

DEPARTMENT 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

AGENCY: Office of the Secretary, Department of Health and Human Services

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 effective 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, S.W., Washington, D.C. 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, S.W., Washington, D.C. 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 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).¹

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.² The Act also

¹ 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.

² 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

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).”³

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

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.

³ This provision becomes moot with the issuance of this guidance.

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.

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,⁴ it is no longer PHI and, therefore, no longer subject to the HIPAA Privacy and Security Rules.⁵ 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.

A. Background

⁴ 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).

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

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-Revision1 “An Introductory Resource Guide for Implementing the HIPAA Security Rule.”⁶

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

⁶ Available at <http://www.csrc.nist.gov/>.

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 transmission⁷); “data at rest” (i.e., data that resides in databases, file systems, and other structured storage methods⁸); “data in use” (i.e., data in the process of being created, retrieved, updated, or deleted⁹); 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”¹⁰) 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.

Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two 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

⁷ Preventing Data Leakage Safeguards Technical Assistance, Internal Revenue Service, <http://www.irs.gov/businesses/small/article/0,,id=201295,00.html>.

⁸ Kanagasingham, P. *Data Loss Prevention*, SANS Institute, 2008.

⁹ Sometimes referred to as “data at the endpoints.”

¹⁰ We solicit comments on methods to protect data in use. See Section III.A.1.

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.¹¹

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-

¹¹ See Section III.A.3.

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 US 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.¹² 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

¹² Golle P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. Available at <http://crypto.stanford.edu/~pgolle/papers/census.pdf>.

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?¹³ Research suggests that doing so could significantly reduce the risk of re-identification.¹⁴

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”¹⁵ 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.¹⁶

¹³ See Section III.A.5.

¹⁴ Golle P. (2006). Revisiting the Uniqueness of Simple Demographics in the US Population. Available at <http://crypto.stanford.edu/~pgolle/papers/census.pdf>.

¹⁵ 45 CFR 164.304, definition of “encryption.”

¹⁶ 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

- i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.¹⁷
 - 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.¹⁸
- 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*,¹⁹ such that the PHI cannot be retrieved.

III. Solicitation of Comments

Technology (IT) systems. The NIST standards are the standards the Federal government uses to protect its information systems.

¹⁷ Available at <http://www.csrc.nist.gov/>.

¹⁸ Available at <http://www.csrc.nist.gov/>.

¹⁹ Available at <http://www.csrc.nist.gov/>.

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?

Charles E. Johnson,
Acting Secretary.