal representative and have agreed to let your personal representative obtain your personal information, we will provide the information to your personal representative. If you have a guardian we will provide the information to your guardian.

Examples of how we use your information include:

**Treatment** - We keep records of the care and services provided to you within the DD Board. For example, your service and support administrator keeps notes on all contacts made in coordinating and arranging for services. If you see a nurse working for the DD Board, the nurse will keep records of any care you receive. DD Board staff may share your personal information while helping to develop your service plan.

If DD Board staff want to share your personal information with anyone who is not employed by the DD Board, you must give them written permission first. However, we may disclose your identity without your permission if necessary for your treatment or to obtain payment for services.

Some personal records, including confidential communications with a mental health professional and substance abuse records, may have additional restrictions for use and disclosure under state and federal law.

**Payment** – We keep records that include payment information and documentation of the services provided to you. Your information may be used to obtain payment for your services from Medicaid, insurance or other sources. For example, we may disclose personal information about the services provided to you to confirm your eligibility for Medicaid and to obtain payment from Medicaid. The DD Board may use your personal information to determine the amount and type of Medicaid services you need and send this information to the proper state department

**Health Care Operations** – We use personal information to improve the quality of care, train staff, manage costs, conduct required business duties, and make plans to better serve you and other individuals enrolled in the DD Board. For example, we may use your personal information to evaluate the quality of treatment and services provided by our service staff.

### **Other Services We Provide**

We may also use your personal information to:

- Determine whether you are eligible for services from the DD Board;
- Recommend to you service alternatives and other possible benefits;
- Tell you about other service providers who may be able to help you;
- Remind you of an appointment unless you tell the DD Board staff that you do not wish to be reminded;
- To allow the DD Board to review direct service contracts;
- To determine whether the waiting lists are being kept in accordance with Ohio law;

- Allow local, state, federal agencies to monitor your services;
- To investigate incidents affecting health and safety, to report these kind of incidents and to take steps to protect your health and safety;
- To allow the DD Board to prepare reports required by the Ohio Department of Mental Retardation and Developmental Disabilities and the Ohio Department of Job and Family Services;
- Contact you for assistance in passing levies, unless you notify the DD Board that you do not wish to be contacted for these purposes.

### **More Information**

For more information about the practices and rights described in this notice:

- Visit our website at \_\_\_\_\_
- Contact the DD Board at the phone number and address on the back of this notice

### **Sharing Your Personal Information**

There are limited situations when we are permitted or required to disclose personal information without your signed authorization. These situations are:

- We may disclose your identity, if necessary, for your treatment or to obtain payment for services.
- To protect victims of abuse, neglect, or domestic violence;
- To reduce or prevent a serious threat to public health and safety;
- For health oversight activities such as investigations, audits, and inspections;
- For lawsuits and similar proceedings;
- For public health purposes such as reporting communicable diseases, work-related illnesses, or other diseases and injuries permitted by law; reporting births and deaths, and reporting reactions to drugs and problems with medical devices;
- When required by law;
- When requested by law enforcement as required by law or court order;

- To coroners, medical examiners, and funeral directors;
- For organ and tissue donation;
- For workers' compensation or other similar programs if you are injured at work and are covered by workers' compensation or other similar programs;
- For specialized government functions such as intelligence and national security;

All other uses and disclosures, not described in this notice, require your signed authorization. You may revoke your authorization at any time with a written statement.

### **Our Privacy Responsibilities**

The DD Board is required by law to:

- Maintain the privacy of your personal information
- Provide this notice that describes the ways we may use and share your personal information
- Follow the terms of the notice currently in effect.

**We reserve the right to make changes to this notice at any time and make the new privacy practices effective for all information we maintain.**

Current notices will be posted in the DD Board facilities and on our website, \_\_\_\_\_.

You may also request a copy of any notice from the the DD Board Privacy Office.

### **Your Individual Rights**

You have the right to:

- Request restrictions on how we use and share your personal information. We will consider all request for restrictions carefully but are not required to agree to any restriction.\*
- Request that we use a specific telephone number or address to communicate with you.
- Inspect and copy your personal information, including service, medical and billing records. Fees may apply.\*
- Request corrections or additions to your personal information. You must give the reasons for wanting the change.\*

- Request an accounting of certain disclosures of your personal information made by us or by Business Associates who are working for us. Your request must state the period of time desired for the accounting. You may ask for an accounting of disclosures made at least three years prior to your request, and in some cases disclosures made for six years prior to your request. The first accounting is free but a fee will apply if more than one request is made in a 12-month period.\*
- Request a paper copy of this notice even if you agree to receive it electronically.

Requests marked with a star (\*) must be made in writing. Contact the DD Board Privacy Office for the appropriate form for your request.

### Contact Us

If you would like further information about your privacy rights, are concerned that your privacy rights have been violated, or disagree with a decision that we made about access to your personal information:

Contact the DD Board

*[insert name or title of person assigned to provide information]*  
*[insert address]*  
*[insert telephone number]*

or E-mail:

We will investigate all complaints and will not retaliate against you for filing a complaint.

You also may file a written complaint with any of the following:

- the Secretary of the U.S. Department of Health and Human Services at 200 Independence Avenue SW, Washington D.C., 20201 or call 1-877-696-6775; or
- The Office for Civil Rights, U.S. Department of Health and Human Services at 200 Independence Avenue SW, Room 509F, HHH Building, Washington D.C., 20201 or call OCR's hotline – voice at 1-800-368-1019, or e-mail at [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov).
- Attorney General for State of Ohio 30 E. Broad St., 17th Floor  
Columbus, OH 43215 or by e-mail at [ohioattorneygeneral.gov/Contact](http://ohioattorneygeneral.gov/Contact)

### BUSINESS ASSOCIATE AGREEMENT

This Agreement is entered into this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_, by and between \_\_\_\_\_ (referred to hereinafter as "Business Associate") and \_\_\_\_\_ (referred to hereinafter as "DD Board"). The parties are entering into this agreement in consideration of the mutual promises contained herein and for other good and valuable consideration.

This Agreement shall be in effect *[define term/duration of the Agreement]*.

WHEREAS, the DD Board will make available and/or transfer to the Business Associate confidential, personally identifiable health information in conjunction with *[describe function to be performed by the Business Associate on behalf of the DD Board]*; and

WHEREAS, such information may be used or disclosed only in accordance with the privacy regulations [45 CFR §§ 164.502(e); 164.504(e)] issued pursuant to the Health Insurance Portability and Accountability Act [42 USC §§ 1320 - 1320d-8], the American Recovery and Reinvestment Act of 2009 and the terms of this Agreement, or more stringent provisions of the law of the State of Ohio;

1. Definitions

- a. *Applicable Law* means Federal and Ohio law which applies to transactions and entities covered by this Agreement.
- b. *Applicable Requirements* means all of the following:
  - i. applicable law
  - ii. policies and procedures of the DD Board which are consistent with applicable law and which apply to information covered by this Agreement and
  - iii. the requirements of this Agreement.
- c. *ARRA* means the American Recovery and Reinvestment Act of 2009.
- d. *HIPAA* means the Health Care Portability and Accountability Act of 1996, 42 USC §§ 1320 - 1320d-8 and regulations promulgated thereunder as may be amended.
- e. *Individual* includes the individual receiving services from the DD Board and the Personal Representative selected by the individual or other person legally authorized to act on behalf of the individual.
- f. *Protected Health Information* ("PHI") is information received from or on behalf of the Covered Entity that meets the definition of PHI as defined by HIPAA and the

regulations promulgated by the United States Department of Health and Human Services, specifically 45 CFR 164.501, and any amendments thereto.

- g. *Underlying Service Contract* [if there is an existing Service Contract which does not include Business Associate Agreement elements] means the contract entered into between the DD Board and the Business Associate [describe existing Service Contract, if any].
2. The DD Board shall provide to the Business Associate a copy of the current Notice of Privacy Practices and any relevant information on changes to or agreed upon restrictions relating to legal permissions for the use or disclosure of PHI.
  3. ***[insert if there is an existing Service Contract]*** This Business Associate Agreement states terms and conditions which are in addition to those in the Underlying Service Contract. Nothing in this Agreement shall be interpreted to change the terms of the Underlying Service Contract except to the extent that such a change is specifically required under the terms of this Agreement.
  4. The Business Associate agrees that it shall not receive, create, use or disclose PHI except in accordance with applicable requirements, including, without limitation, all HIPAA privacy rules applicable to covered entities and business associates, and as follows:
    - a. ***[describe covered function carried out by the Business Associate being performed or refer to an Exhibit, attached to and made a part of the Agreement];***
    - b. If necessary for the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate. PHI may only be disclosed to another person/entity for such purposes if:
      - Disclosure is required by law; or
      - Where the Business Associate obtains reasonable assurances from the person to whom disclosure is made that the PHI released will be held confidentially, and only may be used or further disclosed as required by law or for the purposes of the disclosure; and
      - the person/entity agrees to notify the Business Associate of any breaches of confidentiality;
    - c. To permit the Business Associate to provide data aggregation services relating to the health care operations of the DD Board.

5. The Business Associate and the DD Board agree that neither of them will request, use or release more than the minimum amount of PHI necessary to accomplish the purpose of the use, disclosure or request.
6. The Business Associate shall establish and maintain appropriate safeguards to prevent any unauthorized use or disclosure of PHI and shall conform to the requirements set for in applicable law for security of PHI including, without limitation, the requirements of 45 CFR §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies, procedures and documentation). ***[may want to add more specifics, either here or by Exhibit, attached to and made part of the Agreement, spelling out the safeguards that will be in place, i.e. personnel policies/practices and physical and electronic measures to safeguard data.]***
7. The Business Associate shall report to the DD Board any unauthorized uses/disclosures of which it becomes aware, and shall take all reasonable steps to mitigate the potentially harmful effects of such unauthorized uses/disclosures. Such report shall be made immediately but not later than 30 days after discovery of the unauthorized uses/disclosures. The report of the unauthorized uses/disclosures, shall include the following information:
  - (a) A brief description of what happened, including the date of the unauthorized uses/disclosures and the date of the discovery of the unauthorized uses/disclosures, if known;
  - (b) A description of the types of unsecured PHI involved in the unauthorized uses/disclosures (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
  - (c) Any steps individuals should take to protect themselves from potential harm resulting from the unauthorized uses/disclosures;
  - (d) A brief description of what the Business Associate is doing to investigate the unauthorized uses/disclosures, to mitigate harm to individuals, and to protect against any further unauthorized uses/disclosures.
8. The Business Associate shall ensure that all of its subcontractors and agents are bound by the same restrictions and obligations contained herein whenever PHI is made accessible to such subcontractors or agents, and shall give prior notice to the DD Board of any subcontractors or agents who are to be given access to PHI.
9. The Business Associate shall make all PHI and related information in its possession available as follows:

- a. To the individual or to the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to allow access for inspection and copying in accordance with the provisions of 45 CFR § 164.524;
  - b. To the individual or to the DD Board, to the extent necessary to permit the DD Board to fulfill any obligation of the DD Board to account for disclosures of PHI in accordance with 45 CFR § 164.528.
10. The Business Associate shall make PHI available to the DD Board to fulfill the DD Board's obligation to amend PHI and related information in accordance with 45 CFR § 164.526, and shall, as directed by the DD Board, incorporate any approved amendments to PHI or related statements into the information held by the Business Associate and any subcontractors or agents.
11. The Business Associate shall make its internal practices, books and records relating to the use or disclosure of information received from or on behalf of the DD Board available to the U. S. Secretary of Health and Human Services, or the Secretary's designee, for purposes of determining the DD Board's compliance with the privacy regulations, and any amendments thereto.
12. Upon request by an individual, the Business Associate shall account for all disclosures related to such individual made by the BA pursuant to the HIPAA Privacy Rules, including, without limitation, accountings required under 45 CFR 164.528. *[Alternative: the Business Associate shall, upon request of the DD Board, provide such information as may be necessary to permit the DD Board to provide accountings in accordance with applicable requirements.]*
13. Upon termination of this Agreement, the Business Associate shall, at the option of the DD Board, return or destroy all PHI created or received from or on behalf of the DD Board. The Business Associate shall not retain any copies of PHI except as required by law. If PHI is destroyed, the Business Associate shall provide the DD Board with appropriate documentation/certification evidencing such destruction. If return or destruction of all PHI, and all copies of PHI, is not feasible, the Business Associate shall extend the protections set forth in applicable requirements to such information for as long as it is maintained. Termination of this Agreement shall not affect any of its provisions that, by wording or nature, are intended to remain effective and to continue in operation.
14. The PHI and any related information created or received from or on behalf of the DD Board is and shall remain the property of the DD Board. The Business Associate agrees that it acquires no title in or rights to the information, including any de-identified information.
15. Any non-compliance by the Business Associate or DD Board with the terms of this Agreement or the privacy or security regulations shall be a breach of this Agreement. If





1 of 15 DOCUMENTS

FEDERAL REGISTER

Vol. 74, No. 079

Rules and Regulations

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS)

Office of the Secretary of Health and Human Services

**45 CFR Parts 160 and 164**

**Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information**

*74 FR 19006*

**DATE:** Monday, April 27, 2009

**ACTION:** Guidance and Request for Information.

**SUMMARY:** This document is guidance and a request for comments under section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). ARRA was enacted on February 17, 2009. The HITECH Act (the Act) at section 13402 requires the Department of Health and Human Services (HHS) to issue interim final regulations within 180 days of enactment to require covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates to provide for notification in the case of breaches of unsecured protected health information. For purposes of these requirements, section 13402(h) of the Act defines "unsecured protected health information" to mean protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance, and requires the Secretary to issue such guidance no later than 60 days after enactment and to specify within the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Through this document, HHS is issuing the required guidance and seeking public comment both on the guidance as well as the breach notification provisions of the Act generally to inform the future rulemaking and updates to the guidance.

**DATES:** Comments must be submitted on or before May 21, 2009. The guidance is applicable upon issuance, which occurred on April 17, 2009, through posting on the HHS Web site at <http://www.hhs.gov/ocr/privacy>. However, the guidance will apply to breaches 30 days after publication of the forthcoming interim final regulations. If we

determine that the guidance should be modified based on public comments, we will issue updated guidance prior to or concurrently with the regulations.

**ADDRESSES:** Written comments may be submitted through any of the methods specified below. Please do not submit duplicate comments.

. *Federal eRulemaking Portal:* You may submit electronic comments at <http://www.regulations.gov>. Follow the instructions for submitting electronic comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.

. *Regular, Express, or Overnight Mail:* You may mail written comments (one original and two copies) to the following address only: U.S. Department of Health and Human Services, Office for Civil Rights, *Attention:* HITECH Breach Notification, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201.

. *Hand Delivery or Courier:* If you prefer, you may deliver (by hand or courier) your written comments (one original and two copies) to the following address only: Office for Civil Rights, Attention: HITECH Breach Notification, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, SW., Washington, DC 20201. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

. *Inspection of Public Comments:* All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. We will post all comments received before the close of the comment period at <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** Andra Wicks, 202-205-2292.

#### **SUPPLEMENTARY INFORMATION:**

##### **I. Background**

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009, as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111-5). Subtitle D of [\*19007] the HITECH Act (the Act), entitled "Privacy," among other provisions, requires HHS to issue interim final regulations for breach notification by entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates. In particular, section 13402 of the Act requires HIPAA covered entities to notify affected individuals, and requires business associates to notify covered entities, following the discovery of a breach of unsecured protected health information (PHI). n1

n1 Protected health information (PHI) is individually identifiable health information transmitted or maintained by a covered entity or its business associate in any form or medium. 45 CFR 160.103.

The Act at section 13402(h) defines "unsecured protected health information" to mean PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance. Further, the Act provides that no later than 60 days after enactment, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. n2 The Act also provides that in the case the Secretary does not issue timely guidance, the term "unsecured protected health information" shall mean "protected health information that is not

secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI)." n3

n2 The Act provides that the technologies and methodologies specified in the guidance also are to address the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of the Act. Section 3002(b)(2)(B)(vi) of the Public Health Service Act requires the HIT Policy Committee established in section 3002 to issue recommendations on the development of technologies that allow individually identifiable health information to be rendered unusable, unreadable, or indecipherable to unauthorized individuals when such information is transmitted in the nationwide health information network or physically transported outside of the secured physical perimeter of a health care provider, health plan, or health care clearinghouse. The Department intends to address such standards as they are developed in future iterations of this guidance.

n3 This provision becomes moot with the issuance of this guidance.

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods identified in this guidance, then such information is not "unsecured" PHI. Thus, because the breach notification requirements apply only to breaches of unsecured PHI, this guidance provides the means by which covered entities and their business associates are to determine whether a breach has occurred to which the notification obligations under the Act and its implementing regulations apply. Further, section 13407 of the Act defines "unsecured PHR identifiable information" as personal health record (PHR) identifiable health information that is not protected through the use of a technology or methodology specified in the Secretary's guidance. Thus, this guidance also is to be used to specify the technologies and methodologies that render PHR identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the temporary breach notification requirements that apply to vendors of PHRs and certain other entities (that are not otherwise HIPAA covered entities) under section 13407 of the Act. Section 13407 is to be administered by the Federal Trade Commission (FTC) and requires the FTC to promulgate regulations within 180 days of enactment.

The breach notification provisions of section 13402 apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI (sections 13402(a) and (b)). For purposes of these provisions, "breach" is defined in the Act as "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." The Act includes exceptions to this definition for cases in which: (1) The unauthorized acquisition, access, or use of PHI is unintentional and made by an employee or individual acting under authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship with the covered entity or business associate, and such information is not further acquired, accessed, used, or disclosed; or (2) where an inadvertent disclosure occurs by an individual who is authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, as long as the PHI is not further acquired, accessed, used, or disclosed without authorization (section 13400, definition of "breach").

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach (section 13402(a)). Additionally, following the discovery of a breach by a business associate, the business associate must notify the covered entity of the breach and identify for the covered entity the individuals whose unsecured PHI has been, or is reasonably believed to have been, breached (section 13402(b)). The Act requires the notifications to be made without unreasonable delay but in no case later than 60 calendar days after discovery of the breach, except that section 13402(g) requires a delay of notification where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security.

The Act specifies the following methods of notice in section 13402(e):

. Written notice to the individual (or next of kin if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if specified by the individual).

. In the case in which there is insufficient or out-of-date contact information, substitute notice, including, in the case of 10 or more individuals for which there is insufficient contact information, conspicuous posting (for a period determined by the Secretary) on the home page of the Web site of the covered entity or notice in major print or broadcast media.

. In cases that the entity deems urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.

. Notice to prominent media outlets within the State or jurisdiction if a breach of unsecured PHI affects or is reasonably believed to affect more than 500 residents of that State or jurisdiction.

. Notice to the Secretary by covered entities immediately for breaches involving more than 500 individuals and annually for all other breaches.

. Posting by the Secretary on an HHS Web site of a list that identifies each covered entity involved in a breach in which the unsecured PHI of more than 500 individuals is acquired or disclosed. [\*19008]

Section 13402(f) of the Act requires the notification of a breach to include (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code); (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address. Finally, section 13402(i) requires the Secretary to annually prepare and submit to Congress a report regarding the breaches for which the Secretary was notified.

The Department's interim final regulations will become effective 30 days after publication and will apply to breaches of unsecured PHI thereafter.

## **II. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals**

Please note that this guidance does not address the use of de-identified information as a method to render protected health information (PHI) unusable, unreadable, or indecipherable to unauthorized individuals because once PHI has been de-identified in accordance with the HIPAA Privacy Rule, n4 it is no longer PHI and, therefore, no longer subject to the HIPAA Privacy and Security Rules. n5 However, nothing in this guidance should be construed as discouraging covered entities and business associates from using de-identified information to the maximum extent practicable.

n4 De-identified health information neither identifies nor provides a reasonable basis to identify an individual. The HIPAA Privacy Rule provides two ways to de-identify information: (1) A formal determination by a qualified statistician; or (2) the removal of 18 specified identifiers of the individual and of the individual's relatives, household members, and employers, and the covered entity has no actual knowledge that the remaining information could be used to identify the individual. 45 CFR 164.514(b).

n5 45 CFR Parts 160 and Subparts A, C, and E of Part 164.

*A. Background*

This guidance identifies the technologies and methodologies that can be used to render PHI (as defined in 45 CFR 160.103) unusable, unreadable, or indecipherable to unauthorized individuals. It should be used by covered entities and their business associates to determine whether "unsecured protected health information" has been breached, thereby triggering the notification requirements specified in section 13402 of the Act and its forthcoming implementing regulations.

This guidance is not intended to instruct covered entities and business associates on how to prevent breaches of PHI. The HIPAA Privacy and Security Rules, which are much broader in scope and different in purpose than this guidance, are intended, in part, to prevent or reduce the likelihood of breaches of PHI. Covered entities must comply with the requirements of the HIPAA Privacy and Security Rules by conducting risk analyses and implementing physical, administrative, and technical safeguards that each covered entity determines are reasonable and appropriate. Covered entities and business associates seeking additional information also may want to refer to the National Institute of Standards and Technology (NIST) Special Publication 800-66-Revision 1, "An Introductory Resource Guide for Implementing the HIPAA Security Rule." n6

n6 Available at <http://www.csrc.nist.gov/>.

This guidance is intended to describe the technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals. While covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor, and thus, result in covered entities and business associates not being required to provide the notification otherwise required by section 13402 in the event of a breach. However, while adherence to this guidance may result in covered entities and business associates not being required to provide the notifications in the event of a breach, covered entities and business associates still must comply with all other federal and state statutory and regulatory obligations that may apply following a breach of PHI, such as state breach notification requirements, if applicable, as well as the obligation on covered entities at 45 CFR 164.530(f) of the HIPAA Privacy Rule to mitigate, to the extent practicable, any harmful effect that is known to the covered entity as a result of a breach of PHI by the covered entity or business associate.

In accordance with the requirements of this Act, we are issuing this guidance after consultation with stakeholders. Specifically, we consulted with external experts in health informatics and security, including representatives from several Federal agencies. In issuing this guidance, HHS is soliciting additional public input on the guidance, including whether there are other specific types of technologies and methodologies that should be included in future updates to the guidance if appropriate. This guidance may be modified based on public feedback and updated guidance may be issued prior to or concurrently with the interim final regulations.

The term "unsecured protected health information" includes PHI in any form that is not secured through the use of a technology or methodology specified in this guidance. This guidance, however, addresses methods for rendering PHI in paper or electronic form unusable, unreadable, or indecipherable to unauthorized individuals.

Data comprising PHI can be vulnerable to a breach in any of the commonly recognized data states: "data in motion" (*i.e.*, data that is moving through a network, including wireless transmission n7); "data at rest" (*i.e.*, data that resides in databases, file systems, and other structured storage methods n8); "data in use" (*i.e.*, data in the process of being created, retrieved, updated, or deleted n9); or "data disposed" (*e.g.*, discarded paper records or recycled electronic media). PHI in each of these data states (with the possible exception of "data in use" n10) may be secured using one or more methods. In consultation with information security experts at NIST, we have identified two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction. Both of these methods are discussed below.

74 FR 19006, \*19008

n7 Preventing Data Leakage Safeguards Technical Assistance, Internal Revenue Service, <http://www.irs.gov/businesses/small/article/0,,id=201295,00.html>.

n8 Kanagasingham, P. *Data Loss Prevention*, SANS Institute, 2008.

n9 Sometimes referred to as "data at the endpoints."

n10 We solicit comments on methods to protect data in use. See Section III.A.1.

Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two [\*19009] main features: The strength of the encryption algorithm and the security of the decryption key or process. The specification of encryption methods in this guidance includes the condition that the processes or keys that might enable decryption have not been breached.

This guidance also addresses the destruction of PHI both in paper and electronic form as a method for rendering such information unusable, unreadable, or indecipherable to unauthorized individuals. If PHI is destroyed prior to disposal in accordance with this guidance, no breach notification is required following access to the disposed hard copy or electronic media by unauthorized persons.

Note that the technologies and methodologies referenced below in Section B are intended to be exhaustive and not merely illustrative.

#### Solicitation of Public Comment on Additional Technologies and Methodologies

Because we intend this guidance to be an exhaustive list of the technologies and methodologies that can be used to render PHI unusable, unreadable, or indecipherable to unauthorized individuals, we are soliciting public comment on whether there are additional technologies and methodologies the Department should consider adding to this exclusive list in future iterations of this guidance. n11

n11 See Section III.A.3.

In particular, in the development of this guidance, the Department considered whether PHI in limited data set form should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification, and thus, included in this guidance. A limited data set is PHI from which the 16 direct identifiers listed at 45 CFR 164.514(e)(2) of the HIPAA Privacy Rule, including an individual's name, address, Social Security number, and account number, have been removed. Although a limited data set requires the removal of direct identifiers, the information is not completely de-identified pursuant to 45 CFR 164.514(b) of the HIPAA Privacy Rule. Due to the risk of re-identification of a limited data set, the HIPAA Privacy Rule treats information in a limited data set as PHI, which must be protected and only used or disclosed as permitted by the HIPAA Privacy Rule. However, although the HIPAA Privacy Rule treats information in a limited data set as PHI, the Rule does make distinctions in terms of its requirements between PHI in a limited data set and PHI that contains direct identifiers. First, the HIPAA Privacy Rule permits covered entities to use or disclose PHI in a limited data set in certain circumstances where fully-identifiable PHI is not permitted, such as for research purposes where no individual authorization or an Institutional Review Board waiver of authorization is obtained. See 45 CFR 164.502(a)(1)(vi) and 164.514(e). In these situations, to attempt to control the risk of re-identification of PHI in a limited data set, the HIPAA Privacy Rule requires a data use agreement to be in place between the covered entity and the recipient of the limited data set obligating the recipient to not re-identify the information or contact the individuals (45 CFR 164.514(e)(4)). Second, the HIPAA Privacy Rule further distinguishes between PHI in a limited data set and fully-identifiable PHI by excluding disclosures of PHI in limited data set form from the accounting of disclosures requirement at 45 CFR 164.528(a)(1)(viii).

In determining whether PHI in limited data set form should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification, we considered the following in support of including the

creation of a limited data set in this guidance: (1) Doing so would better align this guidance and the forthcoming federal regulations with state breach notification laws, which, as a general matter, only address the compromise of direct identifiers; and (2) there may be administrative and legal difficulties covered entities face in notifying individuals of a breach of a limited data set in light of limited contact information and requirements in data use agreements.

On the other hand, because PHI in limited data set form is not completely de-identified, the risk of re-identification is a consideration in determining whether it should be treated as unusable, unreadable, or indecipherable to unauthorized individuals for purposes of breach notification, and thus, included in this guidance as an acceptable methodology. Therefore, the Department is interested in receiving public comments on whether the risk of re-identification of a limited data set warrants its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

For those that believe the risk of re-identification of a limited data set warrants exclusion, we also request comment on whether concerns would be alleviated if we required, for purposes of inclusion in the guidance, the removal of certain of the remaining indirect identifiers in the limited data set. For example, some research suggests that a significant percentage of the U.S. population can be identified with just three key pieces of information, along with other publicly available data: gender, birth date (month/day/year), and 5-digit zip code. n12 Would the removal of one further piece of information from the limited data set--either the month and day of birth (but not the year of birth) or the last 3 digits of a 5-digit zip code (in addition to the elements listed in the HIPAA Privacy Rule at 45 CFR 164.514(e)(2) for creation of limited data sets)--sufficiently reduce the risk of re-identification such that this modified data set could be added to this guidance? n13 Research suggests that doing so could significantly reduce the risk of re-identification. n14

n12 Golle P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. Available at <http://crypto.stanford.edu/pgolle/papers/census.pdf>.

n13 See Section III.A.5.

n14 Golle P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. Available at <http://crypto.stanford.edu/pgolle/papers/census.pdf>.

*B. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

(a) Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" n15 and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard. n16

n15 45 CFR 164.304, definition of "encryption."

n16 The NIST Computer Security Division's mission is to provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems. The NIST standards are the standards the Federal government uses to protect its information systems.

(i) Valid encryption processes for data at rest are consistent with NIST Special [\*19010] Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*. n17

n17 Available at <http://www.csrc.nist.gov/>.

(ii) Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, and may include others which are FIPS 140-2 validated. n18

n18 Available at <http://www.csrc.nist.gov/>.

(b) The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, n19 such that the PHI cannot be retrieved.

n19 Available at <http://www.csrc.nist.gov/>.

### **III. Solicitation of Comments**

#### *A. Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*

The Department is seeking comments on its guidance regarding the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals for purposes of section 13402(h)(2) of the Act. In particular, the Department is interested in receiving comments on the following:

1. Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected Universal Serial Bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?

2. With respect to paper PHI, are there additional methods the Department should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?

3. Are there other methods generally the Department should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?

4. Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?

5. Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals? Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?

6. In the event of a breach of protected health information in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?

7. Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

#### *B. Breach Notification Provisions Generally*

In addition to public comment on the guidance, the Department also requests comments concerning any other areas or issues pertinent to the development of its interim final regulations for breach notification. In particular, the Department is interested in comment in the following areas:

1. Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues the Department should consider in promulgating the federal breach notification requirements?

2. Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice would not also satisfy any notice obligations under the state law?

3. Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate would still be required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?

4. The Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

Dated: April 22, 2009.

**Charles E. Johnson,**

*Acting Secretary.*

[FR Doc. E9-9512 Filed 4-22-09; 4:15 pm]

BILLING CODE 4150-03-P