[BILLING CODE: 4153-01]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN: 0991-AB56

Breach Notification for Unsecured Protected Health Information

AGENCY: Office for Civil Rights, Department of Health and Human Services

ACTION: Interim final rule with request for comments.

SUMMARY: The Department of Health and Human Services (HHS) is issuing this interim final rule with a request for comments to require notification of breaches of unsecured protected health information. Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was enacted on February 17, 2009, requires HHS to issue interim final regulations within 180 days to require covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their business associates to provide notification in the case of breaches of unsecured protected health information. For purposes of determining what information is "unsecured protected health information," in this document HHS is also issuing an update to its guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

DATES: Effective Date: This interim final rule is effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Comment Date: Comments on the provisions of this interim final rule are due on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. Comments on the information collection requirements associated with this rule are due on or before [INSERT DATE 14 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by RIN 0991-AB56, by any of the following methods (please do not submit duplicate comments):

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments. Attachments should be in Microsoft Word, WordPerfect, or Excel; however, we prefer Microsoft Word.
- Regular, Express, or Overnight Mail: 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. Please submit one original and two copies.
- Hand Delivery or Courier: Office for Civil Rights, Attention: HITECH Breach Notification, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue, S.W., Washington, D.C. 20201. Please submit one original and two copies. (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. Because comments will be made public, they should not include any sensitive personal information, such as a person's social security number; date of birth; driver's license number, state identification number or foreign country equivalent; passport number; financial account number; or credit or debit card number. Comments also should not include any sensitive health information, such as medical records or other individually identifiable health information.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov or U.S. Department of Health and Human Services, Office for Civil Rights, 200 Independence Avenue, S.W., Washington, D.C. 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FUTHER INFORMATION CONTACT: Andra Wicks, 202-205-2292

SUPPLEMENTARY INFORMATION:

I. Background

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), was enacted on February 17, 2009. Subtitle D of Division A of the HITECH Act (the Act), entitled "Privacy," among other provisions, requires the Department of Health and Human Services (HHS or the Department) to issue interim final regulations for breach notification by covered entities subject to the Administrative Simplification provisions of the Health Insurance

Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191) and their business associates.

These breach notification provisions are found in § 13402 of the Act and apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. The Act incorporates the definitions of "covered entity," "business associate," and "protected health information" used in the HIPAA Administrative Simplification regulations (45 CFR parts 160, 162, and 164) (HIPAA Rules) at § 160.103. Under the HIPAA Rules, a covered entity is a health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan. Business associate, as defined in the HIPAA Rules, means a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of individually identifiable health information. Examples of business associates include third party administrators or pharmacy benefit managers for health plans, claims processing or billing companies, transcription companies, and persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. The HIPAA Rules define "protected health information" as the individually identifiable health information held or transmitted in any form or medium by these HIPAA covered entities and business associates, subject to certain limited exceptions.

The Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured

protected health information. In addition, in some cases, the Act requires covered entities to provide notification to the media of breaches. In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach. Finally, the Act requires the Secretary to post on an HHS web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Section 13400(1) of the Act defines "breach" to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. The Act provides exceptions to this definition to encompass disclosures where the recipient of the information would not reasonably have been able to retain the information, certain unintentional acquisition, access, or use of information by employees or persons acting under the authority of a covered entity or business associate, as well as certain inadvertent disclosures among persons similarly authorized to access protected health information at a business associate or covered entity.

Further, § 13402(h) of the Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance" and provides that the guidance specify the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in

the event of a breach of such information – that is, the information is not considered "unsecured" in such cases. As required by the Act, the Secretary initially issued this guidance on April 17, 2009 (it was subsequently published in the Federal Register at 74 FR 19006 on April 27, 2009). The guidance listed and described encryption and destruction as the two technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

In cases in which notification is required, the Act at § 13402 prescribes the timeliness, content, and methods of providing the breach notifications. We discuss these and the above statutory provisions in more detail below where we describe section-by-section how these new regulations implement the breach notification provisions at § 13402 of the Act.

In addition to the breach notification provisions for HIPAA covered entities and business associates at § 13402, § 13407 of the Act, which is to be implemented and enforced by the Federal Trade Commission (FTC), imposes similar breach notification requirements upon vendors of personal health records (PHRs) and their third party service providers following the discovery of a breach of security of unsecured PHR identifiable health information.[1] As with the definition of "unsecured protected health information," the provisions at § 13407(f)(3) define "unsecured PHR identifiable health information" as PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary of HHS in guidance. Thus, entities subject to the FTC breach notification rules must also use the Secretary's

[1] The FTC issued a notice of proposed rulemaking to implement § 13407 of the Act on April 20, 2009 (74 FR 17914).

guidance to determine whether the information subject to a breach was "unsecured" and, therefore, whether breach notification is required.

When HHS issued the guidance, HHS also published in the same document a request for information (RFI), inviting public comment both on the guidance itself, as well as on the breach provisions of § 13402 of the Act generally. After considering the public comment, we are issuing an updated version of the guidance in Section II below. In addition, we discuss public comment received on the Act's breach notification provisions where relevant below in the section-by-section description of the interim final rule.

We have concluded that we have good cause, under 5 U.S.C. 553(b)(B), to waive the notice-and-comment requirements of the Administrative Procedure Act and to proceed with this interim final rule. Section 13402(j) explicitly required us to issue these regulations as "interim final regulations" and to do so within 180 days. Based on this statutory directive and limited time frame, we concluded that notice-and-comment rulemaking was impracticable and contrary to public policy. Nevertheless, we sought comments in the RFI referenced above and considered those comments when drafting this rule. In addition, we provide the public with a 60-day period following publication of this document to submit comments on the interim final rule.

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

A. Background

As discussed above, § 13402 of the Act requires breach notification following the discovery of a breach of unsecured protected health information. Section 13402(h) of the Act defines "unsecured protected health information" as "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 specify in the guidance the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. As required by the Act, this guidance was issued on April 17, 2009, and later published in the Federal Register on April 27, 2009 (74 FR 19006). The guidance specified encryption and destruction as the technologies and methodologies for rendering protected health information, as well as PHR identifiable health information under § 13407 of the Act and the FTC's implementing regulation, unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. The RFI asked for general comment on this guidance as well as for specific comment on the technologies and methodologies to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Many commenters expressed concern and confusion regarding the purpose of the guidance and its impact on a covered entity's responsibilities under the HIPAA Security Rule (45 CFR part 164, subparts A and C). We emphasize that this guidance does nothing to modify a covered entity's responsibilities with respect to the Security Rule nor does it impose any new requirements upon covered entities to encrypt all protected health information. The Security Rule requires covered entities to safeguard electronic protected health information and permits covered entities to use any security measures

that allow them to reasonably and appropriately implement all safeguard requirements. Under 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii), a covered entity must consider implementing encryption as a method for safeguarding electronic protected health information; however, because these are addressable implementation specifications, a covered entity may be in compliance with the Security Rule even if it reasonably decides not to encrypt electronic protected health information and instead uses a comparable method to safeguard the information.

Therefore, if a covered entity chooses to encrypt protected health information to comply with the Security Rule, does so pursuant to this guidance, and subsequently discovers a breach of that encrypted information, the covered entity will not be required to provide breach notification because the information is not considered "unsecured protected health information" as it has been rendered unusable, unreadable, or indecipherable to unauthorized individuals. On the other hand, if a covered entity has decided to use a method other than encryption or an encryption algorithm that is not specified in this guidance to safeguard protected health information, then although that covered entity may be in compliance with the Security Rule, following a breach of this information, the covered entity would have to provide breach notification to affected individuals. For example, a covered entity that has a large database of protected health information may choose, based on their risk assessment under the Security Rule, to rely on firewalls and other access controls to make the information inaccessible, as opposed to encrypting the information. While the Security Rule permits the use of firewalls and access controls as reasonable and appropriate safeguards, a covered entity that seeks to

ensure breach notification is not required in the event of a breach of the information in the database would need to encrypt the information pursuant to the guidance.

We also received several comments asking for clarification and additional detail regarding the forms of information and the specific devices and protocols described in the guidance. As a result, we provide clarification regarding the forms of information addressed in the National Institute of Standards and Technology (NIST) publications referenced in the guidance. We clarify that "data in motion" includes data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange, while "data at rest" includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method. "Data in use" includes data in the process of being created, retrieved, updated, or deleted, and "data disposed" includes discarded paper records or recycled electronic media.

Additionally, many commenters suggested that access controls be included in the guidance as a method for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. We recognize that access controls, as well as other security methods such as firewalls, are important tools for safeguarding protected health information. While we believe access controls may render information inaccessible to unauthorized individuals, we do not believe that access controls meet the statutory standard of rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. If access controls are compromised, the underlying information may still be usable, readable, or decipherable to an unauthorized individual, and thus, constitute unsecured protected health information for which breach notification is required. Therefore, we have not included access controls in the guidance;

however, we do emphasize the benefit of strong access controls, which may function to prevent breaches of unsecured protected health information from occurring in the first place.

Other commenters suggested that the guidance include redaction of paper records as an alternative to destruction. Because redaction is not a standardized methodology with proven capabilities to destroy or render the underlying information unusable, unreadable or indecipherable, we do not believe that redaction is an accepted alternative method to secure paper-based protected health information. Therefore, we have clarified in this guidance that only destruction of paper protected health information, and not redaction, will satisfy the requirements to relieve a covered entity or business associate from breach notification. We note, however, that covered entities and business associates may continue to create limited data sets or de-identify protected health information through redaction if the removal of identifiers results in the information satisfying the criteria of 45 CFR 164.514(e)(2) or 164.514(b), respectively. Further, a loss or theft of information that has been redacted appropriately may not require notification under these rules either because the information is not protected health information (as in the case of de-identified information) or because the unredacted information does not compromise the security or privacy of the information and thus, does not constitute a breach as described in Section IV below.

In response to comments received, we also make two additional clarifications in the guidance. First, for purposes of the guidance below and ensuring encryption keys are not breached, we clarify that covered entities and business associates should keep encryption keys on a separate device from the data that they encrypt or decrypt. Second,

we also include in the guidance below a note regarding roadmap guidance activities on the part of the NIST pertaining to data storage on enterprise-level storage devices, such as RAID (redundant array of inexpensive disks), or SAN (storage-attached network) systems.

For ease of reference, we have published this updated guidance in this document below; however, it will also be available on the HHS web site at http://www.hhs.gov/ocr/privacy/. Any further comments regarding this guidance received in response to the interim final rule will be addressed in the first annual update to the guidance, to be issued in April 2010.

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 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"[2] and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified

[2] 45 CFR 164.304, definition of "encryption."

below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

(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.[3, 4]

(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with 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, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.[5]

(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. Redaction is specifically excluded as a means of data destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization,[6] such that the PHI cannot be retrieved.

III. Overview of Interim Final Rule

[3] NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available.
[4] Available at http://www.csrc.nist.gov/.
[5] Available at http://www.csrc.nist.gov/.
[6] Available at http://www.csrc.nist.gov/.

We are adding a new subpart D to part 164 of title 45 of the Code of Federal Regulations (CFR) to implement the breach notification provisions in § 13402 of the Act. These provisions apply to HIPAA covered entities and their business associates and set forth the requirements for notification to affected individuals, the media, and the Secretary of HHS following a breach of unsecured protected health information. In drafting this interim final regulation, we considered the public comments received in response to the RFI described above.

In addition, we consulted closely with the FTC in the development of these regulations. Commenters in response to both the RFI as well as the FTC's notice of proposed rulemaking urged HHS and the FTC to work together to ensure that the regulated entities know with which rule they must comply and that those entities that are subject to both rules because they may operate in different roles are not subject to two completely different and inconsistent regulatory schemes. In addition, commenters were concerned that individuals could receive multiple notices of the same breach if the HHS and the FTC regulations overlapped. Thus, HHS coordinated with the FTC to ensure these issues were addressed in the respective rulemakings. First, the rules make clear that entities operating as HIPAA covered entities and business associates are subject to HHS', and not the FTC's, breach notification rule. Second, in those limited cases where an entity may be subject to both HHS' and the FTC's rules, such as a vendor that offers PHRs to customers of a HIPAA covered entity as a business associate and also offers PHRs directly to the public, we worked with the FTC to ensure both sets of regulations were harmonized by including the same or similar requirements, within the constraints of

the statutory language. See Section IV.F. below for a more detailed discussion and an example of our harmonization efforts.

IV. Section-by-Section Description of Interim Final Rule

The following discussion describes the provisions of the interim final rule section by section. Those interested in commenting on the interim final rule can assist the Department by preceding discussion of any particular provision or topic with a citation to the section of the interim final rule being discussed.

A. Applicability—Section 164.400

Section 164.400 of the interim final rule provides that this breach notification rule is applicable to breaches occurring on or after 30 days from the date of publication of this interim final rule. See Section IV.K. Effective/Compliance Date of this rule for further discussion.

B. Definitions—Section 164.402

Section 164.402 of the interim final rule adopts definitions for the terms "breach" and "unsecured protected health information."

1. Breach.

Section 13402 of the Act and this interim final rule require covered entities and business associates to provide notification following a breach of unsecured protected health information. Section 13400(1)(A) of the Act defines "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information." Section 13400(1)(B) of the Act

provides several exceptions to the definition of "breach." Based on § 13400(1)(A), we have defined "breach" at § 164.402 of the interim final rule as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information." We have added paragraph (1) to the definition to clarify when the security or privacy of information is considered to be compromised. Paragraph (2) of the definition then includes the statutory exceptions, including the exception within § 13400(1)(A) that refers to whether the recipient would reasonably have been able to retain the information.

Protected Health Information

We note that the definition of "breach" is limited to protected health information. With respect to a covered entity or business associate of a covered entity, protected health information is individually identifiable health information that is transmitted or maintained in any form or medium, including electronic information. 45 CFR 160.103. If information is de-identified in accordance with 45 CFR 164.514(b), it is not protected health information, and thus, any inadvertent or unauthorized use or disclosure of such information will not be considered a breach for purposes of this subpart. Additionally, § 160.103 excludes certain types of individually identifiable health information from the definition of "protected health information," such as employment records held by a covered entity in its role as employer. If individually identifiable health information that is not protected health information is used or disclosed in an unauthorized manner, it would not qualify as a breach for purposes of this subpart – although the covered entity should consider whether it has notification requirements under other laws. Further, we

note that although the definition of "breach" applies to protected health information generally, covered entities and business associates are required to provide the breach notifications required by the Act and this interim final rule (discussed below) only upon a breach of unsecured protected health information. See also Section II of this document for a list of the technologies and methodologies that render protected health information secure such that notification is not required in the event of a breach.

Unauthorized Acquisition, Access, Use, or Disclosure

The statute defines a "breach" as the "unauthorized" acquisition, access, use, or disclosure of protected health information. Several commenters asked that we define "unauthorized" or that we clarify its meaning. We clarify that "unauthorized" is an impermissible use or disclosure of protected health information under the HIPAA Privacy Rule (subpart E of 45 CFR part 164). Accordingly, the definition of "breach" at § 160.402 of the interim final rule interprets the "unauthorized acquisition, access, use, or disclosure of protected health information" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part." We emphasize that not all violations of the Privacy Rule will be breaches under this subpart, and therefore, covered entities and business associates need not provide breach notification in all cases of impermissible uses and disclosures. We also note that the HIPAA Security Rule provides for administrative, physical, and technical safeguards and organizational requirements for electronic protected health information, but does not govern uses and disclosures of protected health information. Accordingly, a violation of the Security Rule does not itself constitute a potential breach under this subpart, although such a violation may lead to a use or disclosure of protected health information that is not

permitted under the Privacy Rule and thus, may potentially be a breach under this subpart.

The Act does not define the terms "acquisition" and "access." Several commenters asked that we define or identify the differences between acquisition, access, use, and disclosure of protected health information, for purposes of the definition of "breach." We interpret "acquisition" and "access" to information based on their plain meanings and believe that both terms are encompassed within the current definitions of "use" and "disclosure" in the HIPAA Rules. Accordingly, we have not added separate definitions for these terms. We have retained the statutory terms in the regulation in order to maintain consistency with the statute. In addition, we note that while the HIPAA Security Rule at § 164.304 includes a definition of the term "access," such definition is limited to the ability to use "system resources" and not to access to information more generally and thus, we have revised that definition to make clear that it does not apply for purposes of these breach notification rules.

For an acquisition, access, use, or disclosure of protected health information to constitute a breach, it must constitute a violation of the Privacy Rule. Therefore, one of the first steps in determining whether notification is necessary under this subpart is to determine whether a use or disclosure violates the Privacy Rule. We note that uses or disclosures that impermissibly involve more than the minimum necessary information, in violation of §§ 164.502(b) and 164.514(d), may qualify as breaches under this subpart. In contrast, a use or disclosure of protected health information that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule

pursuant to 45 CFR 164.502(a)(1)(iii) and, therefore, would not qualify as a potential breach. Finally, violations of administrative requirements, such as a lack of reasonable safeguards or a lack of training, do not themselves qualify as potential breaches under this subpart (although such violations certainly may lead to impermissible uses or disclosures that qualify as breaches).

Compromises the Security or Privacy of Protected Health Information

The Act and regulation next limit the definition of "breach" to a use or disclosure that "compromises the security or privacy" of the protected health information. Accordingly, once it is established that a use or disclosure violates the Privacy Rule, the covered entity must determine whether the violation compromises the security or privacy of the protected health information.

For the purposes of the definition of "breach," many commenters suggested that we add a harm threshold such that an unauthorized use or disclosure of protected health information is considered a breach only if the use or disclosure poses some harm to the individual. These commenters noted that the "compromises the security or privacy" language in § 13400(1)(A) of the Act contemplates that covered entities will perform some type of risk assessment to determine if there is a risk of harm to the individual, and therefore, if a breach has occurred. Commenters urged that the addition of a harm threshold to the definition would also align this regulation with many State breach notification laws that require entities to reach similar harm thresholds before providing notification. Finally, some commenters noted that failure to include a harm threshold for requiring breach notification may diminish the impact of notifications received by individuals, as individuals may be flooded with notifications for breaches that pose no

threat to the security or privacy of their protected health information or, alternatively, may cause unwarranted panic in individuals, and the expenditure of undue costs and other resources by individuals in remedial action.

We agree that the statutory language encompasses a harm threshold and have clarified in paragraph (1) of the definition that "compromises the security or privacy of the protected health information" means "poses a significant risk of financial, reputational, or other harm to the individual." This ensures better consistency and alignment with State breach notification laws, as well as existing obligations on Federal agencies (some of which also must comply with these rules as HIPAA covered entities) pursuant to OMB Memorandum M-07-16 to have in place breach notification policies for personally identifiable information that take into account the likely risk of harm caused by a breach in determining whether breach notification is required. Thus, to determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, covered entities and business associates may need to consider a number or combination of factors, some of which are described below.[7]

Covered entities and business associates should consider who impermissibly used or to whom the information was impermissibly disclosed when evaluating the risk of harm to individuals. If, for example, protected health information is impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules or to a

[7] Covered entities may also wish to review OMB Memorandum M-07-16 for examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the individual.

Federal agency that is obligated to comply with the Privacy Act of 1974 (5 USC 552a) and the Federal Information Security Management Act of 2002 (44 USC 3541 et seq.), there may be less risk of harm to the individual, since the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. In contrast, if protected health information is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater.

We expect that there may be circumstances where a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such steps eliminate or reduce the risk of harm to the individual to a less than "significant risk," then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

In addition, there may be circumstances where impermissibly disclosed protected health information is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop. Note, however, that if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.

In performing a risk assessment, covered entities and business associates should also consider the type and amount of protected health information involved in the impermissible use or disclosure. If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach. For example, if a covered entity improperly discloses protected health information that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program[8]), or if the protected health information includes information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information. The risk assessment should be fact specific, and the covered entity or business associate should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm – especially in light of fears about employment discrimination.

We also address impermissible uses and disclosures involving limited data sets (as the term is used at 45 CFR 164.514(e) of the Privacy Rule), in paragraph (1) of the

[8] Note that an impermissible disclosure that indicates that an individual has received services from a substance abuse treatment program may also constitute a violation of 42 U.S.C. 290dd-2 and the implementing regulations at 42 CFR part 2. These provisions require the confidentiality of substance abuse patient records.

definition of "breach" at § 164.402 of the interim final rule. In the RFI discussed above, we asked for public comment on whether limited data sets should be considered unusable, unreadable, or indecipherable and included as a methodology in the guidance. A limited data set is created by removing the 16 direct identifiers listed in § 164.514(e)(2) from the protected health information.[9] These direct identifiers include the name, address, social security number, and account number of an individual or the individual's relative, employer, or household member. When these 16 direct identifiers are removed from the protected health information, the information is not completely de-identified pursuant to 45 CFR 164.514(b). In particular, the elements of dates, such as dates of birth, and zip codes, are allowed to remain within the limited data set, which increase the potential for re-identification of the information. Because there is a risk of re-identification of the information within a limited data set, the Privacy Rule treats this information as protected health information that may only be used or disclosed as permitted by the Privacy Rule.

Several commenters suggested that the limited data set should not be included in the guidance as a method to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification is not required. These commenters cited concerns about the risk of re-identification of protected health information in a limited data set and noted that, as more data exists in electronic form and as more data becomes public, it will be easier to combine these various sources to re-

[9] A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

establish the identity of the individual. Furthermore, due to the risk of re-identification, these commenters stated that creating a limited data set was not comparable to encrypting information, and therefore, should not be included as a method to render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

The majority of commenters, however, did support the inclusion of the limited data set in the guidance. These commenters stated that it would be impractical to require covered entities and business associates to notify individuals of a breach of information within a limited data set because, by definition, such information excludes the very identifiers that would enable covered entities and business associates, without undue burden, to identify the affected individuals and comply with the breach notification requirements. Additionally, these commenters cited contractual concerns regarding the data use agreement, which prohibits the recipient of a limited data set from re-identifying the information and therefore, may pose problems with complying with the notification requirements of § 13402(b) of the Act.

These commenters also noted that the decision to exclude the limited data set from the guidance, such that a breach of a limited data set would require breach notification, would reduce the likelihood that covered entities would continue to create and share limited data sets. This, in turn, would have a chilling effect on the research and public health communities, which rely on receiving information from covered entities in limited data set form.

Finally, commenters noted that the removal of the 16 direct identifiers in the limited data set presents a minimal risk of serious harm to the individual by limiting the possibility that the information could be used for an illicit purpose if breached. These

commenters also suggested that the inclusion of the limited data set in the guidance would align with most state breach notification laws, which, as a general matter, only require notification when certain identifiers are exposed and when there is a likelihood that the breach will result in harm to the individual.

We also asked commenters if they believed that the removal of an individual's date of birth or zip code, in addition to the 16 direct identifiers in 45 CFR 164.514(e)(2), would reduce the risk of re-identification of the information such that it could be included in the guidance. Several commenters responded to this question. While some stated that the removal of these data elements would render the information useless to the research and public health communities, which may, for example, require zip codes for many population based studies, many commenters did acknowledge that the removal of these additional identifiers would reduce the risk of re-identification of the information.

After considering these comments, we decided against including the limited data set in the guidance as a method for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals due to the potential risk of re-identification of this information. However, we address breaches of limited data sets in the definition of "breach" as follows.

Under the definition of "breach" at § 164.402, in order to determine whether a covered entity's or business associate's impermissible use or disclosure of protected health information constitutes a breach, the covered entity or business associate will need to perform the risk assessment discussed above. This applies to impermissible uses or disclosures of protected health information that constitute a limited data set, unless, as discussed below, the protected health information also does not include zip codes or dates

of birth. In performing the risk assessment to determine the likely risk of harm caused by an impermissible use or disclosure of a limited data set, the covered entity or business associate should take into consideration the risk of re-identification of the protected health information contained in the limited data set.

Through a risk assessment, a covered entity or business associate may determine that the risk of identifying a particular individual is so small that the use or disclosure poses no significant risk of harm to any individuals. For example, it may be determined that an impermissible use or disclosures of a limited data set that includes zip codes, based on the population features of those zip codes, does not create a significant risk that a particular individual can be identified. Therefore, there would be no significant risk of harm to the individual. If there is no significant risk of harm to the individual, then no breach has occurred and no notification is required. If, however, the covered entity or business associate determines that the individual can be identified based on the information disclosed, and there is otherwise a significant risk of harm to the individual, then breach notification is required, unless one of the other exceptions discussed below applies.

We have provided a narrow, explicit exception to what compromises the privacy or security of protected health information for a use or disclosure of protected health information that excludes the 16 direct identifiers listed at 45 CFR 164.514(e)(2) as well as dates of birth and zip codes. Thus, we deem an impermissible use or disclosure of this information to not compromise the security or privacy of the protected health information, because we believe that impermissible uses or disclosures of this information – if subjected to the type of risk assessment described above – would pose a

low level of risk. We emphasize that this is a narrow exception. If, for example, the information does not contain birth dates but does contain zip code information or contains both birth dates and zip code information, then this narrow exception would not apply, and the covered entity or business associate would be required to perform a risk assessment to determine if the risk of re-identification poses a significant risk of harm to the individual. We invite comments on this narrow exception. We do not believe that this narrow exception will have the unintended consequence of discouraging the use of encryption and other methods for rendering protected health information unusable, unreadable, or indecipherable; however, we invite comments on this issue as well. Finally, we note that this narrow exception should not be construed as encouraging or permitting the use or disclosure of more than the minimum necessary information, in violation of §§ 164.502(b) and 164.514(d).

We do not intend to interfere with research or public health activities that rely on dates of birth or zip codes. Uses and disclosures of limited data sets that include this information continue to be permissible under the Privacy Rule if the applicable requirements, such as a data use agreement, are satisfied. Further, we note that a covered entity or business associate is not responsible for a breach by a third party to whom it permissibly disclosed protected health information, including limited data sets, unless the third party received the information in its role as an agent of the covered entity or business associate. To the extent that a third party recipient of the information is itself a covered entity, and the information is breached while at the third party (i.e., used or disclosed in an impermissible manner and in a manner determined to compromise the privacy or security of the information), then the third party will be responsible for

complying with the provisions of this interim final rule. In cases where a covered entity is the recipient of a limited data set pursuant to § 164.514(e) of the Privacy Rule and it is unable to re-identify the individuals after a breach occurs, it may satisfy the requirements of § 164.404 without re-identifying the information, by providing substitute notice to the individuals as required by paragraph (d)(2) of that section.

We note that the discussion above regarding "limited data sets" applies to any protected health information that excludes the 16 direct identifiers listed at §164.514(e)(2), regardless of whether the information is used for health care operations, public health, or research purposes (see §164.514(e)(3)(i)), and is subject to a data use agreement under § 164.514(e) of the Privacy Rule. Thus, for example, a covered entity that impermissibly uses or discloses data that is stripped of the 16 direct identifiers described above, zip codes, and dates of birth, may take advantage of the exception to what is a breach, regardless of the intended purpose of the use or disclosure or whether a data use agreement was in place.

With respect to any type of protected health information, we note that § 164.414, discussed below, gives covered entities and business associates the burden of demonstrating that no breach has occurred because the impermissible use or disclosure did not pose a significant risk of harm to the individual. Covered entities and business associates must document their risk assessments, so that they can demonstrate, if necessary, that no breach notification was required following an impermissible use or disclosure of protected health information. For impermissible uses or disclosures of protected health information that fall under the narrow exception at paragraph (1)(ii) of this definition, which do not qualify as breaches because the protected health information

is a limited data set that does not include zip codes or dates or birth, documentation that demonstrates that the lost information did not include these identifiers will suffice.

Exceptions to Breach

Section 13400(1) of the Act also includes three exceptions to the definition of "breach" that encompass situations Congress clearly intended to not constitute breaches: (1) unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate (§ 13400(1)(B)(i)); (2) inadvertent disclosure of protected health information from one person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate (§ 13400(1)(B)(ii) and (iii)); and (3) unauthorized disclosures in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information (§ 13400(1)(A)). We have included these three exceptions as paragraphs (2)(i), (ii), and (iii), respectively.

The first regulatory exception at paragraph (2)(i) of this definition, for unintentional acquisition, access, or use of protected health information, generally mirrors the exception in § 13400(1)(B)(i) of the Act. This statutory section excepts from the definition of "breach" the unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or a business associate, if the acquisition, access, or use was made in good faith, within the course and scope of employment or other professional relationship, and does not result in further use or disclosure.

We modified the statutory language to use "workforce members" instead of employees. Workforce member is a defined term in 45 CFR 160.103 and means "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf. This may include a workforce member of a covered entity, an employee of a business associate, or even a business associate of a covered entity. Similarly, to determine whether the access, acquisition, or use was made "within the scope of authority," the covered entity or business associate should consider whether the person was acting on its behalf at the time of the inadvertent acquisition, access, or use.

Additionally, while the statutory language provides that this exception applies where the recipient does not further use or disclose the information, we have interpreted this exception as encompassing circumstances where the recipient does not further use or disclose the information in a manner not permitted under the Privacy Rule. In circumstances where any further use or disclosure of the information is permissible under the Privacy Rule, we interpret that there is no breach because the security and privacy of the information has not been compromised by any such permissible use or disclosure.

To illustrate this exception, we offer the following example. A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then

deletes it. The billing employee unintentionally accessed protected health information to which he was not authorized to have access. However, the billing employee's use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.

In contrast, a receptionist at a covered entity who is not authorized to access protected health information decides to look through patient files in order to learn of a friend's treatment. In this case, the impermissible access to protected health information would not fall within this exception to breach because such access was neither unintentional, done in good faith, nor within the scope of authority.

The second regulatory exception, at paragraph (2)(ii) of this definition, covers inadvertent disclosures and generally mirrors the exception provided in § 13400(1)(B)(ii) and (iii) of the Act, with slight modifications. The statute excepts from the definition of "breach" inadvertent disclosures from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility if the information is not further used or disclosed without authorization. We have modified the statutory language slightly to except from breach inadvertent disclosures of protected health information from a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates. Organized health care arrangement

is defined by the HIPAA Rules to mean, among other things, a clinically integrated care setting in which individuals typically receive health care from more than one health care provider.[10] See 45 CFR 160.103. This includes, for example, a covered entity, such as a hospital, and the health care providers who have staff privileges at the hospital.

We received several comments with respect to this exception, and many commenters asked that we clarify and explain the statutory language regarding what it means to be a "similarly situated individual" and what constitutes the "same facility" for purposes of this exception. We believe that a "similarly situated individual," for purposes of the statute, means an individual who is authorized to access protected health information, and thus, for clarity, we have substituted this language for the statutory language in the regulation. Thus, a person who is authorized to access protected health information is similarly situated, for purposes of this regulation, to another person at the covered entity, business associate of the covered entity, or organized health care arrangement in which the covered entity participates, who is also authorized to access protected health information (even if the two persons may not be authorized to access the same types of protected health information). For example, a physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital. In contrast, the physician is not similarly situated to an employee at the hospital who is not authorized to access protected health information.

[10] 45 CFR 160.103 also defines "organized health care arrangement" to include "an organized system of health care in which more than one covered entity participates" and in which the participating covered entities engage in certain joint utilization review, quality assessment and improvement, or payment activities. In addition, the definition encompasses certain relationships between group health plans and health insurance issuers or health maintenance organizations (HMO), as well as relationships among group health plans which are maintained by the same plan sponsor.

Additionally, we have interpreted "same facility" to mean the same covered entity, business associate, or organized health care arrangement in which the covered entity participates and have substituted this language in the regulation. By focusing on the legal entity or status of the entities as an organized health care arrangement when interpreting "same facility," we believe we have more clearly captured the intent of the statute and have also alleviated commenter concerns that the term "facility" was too narrow. Therefore, the size of the covered entity, business associate, or organized health care arrangement will dictate the scope of this exception. If a covered entity has a single location, then the exception will apply to disclosures between a workforce member and, e.g., a physician with staff privileges at that single location. However, if a covered entity has multiple locations across the country, the same exception will apply even if the workforce member makes the disclosure to a physician with staff privileges at a facility located in another state.

We interpret the statutory limitation that the information not be "further acquired, accessed, used, or disclosed without authorization" as meaning that the information is not further used or disclosed in a manner not permitted by the Privacy Rule. Thus, this exception encompasses circumstances in which a person who is authorized to use or disclose protected health information within a covered entity, business associate, or organized health care arrangement inadvertently discloses that information to another person who is authorized to use or disclose protected health information within the same covered entity, business associate, or organized health care arrangement, as long as the recipient does not further use or disclose the information in violation of the Privacy Rule.

The final regulatory exception to breach at paragraph (2)(iii) of this definition mirrors the exception found in § 13400(1)(A) of the Act. The statute excepts from the definition of "breach" situations in which the unauthorized person to whom protected health information has been disclosed would not reasonably have been able to retain the information. We have slightly modified this language to except from "breach" situations where a covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure of protected health information was made would not reasonably have been able to retain the information.

For example, a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.

As another example, a nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the protected health information from the patient. If the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.

With respect to any of the three exceptions discussed above, a covered entity or business associate has the burden of proof, pursuant to § 164.414(b) (discussed below), for showing why breach notification was not required. Accordingly, the covered entity or

business associate must document why the impermissible use or disclosure falls under one of the above exceptions.

Based on the above, we envision that covered entities and business associates will need to do the following to determine whether a breach occurred. First, the covered entity or business associate must determine whether there has been an impermissible use or disclosure of protected health information under the Privacy Rule. Second, the covered entity or business associate must determine, and document, whether the impermissible use or disclosure compromises the security or privacy of the protected health information. This occurs when there is a significant risk of financial, reputational, or other harm to the individual. Lastly, the covered entity or business associate may need to determine whether the incident falls under one of the exceptions in paragraph (2) of the breach definition.

We treat the breach as having occurred at the time of the impermissible use or disclosure (or in the case of the exceptions listed at paragraphs (2)(i) and (ii) of the definition of "breach," at the time of the "further" impermissible use or disclosure), but recognize that a covered entity or business associate may require a reasonable amount of time to confirm whether the incident qualifies as a breach. As discussed below, a breach is considered discovered when the incident becomes known, not when the covered entity or business associate concludes the above analysis of whether the facts constitute a breach.

2. Unsecured Protected Health Information.

The interim final rule adopts a definition of "unsecured protected health information" to identify to what information the breach notification provisions apply.

Section 13402(h)(1)(A) of the Act defines "unsecured protected health information" as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance issued under [§ 13402(h)(2)]." Further, the Act at § 13402(h)(2) requires that the Secretary specify in the guidance the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Accordingly, the interim final rule defines "unsecured protected health information" to mean 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 guidance. We also provide in the regulation that the guidance will be published on the HHS web site.

Section 13402(h)(2) of the Act required that the Secretary initially issue such guidance, after consultation with stakeholders, no later than 60 days after enactment, or April 17, 2009. As discussed above, the Secretary issued the guidance along with a request for information on April 17, 2009, on the HHS web site at http://www.hhs.gov/ocr/privacy/ and the guidance was later published in the Federal Register on April 27, 2009 (74 FR 19006). The Department has reviewed the public comment received in response to the request for information and provides an update to the guidance in Section II of this document. As provided in this interim final rule, this updated guidance is also (and any future updates will be) available on the HHS web site at http://www.hhs.gov/ocr/privacy/.

We note that the definition of "unsecured protected health information" in the Act and this interim final rule incorporates generally the term "protected health information,"

as defined at 45 CFR 160.103 of the HIPAA Rules, which includes information in any form or medium. Accordingly, the term "unsecured protected health information" can include information in any form or medium, including electronic, paper, or oral form.

C. Notification to Individuals—Section 164.404

Section 164.404 of the interim final rule provides the requirements for the notifications covered entities are to provide to individuals affected by a breach of unsecured protected health information. This section includes implementation specifications regarding timeliness, content, and methods of the notice.

General Rule

Section 164.404(a)(1) provides the general rule that a covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. This regulatory provision implements § 13402(a) of the Act, but does not include the phrase "that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses" used in the statute to describe a covered entity's actions with respect to unsecured protected health information because inclusion of such terms was deemed unnecessary. In addition, the statute refers to protected health information that has been "accessed, acquired, or disclosed"; it does not include "used." In contrast, the statutory definition of "breach" refers to the "acquisition, access, use, or disclosure" of protected health information. For consistency with the definition, therefore, we have added "used" to the list of actions for which notification is required in § 164.404(a)(1).

Breaches Treated as Discovered

Section 164.404(a)(2) states that a breach shall be treated as discovered by a covered entity as of the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity. Thus, a covered entity is not liable for failing to provide notification in cases in which it is not aware of a breach unless the covered entity would have been aware of the breach had it exercised reasonable diligence. Section 164.404(a)(2) further provides that a covered entity is 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 (determined in accordance with the federal common law of agency). These provisions implement § 13402(c) of the Act but clarify that the federal common law of agency is to control in determining who is an agent of the covered entity. This approach is consistent with the HIPAA Enforcement Rule (45 CFR part 160, subparts C through E), which provides that the federal common law of agency applies in determining agency liability under the HIPAA Rules.

We have also modified the statutory language slightly to better conform to existing language in the HIPAA Enforcement Rule by incorporating the term "by exercising reasonable diligence." The term "reasonable diligence" means the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." We have made these clarifications for consistency and uniformity across the regulations.

Because a covered entity or business associate is liable for failing to provide notice of a breach when the covered entity or business associate did not know – but by exercising reasonable diligence would have known – of a breach, it is important for such entities to implement reasonable systems for discovery of breaches. We also note that these provisions attribute knowledge of a breach by a workforce member or other agent (other than the person committing the breach), such as certain business associates, to the covered entity itself. This is important, as knowledge of a breach, i.e., when a breach is treated as "discovered," starts the clock in terms of the period of time a covered entity has to make the notifications required by the interim final rule. Thus, covered entities should ensure their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

Timeliness

Regarding timeliness of individual notifications, § 164.404(b) mirrors the statutory requirement in § 13402(d) of the Act and requires that, except when law enforcement requests a delay in accordance with § 164.412 (provision discussed below), a covered entity shall send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the covered entity. Thus, provisions for timeliness should be read together with the above provisions for when a breach is treated as discovered. We expect a covered entity to make the individual notifications as soon as reasonably possible. The covered entity may take a reasonable time to investigate the circumstances surrounding the breach, in order to collect and develop the information that § 164.404(c) requires to be included in the notice

to the individual. As discussed below, covered entities are also permitted to provide the required information to individuals within the required time period in multiple mailings as the information becomes available.

In response to the RFI, some commenters suggested that suspected but unconfirmed breaches should not be treated as discovered until all the facts of the breach could be confirmed. Others suggested that 60 days was an insufficient amount of time to conduct a complete investigation and send the required notifications. We disagree. Waiting longer than 60 days to notify individuals of breaches of their unsecured protected health information could substantially increase the risk of harm to individuals as a result of the breach and decrease the ability of the individuals to effectively protect themselves from such harm. The statute and interim final rule provide that the notification must be provided without unreasonable delay and in no case later than 60 calendar days. The purpose of this period is to give covered entities and business associates time to conduct a prompt investigation into the incident to identify and collect the information needed to provide meaningful notice to the individual about what happened. Thus, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule.

Further, the duration of an investigation is limited by the statute and interim final rule's requirement that any delay be reasonable – the investigation cannot take an unreasonable amount of time. Thus, if a covered entity learns of an impermissible use or disclosure but unreasonably allows the investigation to lag for 30 days, this would constitute an unreasonable delay. Further, the 60 days is an outer limit and therefore, in

some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification. For example, if a covered entity has compiled the information necessary to provide notification to individuals on day 10 but waits until day 60 to send the notifications, it would constitute an unreasonable delay despite the fact that the covered entity has provided notification within 60 days.

We also note that if a covered entity promptly investigates a reported breach and can swiftly conclude that there was no breach, then the covered entity need not send out breach notifications. For example, where a laptop with unsecured protected health information is initially reported by an employee to be stolen but is discovered the next day in another secure office within the covered entity, then the covered entity need not send out breach notifications.

Content

Section 13402(f) of the Act sets forth the content requirements for the breach notice to the individual. Section 164.404(c) of the interim final rule implements § 13402(f) of the Act and requires the notification to include, to the extent possible, the following elements: (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 protected health information that were 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); (3) any 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 harm to individuals, and to protect against any further breaches;

and (5) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, web site, or postal address. With respect to indicating in the notification the types of protected health information involved in a breach, we emphasize that this provision requires covered entities to describe only the types of information involved. Thus, covered entities should not include a listing of the actual protected health information that was breached (e.g., list in the notice the individual's social security number or credit card number that was breached) and generally should avoid including any sensitive information in the notification itself. Further, in the interim final rule at § 164.404(c)(1)(B), we add the term "diagnosis" in the parenthetical listing of examples of types of protected health information to make clear that, where appropriate, a covered entity may need to indicate in the notification to the individual whether and what types of treatment information were involved in a breach. In addition, at § 164.404(c)(1)(D), we replace the statutory term "mitigate losses" with "mitigate harm to the individual" to make clear that the notification should describe the steps the covered entity is taking to mitigate potential harm to the individual resulting from the breach and that such harm is not limited to economic loss.

Under these content requirements, for example, and depending on the circumstances, the notice to the individual may include recommendations that the individual contact his or her credit card company and information about how to contact the credit bureaus and obtain credit monitoring services (if credit card information was breached); information about steps the covered entity is taking to retrieve the breached information, such as filing a police report (if a suspected theft of unsecured protected

health information occurred); information about steps the covered entity is taking to improve security to prevent future similar breaches; and information about sanctions the covered entity imposed on workforce members involved in the breach.

Some commenters recommended that we impose a page limitation on the length of the notice (e.g., one-page in length) and ensure the content of the notice is non-technical and non-complex so individuals can easily understand the information being provided. We agree that it is important for individuals to be able to understand the information being provided to them in the breach notifications and thus, at § 164.404(c)(2) of the interim final rule, include a requirement that such notifications be written in plain language. To satisfy this requirement, the covered entity should write the notice at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey. We do not impose a page limitation, however, so as not to constrain covered entities in including in the notifications the information they believe could be helpful to individuals.

Further, we note that some covered entities may have obligations under other laws with respect to their communication with affected individuals. For example, to the extent a covered entity is obligated to comply with Title VI of the Civil Rights Act of 1964, the covered entity must take reasonable steps to ensure meaningful access for Limited English Proficient persons to the services of the covered entity, which could include translating the notice into frequently encountered languages. Similarly, to the extent that a covered entity is obligated to comply with Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, the covered entity has an obligation to take steps that may be necessary to ensure effective communication with individuals

with disabilities, which could include making the notice available in alternate formats, such as Braille, large print, or audio.

Methods of Notification

Section 13402(e)(1) of the Act provides for both actual written notice to the individual, as well as substitute notice to the individual if contact information is insufficient or out-of-date. Accordingly, the interim final rule at § 164.404(d) adopts the statutory provisions for actual and substitute breach notification to the individual.

Section 164.404(d)(1)(i) requires a covered entity to provide breach notice to the individual in written form by first-class mail at the last known address of the individual. Consistent with the statute, the interim final rule also provides that written notice may be in the form of electronic mail, provided the individual agrees to receive electronic notice and such agreement has not been withdrawn. We note that, consistent with § 164.502(g) of the Privacy Rule, where the individual affected by a breach is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice to the parent or other person who is the personal representative of the individual will satisfy the requirements of § 164.404(d)(1). The statute also requires that, if the individual is deceased, notice must be sent to the last known address of the next of kin. The interim final rule adopts this provision at § 164.404(d)(1)(ii), but provides that such notice be sent to either the individual's next of kin or personal representative, as such term is used for purposes of the Privacy Rule, recognizing that in some cases, a covered entity may have contact information for a personal representative of a deceased individual rather than the next of kin. We believe this conforms to the intent of the statute and improves consistency between this subpart and the Privacy Rule. Under 45 CFR 164.502(g), a "personal

representative" of a deceased individual is a person who has authority to act on behalf of the decedent or the decedent's estate. The interim final rule also clarifies that a covered entity is only required to provide notice to next of kin or the personal representative if the covered entity both knows the individual is deceased and has the address of the next of kin or personal representative of the decedent. This clarification should address some of the comments which raised both administrative and privacy concerns with a covered entity being required to obtain contact information for next of kin of a deceased patient, if the individual did not otherwise provide the information while alive.

If a covered entity does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, the covered entity must provide substitute notice for the unreachable individuals in accordance with § 164.404(d)(2) of the interim final rule. Substitute notice should be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals. Whatever form of substitute notice is provided, the notice must contain all the elements that § 164.404(c) requires be included in the direct written notice to individuals. With respect to decedents, however, the rule provides that a covered entity is not required to provide substitute notice for the next of kin or personal representative in cases where the covered entity either does not have contact information or has out-of-date contact information for the next of kin or personal representative.

Section 164.404(d)(2) requires that the substitute form of notice be reasonably calculated to reach the individuals for whom it is being provided. If there are fewer than 10 individuals for whom the covered entity has insufficient or out-of-date contact

information to provide the written notice, § 164.404(d)(2)(i) permits the covered entity to provide substitute notice to such individuals through an alternative form of written notice, by telephone, or other means. For example, if the covered entity learns that the home address it has for one of its patients is out-of-date but it has the patient's e-mail address, it may provide substitute notice by e-mail even if the patient has not agreed to electronic notice. Similarly, in the above example, if the covered entity has a current telephone number rather than e-mail address for the patient, then the covered entity may telephone the patient and provide the information required by the notice over the phone. We note however, that the covered entity should be sensitive to not unnecessarily disclose protected health information in the process of providing substitute notice, such as where the covered entity leaves an answering machine message that could be picked up by other household members. In such cases, the covered entity should take care to limit the amount of information disclosed on an answering machine message, such as, for example, by leaving only its name and number and indicating it has a very important message for the individual. Alternatively, posting a notice on the web site of the covered entity or at another location may be appropriate if the covered entity lacks any current contact information for the patients, so long as the posting is done in a manner that is reasonably calculated to reach the individuals.

If a covered entity has insufficient or out-of-date contact information for 10 or more individuals, then § 164.404(d)(2)(ii) requires the covered entity to provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. As described

above, these substitute notifications must be provided in a manner that is reasonably calculated to reach the affected individuals. In addition, substitute notice through the website or media for 10 or more individuals requires the covered entity to have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured protected health information may be included in the breach and to include the number in the notice.

If the covered entity chooses to provide substitute notice on the home page of its web site, the notice must be conspicuous and posted for at least 90 days. A covered entity may provide all the information described at § 164.404(c) directly on its home page or may provide a hyperlink to the notice containing such information. We interpret "home page" to include the home page for visitors to the covered entity's web site and the landing page or login page for existing account holders. If a covered entity uses a hyperlink on the home page to convey the substitute notice, the hyperlink should be prominent so that it is noticeable given its size, color, and graphic treatment in relation to other parts of the page, and it should be worded to convey the nature and importance of the information to which it leads.

Alternatively, or if the covered entity does not have or does not wish to use a web site for the substitute notice, the covered entity may provide substitute notice of the breach in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. What constitutes major print or broadcast media for a particular area will depend on the geographic area where the affected individuals are likely to reside and what is reasonably calculated to reach the affected individuals. We emphasize that what is considered major print or broadcast media for a metropolitan area

may be very different from what is considered major print or broadcast media in a rural area. For example, if the affected individuals are reasonably likely to reside in a rural area, then a local newspaper could be the major newspaper serving that area and most likely to reach the individuals affected. For affected individuals in a metropolitan area, then a newspaper serving the entire metropolitan area or the entire State would be more likely to reach the individuals affected. If the affected individuals likely reside in different regions or States, then the covered entity may need to utilize multiple media outlets to reasonably reach these individuals.

Also, we clarify in this interim final rule that any notice in print or broadcast media under this section must be conspicuous, similar to the posting on the web site. Thus, for example, for notice in print media, thought should be given to what location and duration of the notice is reasonably calculated to reach the affected individuals.

Some commenters were concerned that providing substitute notice in major media would be costly and onerous. Covered entities that are concerned with the cost of providing substitute notice in this manner have the option of instead posting the substitute notice on their web sites. For smaller covered entities that do not have web sites, we would expect those covered entities generally serve a patient population located in a relatively compact and discrete area. In such cases, the geographic area in which the affected individuals reside would be comparably small, and, therefore, we do not believe that providing substitute notice in the appropriate local newspaper or television station would be excessively costly or onerous. Finally, we note that covered entities with out-of-date or insufficient contact information for some individuals can attempt to update the contact information so that they can provide direct written notification, in order to limit

the number of individuals for whom substitute notice is required and, thus, potentially avoid the obligation to provide substitute notice through a web site or major print or broadcast media under §164.404(d)(2)(ii).

Other commenters were concerned that the requirement to include a toll-free phone number in the substitute media notice would overly burden a covered entity with calls from individuals unaffected by the breach. We note that the statute requires that covered entities include a toll-free phone number in cases where substitute notice is required for 10 or more individuals. Covered entities concerned with the number of calls they may receive from unaffected individuals may wish to include sufficient information in the notice itself or a web address in the notice for more information (or other means) as a way for individuals to determine whether their information may have been included in the breach.

Additional Notice in Urgent Situations

Finally, § 164.404(d)(3) of the interim final rule implements the provision in the statute at § 13402(e)(1)(c), which makes clear that notice by telephone or other means may be made, in addition to written notice, in cases deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information. We emphasize however that such notice, if utilized, is in addition to, and not in lieu of, the direct written notice required by § 164.404(d)(1).

D. Notification to the Media—164.406

Section 164.406 implements § 13402(e)(2) of the Act, which requires that notice be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500

residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This media notice differs from the substitute media notice described in § 164.404(d)(1)(2) in that it is directed "to" the media and is intended to supplement, but not substitute for, individual notice. The Act requires that notification to the media under this provision be provided within the same timeframe as notice is to be provided to the individual. See § 13402(d)(1) of the Act. Accordingly, § 164.406(b) of the interim final rule requires a covered entity to notify prominent media outlets without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. In paragraph (c) of this section, we require that notification to the media under this provision include the same information required to be included in the notification to the individual under § 164.404(c). We expect that most covered entities will provide notification to the media under this section in the form of a press release.

Commenters asked that we define what constitutes a "prominent media outlet." We do not define "prominent media outlet" in this regulation because what constitutes a prominent media outlet will differ depending upon the State or jurisdiction affected. For example, for a breach affecting 500 or more individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sport, politics) would not be viewed as a prominent media outlet. If a breach affects 500 or more individuals in a limited jurisdiction, such as a city, then a prominent media outlet

may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.

Commenters also asked HHS to clarify what is meant by "State or jurisdiction" for purposes of notice to the media under this provision. We note that "State" is already defined at § 160.103 of the HIPAA Rules to mean "any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam." That definition applies to this new provision. We also note that the Act includes a definition of "State" which applies for purposes of this provision and defines "State" to include, in addition to what is included at §160.103, American Samoa and the Northern Mariana Islands. Thus, we provide at §164.406(a) that, for purposes of this provision, "State" also includes American Samoa and the Northern Mariana Islands. With respect to jurisdiction, we clarify that, for purposes of this provision, jurisdiction is a geographic area smaller than a state, such as a county, city, or town.

To illustrate how these provisions apply, we provide the following example. If laptops containing the unsecured protected health information of more than 500 residents of a particular city were stolen from a covered entity, notification under this section should be provided to prominent media outlets serving that city. In this case, the prominent media outlet may be a major television station or newspaper (or other media outlet) serving primarily the residents of that city or a prominent media outlet serving the entire state. Alternatively, for a breach involving 500 or more residents across a State and not within any one particular county or city of the State, the prominent media outlet chosen must serve the entire State.

In response to comments received, we also offer clarification on how to address a breach involving residents in multiple States or jurisdictions. For example, if a covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media pursuant to § 164.406. However, individual notification under §164.404 would be required, as would notification to the Secretary under § 164.408 because the breach involved 500 or more individuals. Conversely, if a covered entity discovered a breach of unsecured protected health information involving 600 residents within the state of Maryland and 600 residents of the District of Columbia, notification must be provided to a prominent media outlet serving the state of Maryland and to a prominent media outlet serving the District of Columbia.

We also recognize that in some cases a breach may occur at a business associate and involve the protected health information of multiple covered entities. In that case, a covered entity involved would only be required to provide notification to the media if the information breached included the protected health information of 500 or more individuals located in any one State or jurisdiction. For example, if a business associate discovers a breach affecting 800 individuals, the business associate must notify the appropriate covered entity (or covered entities) subject to § 164.410 (discussed below). If 450 of the affected individuals are patients of one covered entity and the remaining 350 are patients of another covered entity, because the breach has not affected more than 500 individuals at either covered entity, there is no obligation to provide notification to the

media under this section. Additionally, neither covered entity has the obligation of notifying the Secretary under § 164.408(b) concurrently with notice to the affected individuals; however, both covered entities must include this breach in their annual submission to the Secretary pursuant to § 164.408(c). In cases where the entities involved are unable to determine which entity's protected health information was involved, the covered entities may consider having the business associate provide the notification to the media on behalf of all of the covered entities.

Section 164.406(c) sets forth the content requirement for covered entities notifying the media. In this section, we require that the notice to the media include the same content as that required for notification to the individual under § 164.404(c). We emphasize that this provision does not replace either direct written or substitute notice to the individual under §164.404. If a covered entity is required to provide substitute notice under § 164.404(d)(2)(ii)(A) and chooses to do so through major print or broadcast media, notification to the media under this section would only satisfy such substitute notice if the prominent media outlet ran a notification reasonably calculated to reach the individuals for which substitute notice was required and included all the information required be provided in the individual notice, including the toll-free number required by § 164.404(d)(2)(ii)(B).

E. Notification to the Secretary—164.408

Section 164.408 of the interim final rule implements § 13402(e)(3) of the Act, which requires covered entities to notify the Secretary of breaches of unsecured protected health information. For breaches involving 500 or more individuals, the Act requires covered entities to notify the Secretary immediately. For breaches involving less than

500 individuals, the Act provides that a covered entity may maintain a log of such breaches and annually submit such log to the Secretary documenting the breaches occurring during the year involved.

Section 164.408(a) of the interim final rule contains the general rule that requires a covered entity to notify the Secretary following the discovery of a breach of unsecured protected health information. Section 164.408(b) provides the implementation specification for breaches involving 500 or more individuals. Section 164.408(c) provides the implementation specification for breaches involving fewer than 500 individuals.

With respect to breaches involving 500 or more individuals, we interpret the term "immediately" in the statute to require notification be sent to the Secretary in the case of these larger breaches concurrently with the notification sent to the individual under §164.404, which must be sent without unreasonable delay but in no case later than 60 calendar days following discovery of a breach. Many commenters were concerned that covered entities would be required to provide notification to the Secretary in a much shorter time frame than the other notifications required by the Act, making it difficult for covered entities to comply. This interpretation thus allows the notice to the Secretary to include all of the information provided in the notice to the individual and better avoids the situation where a covered entity reports information to the Secretary that later turns out to be incorrect because the entity did not have sufficient time to conduct an investigation into the facts surrounding the breach. In addition, this interpretation satisfies the statutory requirement that notifications of larger breaches be provided to the Secretary immediately as compared to the reports of smaller breaches the statute allows

be reported annually to the Secretary. The interim final rule also provides that the notification be provided in a manner to be specified on the HHS web site. The Department will post instructions on its web site for submitting both this notification as well as the annual notification described below. In addition, as required by § 13402(e)(4) of the Act, the Secretary will post on the HHS web site a list of covered entities that submit reports of breaches of unsecured protected health information involving more than 500 individuals.

Covered entities must notify the Secretary of discovered breaches involving more than 500 individuals generally, without regard to whether the breach involved more than 500 residents of a particular State or jurisdiction (the threshold for triggering notification to the media under § 164.406 of the interim final rule). Thus, where a covered entity has discovered a breach of 600 individuals, 300 of which reside in Maryland and 300 of which reside in the District of Columbia, notification of the breach must be provided to the Secretary concurrently with notification to the affected individuals. However, the breach in this example would not trigger the requirement to notify the media under § 164.406 because the breach did not involve more than 500 residents of any one State or jurisdiction.

For breaches involving less than 500 individuals, § 164.408(c) requires a covered entity to maintain a log or other documentation of such breaches and to submit information annually to the Secretary for breaches occurring during the preceding calendar year. As recommended by several commenters, we have designated a date for submission of the information to the Secretary. The interim final rule requires the submission of this information to the Secretary no later than 60 days after the end of each

calendar year. As with notification of the larger breaches above, the interim final rule provides that information about breaches involving less than 500 individuals is to be provided to the Secretary in the manner specified on the HHS web site. HHS will specify on its web site the information to be submitted and how to submit such information.

For calendar year 2009, the covered entity is only required to submit information to the Secretary for breaches occurring after the effective date of this regulation; i.e., on or after [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. Information about breaches occurring prior to that date need not be submitted. This is because, pursuant to §164.400, this subpart only applies to breaches occurring on or after that date.

We emphasize that although covered entities need only provide notification to the Secretary of breaches involving less than 500 individuals annually, they must still provide notification of such breaches to affected individuals without unreasonable delay and not later than 60 days after discovery of the breach pursuant to § 164.404. In addition, we note that pursuant to § 164.414(a), a covered entity must follow the documentation requirements that otherwise apply to the HIPAA Privacy Rule under § 164.530 with respect to the requirements of this rule. Thus, pursuant to § 164.530(j)(2), covered entities must maintain the internal log or other documentation for six years. Further, as with other required documentation, a covered entity must make such information available to the Secretary upon request in accordance with § 160.310.

F. Notification by a Business Associate—164.410

Section 13402(b) of the Act requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or

discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information. Section 164.410(a) implements § 13402(b) of the Act, but does not include the terms "that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses" used in the statute to describe a business associate's actions with respect to unsecured protected health information because inclusion of such terms was deemed unnecessary.

Thus, following the discovery of a breach of unsecured protected health information, a business associate is required to notify the covered entity of the breach so that the covered entity can notify affected individuals. We clarify that a business associate that maintains the protected health information of multiple covered entities need notify only the covered entity(s) to which the breached information relates. However, in cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potential affected covered entities.

We received several comments in support of adding a provision to require business associates to provide notice to a senior official or privacy official at the covered entity. We do not believe such a provision is necessary, however. Covered entities and business associates already have established business relationships and communication channels, including with respect to privacy and security matters. For example, the HIPAA Rules already require a business associate contract to provide that the business associate report to the covered entity uses or disclosures not provided by the contract as well as security incidents of which the business associate becomes aware. See 45 CFR 164.504(e)(2)(ii)(C) and 164.314(a)(2)(i)(C). Thus, we believe it is appropriate to leave

it up to covered entities and business associates to determine how the required reporting should be implemented.

Section 164.410(a)(2) implements § 13402(c) of the Act, which provides when a breach is to be treated as discovered by the business associate. Accordingly, § 164.410(a)(2) states that 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. Section 164.410(a)(2) further provides that 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 (determined in accordance with the federal common law of agency). As with §164.404(a)(2) with respect to a covered entity's knowledge of a breach, we clarify in this provision that the federal common law of agency is to control in determining who is an agent of the covered entity. This approach is consistent with the HIPAA Enforcement Rule (45 CFR part 160, subparts C through E), which provides that the federal common law of agency applies in determining agency liability under the HIPAA Rules. Also, as with § 164.404(a)(2), we have modified the statutory language slightly to better conform to existing language in the HIPAA Enforcement Rule at 45 CFR 160.410, by incorporating the term "reasonable diligence." We have made these clarifications for consistency and uniformity across the regulations.

Section 164.410(b) implements § 13402(d)(1) of the Act and provides that, with the exception provided in § 164.412, a business associate must provide notice of a breach

of unsecured protected health information to a covered entity without unreasonable delay and in no case later than 60 days following the discovery of a breach. With respect to breaches at the business associate, the covered entity must provide the required notifications to affected individuals under § 164.404(a) without unreasonable delay, but no later than 60 days.

If a business associate is acting as an agent of a covered entity, then, pursuant to § 164.404(a)(2), the business associate's discovery of the breach will be imputed to the covered entity. Accordingly, in such circumstances, the covered entity must provide notifications under §164.404(a) based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity. In contrast, if the business associate is an independent contractor of the covered entity (i.e., not an agent), then the covered entity must provide notification based on the time the business associate notifies the covered entity of the breach. As reflected in the comments we received in response to the timing of business associate notification to a covered entity following a breach, covered entities may wish to address the timing of the notification in their business associate contracts.

Section 164.410(c) implements the second sentence of § 13402(b) of the Act, which specifies the information that a business associate must provide to a covered entity following a breach of unsecured protected health information. Section 164.410(c)(1) requires business associates, to the extent possible, to provide covered entities with the identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached. Depending on the circumstances, business associates may provide the covered entity with immediate notification of the breach, as

discussed above and then follow up with the required information in § 164.410(c) when available but without unreasonable delay and within 60 days.

Section 164.410(c)(1) departs slightly from the statutory language by only requiring business associates to provide this information "to the extent possible." Based on some comments received, we recognize that there may be situations in which a business associate may be unaware of the identification of the individuals whose unsecured protected health information was breached. For example, a business associate that is a record storage company holds hundreds of boxes of paper medical records on behalf of a covered entity. The business associate discovers that several boxes are missing and is unable to provide the covered entity with a list of the individuals whose information has been breached. It is not our intent that the business associate delay notification of the breach to the covered entity, when the covered entity may be better able to identify the individuals affected.

Further, we recognize that, depending on the circumstances surrounding a breach of unsecured protected health information, a business associate may be in the best position to gather the information the covered entity is required by § 164.404(c) to include in the notification to the individual about the breach. Thus, in addition to the identification of affected individuals, § 164.410(c)(2) requires a business associate to provide the covered entity with any other available information that the covered entity is required to include in the notification to the individual under § 164.404(c), either at the time it provides notice to the covered entity of the breach or promptly thereafter as information becomes available. Because we allow this information to be provided to a covered entity after the initial notification of the breach as it becomes available, a

business associate should not delay the initial notification to the covered entity of the breach in order to collect information needed for the notification to the individual. To ensure the covered entity is aware of all the available facts surrounding a breach, we also note that a business associate should provide this information even if it becomes available after notifications have been sent to affected individuals or after the 60-day period specified in § 164.410(b) has elapsed.

In response to a significant number of commenters who expressed concern that this requirement would prevent covered entities and their business associates from addressing these issues in their business associate contracts, we emphasize that we do not intend for this section to interfere with the current relationship between covered entities and their business associates. Business associates and covered entities will continue to have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals and when the notification from the business associate to the covered entity will be required, following a breach of unsecured protected health information, so long as all required notifications are provided and the other requirements of the interim final rule are met. We encourage the parties to consider which entity is in the best position to provide notice to the individual, which may depend on circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual. We also encourage the parties to ensure the individual does not receive notifications from both the covered entity and the business associate about the same breach, which may be confusing to the individual.

Finally, we note that where an entity provides PHRs to customers of a HIPAA covered entity through a business associate arrangement but also provides PHRs directly

to the public and a breach of its records occurs, in certain cases, as described in its rule, the FTC will deem compliance with certain provisions of HHS' rule as compliance with FTC's rule. In particular, in such situations, it may be appropriate for the vendor to provide the same breach notice to all its PHR customers since it has a direct relationship with all the affected individuals. Thus, in those limited circumstances where a vendor of PHRs (1) provides notice to individuals on behalf of a HIPAA covered entity, (2) has dealt directly with these individuals in managing their personal health record accounts, and (3) provides notice to its customers at the same time, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be compliance with the corresponding FTC rule provisions.[11]

G. Law Enforcement Delay—164.412

Section 13402(g) of the Act provides that if a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under 45 CFR 164.528(a)(2) of the Privacy Rule in the case of a disclosure covered under such section. Section 164.412 implements § 13402(g) of the Act and thus, requires a covered entity or business associate to temporarily delay notification under §§ 164.404, 164.406, 164.408, and 164.410 if instructed to do so by a law enforcement official.

We retain the definition of "law enforcement official" currently used in the Privacy Rule at § 164.501, which defines such person as "an officer or employee of any

[11] We note, however, that with respect to the customers to whom it provides PHRs directly, the vendor must comply with all other FTC rule requirements, including the requirement to notify the FTC within ten business days after discovering the breach.

state agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law." However, in this interim final rule, we move the definition up to §164.103 so that it will apply to this subpart D as well as continue to apply to subpart E (Privacy Rule).

Section 164.412(a), which is based on the requirements of 45 CFR 164.528(a)(2)(i) of the Privacy Rule, provides for a temporary delay of notification in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In these instances, the covered entity is required to delay the notification, notice, or posting for the time period specified by the official.

Similarly, § 164.412(b), which is based on 45 CFR 164.528(a)(2)(ii) of the Privacy Rule, requires a covered entity or business associate to temporarily delay a notification, notice, or posting if a law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security. However, in this case, the covered entity or business associate is required to document the statement and the identity of the official and delay notification for no longer than 30 days, unless a written statement meeting the above requirements is provided during that time. We interpret these provisions as tolling the time within which notification is required under §§ 164.404, 164.406, 164.408, and 164.410, as applicable.

H. Administrative Requirements and Burden of Proof—164.414

Section 164.414(a) requires covered entities to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) of the Privacy Rule with respect to the breach notification provisions of this subpart. These provisions, for example, require covered entities and business associates to develop and document policies and procedures, train workforce members on and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding these policies and procedures or a failure to comply with them, and require covered entities to refrain from intimidating or retaliatory acts. Thus, a covered entity is required to consider and incorporate the requirements of this subpart with respect to its administrative compliance and other obligations. In addition to §164.414(a), to make clear that these provisions apply to this subpart as well as subpart E, we have made conforming modifications in each of the above sections of the Privacy Rule to include a reference to this subpart D.

Consistent with § 13402(d)(2) of the Act, § 164.414(b) provides that, following an impermissible use or disclosure under the Privacy Rule, covered entities and business associates have the burden of demonstrating that all notifications were made as required by this subpart. Additionally, as part of demonstrating that all required notifications were made, we clarify in the regulatory text that a covered entity or business associate, as applicable, also must be able to demonstrate that an impermissible use or disclosure did not constitute a breach, as such term is defined at § 164.402, in cases where the covered entity or business associate determined that notifications were not required. We also make conforming changes to § 160.534 of the HIPAA Enforcement Rule to make clear

that, during any administrative hearing, the covered entity has the burden of going forward and the burden of persuasion with respect to these issues.

Thus, when a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment (discussed above in § 164.402) or the application of any exceptions to the definition of "breach" to demonstrate that notification was not required.

I. Other Conforming Changes to the HIPAA Rules

In addition to the conforming modifications discussed above, we make the following changes to align the HIPAA Rules in light of the new breach notification requirements of this rule. First, we revise the statutory basis and purpose sections at §§ 160.101 and 164.102 to include references to § 13402 of the Act. Second, in Part 160, for purposes of the preemption of State law, we amend § 160.202 to revise the definition of "contrary" to include a reference to § 13402 of the Act. (See below for a discussion of preemption and these new requirements.) Finally, in Part 164, subpart C, which contains the HIPAA Security Rule requirements, we revise the definition of "access" in § 164.304 to make clear that the definition does not apply to any use of the term in subpart D.

J. Preemption

We received several public comments regarding the issue of preemption and the interaction between this regulation and state breach notification laws. HIPAA (Pub. L. 104-191) added § 1178 of the Social Security Act, 42 U.S.C. 1320d-7, which sets forth the general effect of the HIPAA provisions on State law. Section 1178 provides that HIPAA administrative simplification provisions generally preempt conflicting State law.

This section of the statute is implemented by 45 CFR 160.203, which states that a standard, requirement, or implementation specification that is adopted as regulation at 45 CFR parts 160, 162, or 164 and that is "contrary to a provision of State law preempts the provision of State law." Section 160.203 provides several exceptions in which State law will not be preempted; however, we do not believe these exceptions apply to the breach notification regulations in 45 CFR part 164 subpart D.[12] Therefore, contrary State law will be preempted by these breach notification regulations. We solicit comment in this area.

Whether a State law is contrary to these breach notification regulations is to be determined based on the definition of "contrary" at § 160.202. A State law is contrary if "a covered entity could find it impossible to comply with both the State and federal requirements" or if the State law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the breach notification provisions in the Act. As discussed above, we make a conforming change to paragraph (2) of the definition of "contrary" in this section to incorporate reference to the breach notification provisions at § 13402 of the Act. Therefore, covered entities will need to analyze relevant State laws with respect to this regulation to understand the interaction and apply this preemption standard appropriately.

Although we received many comments concerning perceived conflicts between the interaction of State laws and these breach notification provisions, based on the "contrary" standard for preemption, in general we believe that covered entities can

[12] We do not interpret the preemption exception at § 160.203(b), which addresses more stringent State law related to privacy, as applying to these breach notification provisions because that paragraph only applies to the provisions of the Privacy Rule promulgated under § 264(c) of the HIPAA statute. See § 264(c)(2) of HIPAA.

comply with both the applicable State laws and this regulation. In addition, based on the comments received, we believe that, in most cases, a single notification can satisfy the notification requirements under State laws and this regulation. For example, if a state breach notification law requires notification to be sent to the individual within five days following the detection of a breach, a covered entity that sends that notice within five days to comply with State law will also be in compliance with this regulation, as the covered entity must send the notification "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." If covered entities do not have all the information required by this regulation available to them within five days, they may send the individual an additional notification when they have accumulated the appropriate information.

Likewise, if a State law requires a breach notification but requires additional elements be included in the notice, or requires that certain elements be described in a certain way, there is no conflict between the State law and this regulation. As the Act and interim final rule are flexible in terms of how the elements are to be described, and do not prohibit additional elements from being included in the notice, covered entities can develop a notice that satisfies both laws.

K. Effective/Compliance Date

Section 13402(j) of the Act states that § 13402 applies to breaches that are discovered by a covered entity or business associate on or after 30 calendar days from the date of publication of this interim final rule. Commenters expressed concern that this effective date did not allow enough time for covered entities to implement the guidance for rendering protected health information unusable, unreadable, or indecipherable to

unauthorized individuals or have systems in place to comply with the requirements of the rule and suggested that compliance with these breach notification provisions not be required in 30 days.

In response, we note that the guidance on securing protected health information is not mandatory; it is discretionary. Accordingly, a covered entity or business associate will not be out of compliance with this subpart if, after the date set forth at § 164.400, the entity maintains unsecured protected health information. We recognize, though, that many covered entities and business associates are voluntarily choosing to secure their protected health information in accordance with the guidance in order to avoid the possibility of having to provide breach notifications pursuant to this subpart. We encourage covered entities and business associates to take such an approach – securing their protected health information – and understand that the process may take more than 30 days from the publication of this interim final rule.

We also recognize that it will take covered entities and business associates time to implement the processes and procedures necessary to comply with this subpart. For example, once compliance with this subpart is required, a covered entity or business associate will be held accountable for breaches that, through the exercise of reasonable diligence, would have been known to the entity. This means that a covered entity or business associate must have reasonable systems in place to detect breaches. Putting such systems in place may take some time.

On the other hand, the majority of states already have breach notification laws in place. While this interim final rule differs from any such State laws, we believe that most covered entities or business associates should already have some form of breach

notification procedures in place. Those covered entities and business associates should be able to build upon such existing procedures in order to come into compliance with this interim final rule.

We have decided that, consistent with § 13402(j) of the Act, the provisions of this subpart are effective, and compliance is required, for breaches occurring on or after 30 calendar days from the publication of this rule. However, based on the concerns described above, and based on some ambiguity within the statute,[13] we will use our enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication of this rule, or [INSERT DATE 180 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. During this initial time period – after this rule has taken effect but before we are imposing sanctions – we expect covered entities to comply with this subpart and will work with covered entities, through technical assistance and voluntary corrective action, to achieve compliance.

V. Impact Statement and Other Required Analyses

A. Introduction

Section 13402 of the Act prescribes in specific terms the obligations and responsibilities on HIPAA covered entities to notify an affected individual when a breach of his or her unsecured protected health information occurs, to notify the Secretary, to

[13] While § 13402(j) of the HITECH Act provides that § 13402 becomes effective 30 calendar days after publication of this interim final rule, it is § 13410(a)(2) that provides the Department with authority to impose civil money penalties, pursuant to § 1176 of the Social Security Act (42 U.S.C. 1320d-5), on violations by covered entities of the requirements imposed by the HITECH Act, including those of § 13402. Moreover, authority to impose civil money penalties on business associates for violations of the HITECH Act is provided by §§ 13401(b) and 13404(c). Sections 13410(a)(2), 13401(b), and 13404(c) do not become effective until February 18, 2010 (see § 13423 of the Act). Thus, there is a statutory ambiguity due to the HITECH Act providing an effective date of 30 days from publication of this rule, but a later date for when the Department may impose civil money penalties for violations of § 13402.

notify the media in certain circumstances, and for business associates to notify covered entities of such breaches. In most instances, the interim final regulation adheres and conforms to the language of the statute in defining terms and in prescribing remedies. The rule tracks the language of the statute with regard to the actions covered entities must take to notify an affected individual when a reportable breach occurs, the time frame in which the covered entity must act, the mode of communicating with an affected individual and the content of the notice.

The prescriptive language of the statute leaves little discretion for the Secretary in how to implement the statute. Measures we have taken to modify the statutory language are minimal and were undertaken to make certain terms used in the statute conform to other parts of the HIPAA Rules. We also clarify when a breach of protected health information compromises the security or privacy of such information. Yet, because the statutory language is so detailed and specific as to the requirements and definitions placed on covered entities, and because we have endeavored to follow the statutory language as closely as possible, we believe that, in large measure, the economic burden imposed on covered entities results from the statute and not from the interim final regulation.

We have examined the impacts of this rule as required by Executive Order 12866 on Regulatory Planning and Review (September 30, 1993, as further amended), the Regulatory Flexibility Act (RFA) (5 U.S.C. 601 et seq.), section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532), Executive Order 13132 on Federalism (August 4, 1999), and the Congressional Review Act (5 U.S.C. 804(2)).

Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). A regulatory impact analysis (RIA) must be prepared for major rules with economically significant effects ($100 million or more in any one year). This interim final rule is not an economically significant rule because we estimate that the breach notification requirements are not expected to cost more than $100 million per year. Nevertheless, because of the public interest in this rule, we have prepared a RIA that to the best of our ability presents the costs and benefits of the proposed rule. We request comments on the economic analysis provided in this proposed rule.

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. The scope of the interim final rule will apply to all HIPAA covered entities and their business associates. Based on U.S. business census data provided to the Small Business Administration Office of Advocacy there were 605,845 entities classified under the North American Industrial Classification System (NAICS) 62. Code 62 encompasses physicians, dentist, ambulatory care, centers, kidney dialysis centers, family planning clinics, home care services, mental health and drug rehabilitation centers, medical laboratories, hospitals and nursing facilities. In addition, based on data from the Centers for Medicare & Medicaid Services, we estimate that there are 107,567 suppliers of durable medical equipment and prosthetics. Almost all of these health providers fall under the RFA's definition of a small entity by either meeting the Small Business

Administration's (SBA) size standard of a small business or by being a non-dominant nonprofit organization. The SBA's size standard for NAICS 62 ranges between $7 million and $34.5 million in annual receipts. Also covered under HIPAA are health insurance firms and third party administrators (NAICS codes 524114 and 524292). The 2006 business census data shows that there are 1,045 insurance firms and 3,522 third party administrators. Of the combined total of health insurance firms and third party administrators, we estimate that approximately 71 percent, or 3,266, meet the SBA's definition of a small entity of annual receipts of $7 million or less. Pharmacies are also considered covered entities under HIPAA (NAICS code 44611) and based on the 2007 National Association of Chain Drug Stores Industry Profile approximately 17,500 independent pharmacy drugstores meet the SBA definition of a small business of $7 million or less in annual receipts. For more information on SBA's size standards, see the Small Business Administration's web site at http://sba.gov/idc/groups/public/documents/sba_homepage/serv_sstd_tablepdf.pdf.

Although the RFA only requires an initial regulatory flexibility analysis (IRFA) when an agency issues a proposed rule, the Department has a policy of voluntarily conducting an IRFA for interim final regulations. We examine the burden of the interim final regulation in section D below.

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) also requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. In 2009, that threshold is approximately $133 million. This rule

will not impose an unfunded mandate on States, tribal government or the private sector of more than $133 million annually.

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct costs of compliance on State and local governments, preempts State law, or otherwise has Federalism implications. Section 13421(a) of the Act expressly provides that provisions or requirements of subtitle D of the Act, which includes the provisions requiring breach notification, shall preempt State law in the same respect that the HIPAA Rules preempt State law pursuant to § 1178 of the Social Security Act. Accordingly, this rule expressly adopts the preemption provisions that are applicable to the HIPAA Rules and as discussed in Section IV.J. Preemption above.

B. Why Is This Rule Needed?

This regulation is required to implement § 13402 of the Act. The purpose of the statute is to establish a uniform requirement on all HIPAA covered entities to inform individuals of when the individual's unsecured protected health information has been improperly used or disclosed and the result of the improper use or disclosure may lead to financial damage, harm to the individual's reputation, or other harm. Without the statutory requirement for notifying an individual of data breaches, it would be left to the entity to decide whether to notify an affected individual or the decision would be subject to significantly varying State laws (which are generally focused on breaches of financial information rather than health information).

Because notification requires expenditures and exposes the covered entity to loss of business and possible legal action, there is little incentive for the entity to take such

action. While individuals whose protected health information was improperly accessed would be forewarned and as a result of being notified, could take action to mitigate financial or personal harm, they may not continue to patronize the entity which notifies them. If alternative providers in the individual's community offer similar services, the individual may take their business to one of the alternative entities. Moreover, if other individuals, not directly affected by the breach, learn of the event, they too may seek services from other providers out of fear that their protected health information may be improperly accessed. The Ponenmon Institute, LLC report of February 2009, "2008 Annual Study: Cost of a Data Breach" estimates that 69 percent of the cost of a data breach is the result of lost business (see page 4). The study identifies the health care industry as experiencing the highest customer turnover rate directly attributable to data breaches of protected health information. Moreover, since a health care provider is unlikely to suffer financially from the direct loss of protected health information, there is little incentive for the covered entity to notify affected individuals.

In such situations, the covered entity may perceive that it is more beneficial to not disclose breaches. The possibility of lawsuits arising out of a lack of response to the breach represents a risk but one which is uncertain and lies in the future. This compares to the more imminent and certain risk of loss of business if the entity discloses the breach.

By imposing a duty on all covered entities to notify affected individuals of breaches of protected health information, the statute and the interim final regulation place a similar burden on all covered entities to notify affected individuals and run the same risk of losing business as a result of notification. Moreover, requiring breach notification

creates an incentive on all covered entities to invest in data security improvements in efforts to minimize the possibility of reportable data breaches.

At the same time that the statute and interim final regulation create the incentive to minimize breaches of protected health information, in the event that a breach occurs, the affected individual will be notified and thereby be given an opportunity to mitigate any harm that may result from the breach.

C. Costs and Benefits

1. Summary of Costs and Benefits

Throughout the following analysis we invite comments on specific portions of our analysis. The public, however, is invited to offer comments on any and all elements of the analysis and the assumption underlying the analysis.

Costs: In the analysis that follows, we applied the provisions of the interim final regulation to the dataset of data breaches found at DataLossdb.org. The database shows, among other things, the name of the organization and the type of business, such as finance, medical, government, education, or business. The field called "Total Affected" shows a count of either records or individuals affected by the breach. Without examining the source reports of the breach, we do not know which is being reported. For these purposes, we will take the more conservative approach and assume that the count is of individuals. We acknowledge the possibility that an individual may have more than one record housed at a provider, especially if the provider is a multi-unit facility. An individual may have separate inpatient, outpatient, and clinic records. Thus, a major breach could involve more than one record per breach, and to the extent that this is the case, we may overstate the costs, which we believe is preferable to understating them.

The data we selected covers calendar year 2008 and includes the subset of breaches from medical firms or containing medical information. Our analysis, thus, not only includes HIPAA covered entities found in the dataset but may include business associates of HIPAA covered entities. In addition, the data may include breaches of health information that State agencies may hold such as Medicaid State agencies that also serve as health plans and are also HIPAA covered entities. Table 1 presents the estimated costs of the interim final rule based on 2008 breaches presented in the DataLossdb.org tables.

Upon examining the distribution of affected individuals and records for 2008, we identified one breach involving 2.2 million individuals. The incident occurred at a major university hospital system and involved the theft of backup tapes that were being transported to storage. The next highest breach affected 344,482 individuals. Including the outlier breach in our analysis, we believe, would significantly skew the analysis. Removing this case produces a more homogeneous distribution of affected individuals and improves the reliability of the analysis. Removing the outlier reduced the number of affected individuals from 5,087,032 to 2,887,032.

Although the type of data breach that occurred in 2008 was not unusual, the number of persons affected was six times greater than the next highest breach and the number of individuals affected is far from the average number for the year. In 2007, a State mental health agency reported the loss of records affecting 2.9 million individuals resulting from the agency's data processor's negligence. The next largest breach in 2007 involved 375,000 individuals and represents one eighth the number of individuals in the mental health agency breach.

Without doubt, breaches of the magnitude we see in the university hospital and State mental health breaches are a serious concern to the Department. Excluding such disproportionately large breaches from the cost analysis should not be construed as a lack of interest or concern in the security of protected health information at these institutions. We could have included the university hospital breach in our 2008 analysis, but it is clear that the incident does not represent the average or typical case. Since our purpose is to present and illustrate the costs of an average breach, we believe that the inclusion of the one unusually large breach in 2008 would skew the results and present a distorted picture of the level of costs that a typical covered entity could expect.

In reviewing the following analysis, one must keep in mind that we are able to capture only breaches that are either reported to the DataLoss database or are reported in the media. We suspect that some percent of breaches in the healthcare sector as well as in other sectors of the economy go unreported either because they are not detected or because, in the opinion of the entity, no harm was done. We cannot determine if the "no harm" type of unreported breach would meet the harm threshold in § 164.402 of the interim final rule for a reportable breach. If some or all of such breaches reach the harm threshold for a breach, as defined in the interim final rule, then the analysis understates the cost of the rule to the degree that these breaches are not included in our analysis.

Table 1 shows the costs of the provisions of the interim final rule. We also present the costs required for investigating breaches and the amount of time we anticipate individuals will spend calling the toll-free number. The total cost estimated for the rule is $17 million based on the number of breaches and the number of affected individuals.

Table 1. Summary of Compliance Cost for Notifying Affected Individuals*

Cost Elements	Number of Breaches	Number of Affected Individuals	Cost/Breach	Cost/Affected Individuals	Cost
E-mail and 1st Class Mail	106	2,888,804	$12,986	$0.477	1,376,528
Alternative Notices					
Media Notice	70	2,888,804	$487	$0.012	$34,080
Toll-Free Number	70	2,888,804	$117,676	$2.851	$8,237,309
Imputed cost to affected individuals	70	2,888,804	$103,172	$2.500	$7,222,010
Notice to Media Breach 500+	56	2,887,032	$75	$0.001	$4,200
Report to the Secretary	56	2,887,032	$75	$0.001	$4,200
Investigation Costs					
Under 500	50	1,772	$400	$11	$20,000
Over 500	56	2,887,032	$2,211	$0.043	123,800
Annual Report to the Secretary	106	2,888,804	$30	$0.001	$3,180
TOTAL COST			$160,616	$5.89	$17,025,306

* Source: www.datalossdb.org

Our cost impact for HIPAA covered entities of approximately $17 million is approximately 350 percent of the FTC cost estimate for non-HIPAA covered entities. The FTC estimate was based on requiring toll-free lines for six months. Their final rule requires toll-free lines for only three months, as does this rule. This should reduce the FTC estimated costs by approximately half to about $5 million; about 30 percent of our cost estimate for HIPAA covered entities of $17 million.

Benefits: Notifying individuals of a breach of their personal health information as close in time to the breach can benefit the individuals directly affected, as well as other entities such as credit card companies and credit agencies. We found little information showing the monetary benefits of medical data notification, but one study[14] presents evidence to show that the sooner affected individuals learn of their personal financial information being compromised, the lower the risk of financial loss to the individual.

We did not find any information regarding the benefits of notification of breached medical information. However, early notification of the breach of sensitive medical information may help an affected individual mitigate the embarrassment that exposure of sensitive medical information may cause. Notification may permit an individual to intervene sooner rather than later to forestall the harmful effects of damaging information. As suggested above, perhaps the greatest benefit of improved data security accrues to the HIPAA entity. We believe the cost of notifying affected individuals and loss of business that may result from a breach of protected health information provide strong incentives for the entity to improve its data security so as to prevent future breaches.

2. Costs

In this analysis we rely entirely on historical data from 2008 for estimating the costs of the interim final rule. We could have attempted to project future costs but two factors argued against such an effort. First, the DataLossdb dataset provides only four years of reasonably good data going back to 2005. Although, in theory, we could use the four data points to establish a trend, it is not clear whether the trend presented for the four

[14] "Toward a Rational Personal Data Breach Notification Regime," by Michael Turner: Information Policy Institute, June, 2006.

years represents a trend in the number of breaches reported, or a trend in the reporting of breaches. In the first instance, the growth in data breaches would be the result of a real growth in the number of breaches. If this were the case, we would have confidence that the data represented a real trend. In the latter case, however, the growth in the number of breaches may simply reflect a growth in the reporting of breaches rather than an actual growth in the number of breaches. Under these circumstances, projecting a future trend would lead us to erroneous conclusions. More likely, the changes we see from year to year are a combination of both phenomena, which still leaves us with the problem of discerning the real change in breaches from the growth in reporting breaches. Therefore, we decided to base our estimates on the latest and most complete year of data available.

The second factor is the Department's implementation of the ARRA provisions regarding health information and privacy. Implementation of incentive payments to health care providers and the issuance of health IT standards provided in the ARRA is likely to stimulate adoption of health IT systems; and with growth in IT adoption, one may expect the number of data breaches of protected health information to increase.

At the same time, the Department is taking steps to ensure greater protection of protected health information, for example, by promulgating this interim final rule along with the encryption guidance that the Department issued on April 17, 2009. In the event that protected health information is compromised, affected individuals will be notified of breaches.

As a result of the efforts to both stimulate growth in the adoption of health IT (and the implications that has for increased risk of data breaches) and the countervailing efforts to reduce the incidences of breaches by encrypting records, we believe that at the

present time there is no reasonable way to forecast the net effects of both the change in costs or number of breaches that are likely to occur. Nevertheless, to the extent that the rate of adoption of encryption technology out paces health IT adoption, we can predict fewer reportable breaches under this rule. Given the state of flux, however, we believe the most prudent analysis is to simply rely on the historical data at hand.

a. Affected Entities

Section 13402 of the Act applies to HIPAA covered entities that are health care providers, health plans, or clearinghouses and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information. Based on 2006 data from the Office of Advocacy, Small Business Administration there are 605,845 health care entities, 4,567 health insurance plans and third party administrators. The Centers for Medicare & Medicaid Services report 107,567 durable medical equipment and prosthetic suppliers, and the National Association of Chain Drug Stores reports 88,396 pharmacies. In addition, we estimate that each covered entity has contractual arrangements with three business associates as defined under our regulations at 45 CFR 160.103. It should be noted, however, that many of the same business associates contract or have arrangements with many different HIPAA covered entities. To the extent that this occurs, the total number of business associates will be overstated. Since we do not know the extent of duplication among business associates, we cannot estimate the number of business associates affected by this rule. However, we can estimate that approximately 0.9 million HIPAA covered entities will be subject to the interim final rule. Table 2 presents the number of HIPAA covered entities. However, as noted, only the number of HIPAA

covered entities is well established. It is possible the number of affected business associates could be small if a few firms contracted with many HIPAA entities. In any event, we need not speculate about this relationship as our cost estimate is not based on the number of affected entities. Instead, it is based on a unique database of breaches and affected individuals as described below.

Table 2. Number of HIPAA Covered Entities by NAICS Code[1]

NAICS CODE	PROVIDERS/SUPPLIERS	# OF ENTITIES
622	Hospitals (General Medical and Surgical, Psychiatric and Drug and Alcohol Treatment, Other Specialty)	4,060
623	Nursing Facilities (Nursing care facilities, Residential mental retardation, mental health and substance abuse facilities, Residential mental retardation facilities, Residential mental health and substance abuse facilities, Community care facilities for the elderly, Continuing care retirement communities)	34,400
6211-6213	Offices of MDs (DOs, Mental health, Dentists, Practitioners, PT, OT, ST, Audiologists)	419,286
6214	Outpatient Care Centers (Family Planning Centers, Outpatient Mental Health and Drug Abuse Centers, Other Outpatient Health Centers, HMO Medical Centers, Kidney Dialysis Centers, Freestanding Ambulatory Surgical and Emergency Centers, All Other Outpatient Care Centers)	13,962

6215	Medical Diagnostic, and Imaging Services	7,879
6216	Home Health Services	15,329
6219	Other Ambulatory Care Services (Ambulance and Other)	5,879
n/a	Durable Medical Equipment Supliers[2]	107,567
4611	Pharmacies[3]	88,396
524114	Heath Insurance Carriers	1,045
524292	Third Party Administrators	3,522

[1] Office of Advocacy, Small Business Administration http://www.sba.gov/advo/research/data.html

[2] Centers for Medicare and Medicaid Services

[3] The Chain Pharmacy Industry http://www.nacds.org/wmspage.cfm?parm1=507

Healthcare clearinghouses are also considered covered entities. In the final rule implementing the 5010 standard published in the Federal Register on January 16, 2009 (74 FR 3318), we estimated that 162 clearinghouses will be affected by the interim final rule.

b. How Many Breaches Will Require Notification?

(1) What is a Breach of Protected Health Information?

The interim final rule at § 164.402 defines a breach as an event that "compromises the security or privacy of the protected health information," which means that it poses a significant risk of financial, reputational, or other harm to the individual. Events such as hacking into a database to steal protected health information would clearly constitute a breach of protected health information. Other events, however, such as a hospital inadvertently posting protected health information on a web site, or the office staff mailing a medical report to the wrong patient, may constitute a breach. In the case

of posting information on a facility's web site or mailing the wrong report, the entity responsible for the inappropriate release of protected health information may not have to notify the affected person if the entity has determined (e.g., by performing a risk assessment) that the release of the protected health information will not result in financial, reputational, or other harm to the individual. For example, if a general hospital impermissibly posted protected health information on its web site that included only an individual's name and address, under paragraph (1) of the definition of "breach" at § 164.402(1), the facility may not have to notify affected individuals if it determines that only minimal or no harm could result from such an inadvertent posting. However, if the same information were posted on the web site of a drug rehabilitation facility, a reasonable person may conclude that the association of a person's name with the facility could cause damage to their reputation. In that case, the provider would be required to notify the affected individuals. Therefore, a covered entity may not assume that these types of breaches do not require notices to the affected individuals. The entity must undertake an analysis of the information that was improperly divulged and only after an investigation may it conclude that the information released poses no significant harm.

Contrasted with an event that clearly falls into the category of a data breach and, after investigation requires notice to affected individuals, paragraph (2) of the definition of "breach" at § 164.402 specifies three types of improper uses and disclosures of protected health information that are excluded from the definition of a breach. The first is unintentional access to protected health information in good faith in the course of performing one's job, and such access does not result in further impermissible use or disclosure. For example, a staff person receives and opens an e-mail from a nurse

containing protected health information about a patient that the nurse mistakenly sent to the staff person, realizes the e-mail is misdirected and then deletes it.

The second exclusion is an inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates. For example, a nurse calls a doctor who provides medical information on a patient in response to the inquiry. It turns out the information was for the wrong patient. Such an event would not be considered a breach under paragraph (2)(ii) of the definition of "breach" at § 164.402, provided the information received was not further used or disclosed in a manner not permitted by the Privacy Rule.

The third type of improper disclosure that is excluded from the definition of a "breach" is when protected health information is improperly disclosed, but the covered entity or business associate believes, in good faith, that the recipient of the unauthorized information would not be able to retain the information. For example, a nurse hands a patient a medical report, but quickly realizes that it was someone else's report and requests the return of the incorrect report. In this case, if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then providing the patient report to the wrong patient does not constitute a breach.

(2) How Many Breaches Occur and How Many Individuals Are Affected?

The sources for identifying the number of HIPAA covered entity breaches and the number of individuals is limited to State health agencies and one database maintained by a nonprofit organization. There is no national registry of data breaches that captures all

data breaches. Thus, we have to rely on the few sources available to us and accept that each source has specific limitations. Essentially, we examined three sources and methods for estimating the number of breaches and then attempted to apply them to the universe of HIPAA covered entities and their business associates.

On April 20, 2009, the FTC published a proposed rule that would implement § 13407 of ARRA (74 FR 17914) and that applies to entities that are not HIPAA covered entities but which may retain, accept, and process personal health information in the form of personal health records. Examples of the kind of entities to which the FTC rule applies are web-based organizations that will receive, store, and maintain an individual's health information for that individual. The FTC estimated there are 900 such entities.

To arrive at an estimate of the number of breaches per year that would occur to personal health records that these entities retain, the FTC examined a general database of breaches from 2002 to 2007. They identified 246 breaches occurring within the 5-year period for businesses. Averaging the number of breaches over the 5-year period equals 50 breaches per year. FTC next identified 418,713 retail businesses with revenues of $1 million or more per year. However, concerned that applying the annual number of breaches to so large a number would yield an unrealistically small number of breaches per entity, the FTC took one percent of the number of retail businesses (which equals 4,187 entities) on the assumption that only one percent of the industry had such weak security that they would be attractive targets for data breaches. The FTC then calculated the breach rate based on the smaller number. The resulting rate is 1.2 percent which when applied to the 900 entities the FTC identified as maintainers of personal health records, equals 11 breaches per year.

To estimate the number of affected individuals, the FTC used a survey by the Ponemon Institute, "National Survey on Data Security Breach Notification," 2005 to derive a percent of the number of individuals notified as a result of a breach. Using 11.6 percent and applying the value to an estimated 2 million individuals using the services of the 900 personal health record holders, the FTC estimated that 232,000 individuals will be notified each year of data breaches. We believe this methodology has little applicability to the HIPAA universe of covered entities.

We do not believe these estimates are appropriate for the purposes of this rule for several reasons. First, the HIPAA covered universe contains many more, but also much smaller, entities than the FTC web-based universe. Second, this rule exempts many small breaches from reporting requirements because they either fall under the exceptions to the definition of "breach" in the regulation or the entity determines that no harm will occur. Third, although we use historical data for our impact estimates, it is possible that the provisions of this rule that exempt from the notification requirements data encrypted pursuant to the Secretary's guidance may greatly reduce the future number of reportable breaches; and fourth, as the FTC itself states, their costs are over-estimated because they apply all cost factors to all estimated web-based breaches.

Because the interim final regulation specifies different levels of responses on the part of HIPAA covered entities when unsecured protected health information is breached, we had to determine the number of breaches occurring using the size categories contained in our interim final regulation. The regulation requires increasing levels of notification for breaches that affect fewer than ten individuals, 10 to 499 individuals and for breaches affecting more than 500 individuals.

Rather than follow the approach the FTC adopted we turned to the DataLoss database maintained by the Open Security Foundation at http://datalossdb.org/. The database identifies data breaches by type of business and the number of records or individuals affected. Because business associates also must comply with provisions of the interim final rule in addition to HIPAA covered entities, we looked at all entries that either were identified as a medical entity or identified medical information as being involved in the data breach. Table 3 is a summary of the findings from the database for the year 2008, categorized by the number of individuals affected by each breach. We chose 2008 because it is the latest year for which we have a full year of data.

Table 3. Number of Breaches by Number of Affected for 2008

		Year
Affected size	Data	2008
Unknown	Breaches	36
	Affected Individuals	-
10 to 499	Breaches	14
	Affected Individuals	1,772
500 or More*	Breaches	56
	Affected Individuals	2,887,032
Total Number of Breaches		107
Total Sum of Total Affected		2,888,804

* Data for 2008 is adjusted to remove one outlier breach of 2.2 million records

As Table 3 demonstrates, the number of breaches and the number affected individuals are substantially smaller than the numbers we would generate using the FTC approach: 2.9 million affected individuals and 106 breaches. There are nevertheless, shortcomings associated with the data displayed in the table. As discussed previously, the meaning of "Total Affected" is not clear. Without examining each table data entry, it is impossible to know precisely if the numbers in the cells represent individuals, records, or both. In looking at a small sample of the descriptive detail for actual database entries,

we found evidence for both individuals and records. We assume that in the cases where the number of records breached was reported, that the number corresponds roughly to the number of individuals—that each record represents an individual. Yet, because an individual may have more than one record in data that was improperly accessed, our estimate of the affected number of individuals may be overstated. We invite public comment on this point.

Another concern we have is the table does not show any affected individuals or records for the "under ten" grouping. Because "Unknown" in the database is blank, the default value is zero. However, it would be improper to assume that the actual value of the reported "Total Affected" was zero. There is evidence, on the other hand, that the "Total Affected" in this group is less than 500 based on information we were able to obtain from the California Department of Public Health. For the first six months of this year (the first year that California's law requiring notification of data breaches involving protected health information went into effect), of the 196 cases that have been examined to date, none of the cases has involved more than 499 affected individuals. We interpret this fact as pointing to the likelihood that the number of individuals or records affected where the number is unknown is likely to be less than 500 and a majority of cases may fall into the under ten category. Because of the gap in the data for breaches involving fewer than ten individuals, our estimate for this group may be understated. We invite public comment on this point.

The third limitation is the way information finds its way into the database. Since the database is privately maintained and operated and is not responsible to either a state or federal agency for regulating its content, the completeness and accuracy of information

posted on the web site is unknown. Generally, the information posted on the web site is gleaned from published sources or individuals with knowledge of the breaches submitting information. Nevertheless, we cannot be completely confident in the reliability of the information obtained from this source. Therefore, as is evident from the lack of affected records or individuals in the "under ten" grouping, it is highly likely that a certain number of breaches never reach the database, thus resulting in an undercount of the total number of breaches and the total number of individuals or records affected. We invite public comment on this point.

(3) Estimating the Costs

(a) Baseline

Approximately 45 States have laws that to varying degrees contain breach notification provisions similar to the Act. These 45 States require notification of individuals whose information was in some manner compromised as a result of inappropriate access to their information. Several States also link their requirements to federal notification requirements. Thus while all the States with breach laws require some form of notification to affected individuals, those States whose laws conform to the Federal requirements need only develop procedures to conform to their State laws in addition to the interim final rule. The entities in those States, thus, will have a small compliance burden compared to the entities in other states.

Because not all states have a notification requirement, in our estimation of the costs of the interim final rule, we will assume that no State has a notification requirement. Yet, clearly this would significantly overstate the burden imposed on HIPAA covered entities because HIPAA covered entities have trained their staffs and have prepared

procedures to follow when a breach occurs to comply with existing requirements of most of the states. To ameliorate the overstatement of our cost estimate somewhat, we will assume the costs for training personnel and for developing procedures have already been expended and are therefore in the baseline and we did not estimate these costs in our analysis. We invite public comment on these assumptions.

(b) Estimation of Costs

In its notice of proposed rulemaking, the FTC identified the cost elements that an entity will encounter when complying with the interim final rule. We examine the cost of notifying affected individuals by first class mail, issuing a substitute notice in major media or on a web site along with a toll-free phone number, notifying prominent media in the event of a breach involving 500 or more individuals, and notifying the Secretary of a breach, as well as the costs of investigating breaches.

Cost of notifying affected individuals by first class mail or e-mail

Section 164.404 requires all covered entities to notify an individual whose unsecured protected health information is believed to have been breached as defined in the interim final rule, either by first class mail, or if the individual has agreed, by e-mail. In its analysis, the FTC assumed that 90 percent of the notices to affected individuals will be e-mailed and only 10 percent will be sent by regular first class mail. Since the firms that the FTC is addressing are primarily web-based, assuming that the vast majority of communications would be conducted through e-mail is a reasonable assumption. For HIPAA covered entities, 90 percent of which are small businesses or nonprofit organizations, that engage the entire U.S. population in providing health care services, we believe that notification through e-mail will be much more limited than in the case of the

entities the FTC regulates. Most physicians appear concerned with the lack of confidentiality associated with e-mail use, and many older patients may be uncomfortable with and/or do not have access to e-mail. We, therefore, assume that only 50 percent of individuals affected as a result of a breach of unsecured protected health information will receive e-mail notices.

There will be certain costs that both e-mail and first-class mail communication will share. The cost of preparing the notice and preparing a draft will apply to both forms. The median hourly wage for a healthcare practitioner and technical worker in 2008 was $27.[15] Doubling the amount to account for fringe benefits equals $54. If we assume 30 minutes per breach for composing the letter, the cost equals $27. We assume that it will take 30 minutes per breach for an administrative assistant to draft the letter in either e-mail or printed formats and to document the letter to comply with §§ 164.414(a) and 164.530(j). The median hourly wage for office and administrative support staff is $14.32 per hour. Accounting for benefits, the hourly costs is $29. For the 30 minutes, we estimate $15 per breach. The combined cost for composing and preparing the document is approximately $42 per breach. Half of the cost will be allocated to the mailing of the first-class letter and the other half to the sending of e-mails.

Although computer costs for sending e-mail will be insignificant, it will take staff time to select the e-mail address from the entity's mailing list. We assume that a staff person could process and send 200 e-mails per hour at a cost of $30 per hour. For each mailed notice we assume $0.06 for paper and envelope and $0.44 for a first class stamp,

[15] Department of Labor, Occupational Employment Statistics; Healthcare Practitioner and Technical Occupations. http://www.bls.gov/oes/

totaling $0.50 per letter. We estimate another $30 per hour to prepare the mailing by hand at a rate of 100 letters per hour.

Using the data from Table 3 above for 2008 (the latest year for which we have a complete year of data), there were a total of 106 breach events reported including those of an unknown number of affected records or individuals. Multiplying the number of breaches by the cost of composing and drafting a notice (106 x $42) equals $4,346. Allocating half the costs to e-mailing and the same amount to regular mail yields $2,173 to each category.

For 2008, there were 2,888,804 reported affected individuals. Splitting this number evenly between e-mail and regular mail gives us 1,444,402 affected individuals for each notice category. For e-mails we divide affected individuals by the number of addressed envelopes processed in an hour (200) and multiply by the hourly cost of $30. To this number we add the $2,173 giving us an estimated cost for e-mail notices of $218,833.

We follow the same method for estimating the cost of mailing notices using postal mail plus the cost of postage and supplies. Dividing 100 letters per hour into 1,444,402 yields 14,444 hours which is then multiplied by $30 plus postage and supplies of plus the costs of composing and drafting equals $ 1,157,695. Summing the cost of e-mail and postal mail notices equals $1,376,528. Table 4 presents the results of our analysis. We invite public comment on this analysis and our assumptions.

Table 4. Cost of E-Mail and First Class Mail to Affected Individuals

	composing and drafting	breaches	composing and drafting costs	affected individuals or records	hours to prepare mailing	cost to prepare mailing	postage and supplies	Total

mail	21	106	$2,173	1,444,402	14,444	$433,321	$722,201	$1,157,695
e-mail	21	106	$2,173	1,444,402	7,222	$216,660		$218,833
Total			$4,346	2,888,804				**$1,376,528**

Cost of Substitute Notice

In the event that a HIPAA covered entity is not able to contact an affected individual through e-mail or postal mail, it must attempt to contact the person through some other means. If the number of individuals who cannot be reached through the mailings is less than ten, the entity may attempt to reach them by some other written means, or by telephone. We do not know how many breaches occurred with fewer than ten affected individuals and therefore cannot estimate a cost for contacting them. We believe, however, that the costs would be very small and as a result we have not attempted to estimate the costs of contacting them.

In the event that the covered entity is unable to contact 10 or more affected individuals through e-mail or postal mail, the interim final rule requires the entity to (1) publish a notice in the media (newspaper, television, or radio) containing the information contained in the mailed notice or post a notice on its web site, and (2) set up a toll-free number. The toll-free number is to be included in the public notice and web site.

Based on the cost for publishing a public notice in the two leading newspapers, in the Washington D.C. area, rates range between $2.91 and $15.23 per line. Based on these numbers, we estimate the cost of a public notice will cost between $80 and $400. Taking the mean of the range, we estimate an average price of $240 per notice. If we assume that a provider will publish two notices, the cost will be $480. Multiplying this

amount by the number of breaches reported in 2008 for the 10 to 499 and 500 or more groupings (70), yields $33,600.

It is conceivable that some breaches involving more than 10 but fewer than 500 individuals may require notices in several states or jurisdictions. The probability of this event occurring, however, we believe, is low and we did not attempt to estimate the costs of such an event.

If a HIPAA covered entity has a web site, we assume there will be no cost to post the notice to the web site.

The cost of setting up a toll-free phone number is a straight forward process of contacting any one of a number of service providers who offer toll-free service. In checking the internet, we found prices for toll-free service ranging from $0.027 per minute for a basic mail box arrangement to $0.07 per minute. Some require a monthly fee ranging from $10 to $15 per month. A major, national phone service company offers toll-free service for $15 per month per toll-free number and per minute charge of $0.07. There is a one-time charge of $15. For purposes of our analysis, we will use the costs of $15 per month plus $15 activation fee and $0.07 per minute.

Since the regulation requires providers to maintain a toll-free number for three months, the monthly charge plus initial fee per breach will be $60. To estimate the number of calls to the toll-free number we assumed that more individuals than those who did not receive a notice or who are not affected by the breach would call out of concern that their protected health information might have been compromised. The calls from individuals who are not affected will make up for the affected individuals who will not call the number either because they did not learn of the breach or are not concerned.

In its proposed rule, the FTC estimated that 5,000 people would call within the first month and then decline to an average of 1,000 calls per month. Since most HIPAA covered entities do not serve that many patients, we decided to use the mean number of affected individuals for each of the two groups, 10-499 and 500 or more affected individuals. For breaches with 10-499 affected individuals, the mean is 127 and for 500 or more, the mean equals 51,554 individuals. Since multiplying the mean times the number of breaches equals the total number of affected individuals, we assume that breaches affecting between 10 and 500 individuals will generate 1,772 calls. Similarly, for breaches affecting 500 or more individuals, we assume 2,887,032 calls. Assuming that a call averages five minutes at $0.07 per minute, we estimate the total cost for all calls to equal $1,011,084. Added to this is $4,200 that represents the monthly fee per breach (70 breaches) for three months plus the one-time fee (totaling $60 per breach). This brings the total cost of toll-free lines to $ 1,015,284.

To this cost, we must also include the office staff time to answer the incoming calls at $30 per hour. Based on an average of five minutes per call, a staff person could handle 12 calls per hour. Dividing 12 into 2,888,804 equals 240,734 hours and then multiplied by $30 equals $7,222,025. Summing all cost elements yields a total cost of $8,237,309.

To the degree that firms already maintain toll-free phone lines, our estimate overstates the costs of setting up a toll-free line as required under the rule.

Table 5 presents our cost analysis.

Table 5. Cost for Setting Up a Toll-Free Line for Three Months

Costs	Number of Breaches 11-499 (14)	Number of Breaches 500 + (56)	Number of Call 11-499 (1772)	Number of call 500 + (2,887,032)	Total
Monthly Charges for 3 months + 1-time Charge ($60/breach)	$840	$3,360			$4,200
Direct Calling Charges @ $.07/min x 5 minutes			$622	$1,010,461	$1,011,084
Labor cost @ $30/hr x 5 min per call			$4,445	$7,217,580	$7,222,025
Total	$840	$3,360	$5,067	$8,228,041	$8,237,309

In addition to the cost of the toll-free number and staff time answering calls, we also imputed a cost to the time individuals will spend calling the toll-free number. In estimating the time involved, we assumed that a person will spend five minutes per call. However, the person may not get through the first time and thus may have to call back a second time which could add another 5 minutes. Taking the average between 5 and 10 minutes, we used an average call time of 7.5 minutes.

For purposes of imputing cost to an individual's time, we took the mean compensation amount from the Bureau of Labor Statistics of $20.32 for all occupations at http://www.bls.gov/oes/current/oes_nat.htm. Dividing 60 by 7.5 minutes yields 8 calls per hour. Dividing the number of calls per hour into 2,888,804 calls and then multiplying by $20, gives us a cost of $ 7,222,010. We invite the public to comment on our analysis and assumptions.

Cost of Breaches Involving 500 or More Individuals

If a covered HIPAA entity experiences a data breach of protected health information affecting 500 or more individuals, §164.406 of the interim final rule requires

the entity to notify the media in the jurisdiction or State in which 500 or more individuals reside. Also, §164.408 requires the entity to submit a report to the Secretary at the same time it notifies the media. The covered entity must take these steps in addition to undertaking efforts to directly notify affected individuals by first-class mail or e-mail and through alternative means of notification if it cannot contact 10 or more individuals.

We anticipate that, when a covered entity must notify the media under the interim final rule, it will issue a press release. The tasks involved in issuing the press release will be the drafting of the statement and clearing it through the organization. We assume that drafting a one-page statement will contain essentially the same information provided in the notice to affected individuals and will take 1 hour of an equivalent to a GS-12 Federal employee, earning $29 per hour. Multiplying the amount by two to account for benefits equals $58. Approval of the release involves reading the document. We expect this activity to take 15 minutes. The average hourly rate for a public relations manager is approximately $49 in 2008. Doubling the amount for benefits equals $98. Rounding up to $100, one quarter of an hour equals $25 for approving the release. The total cost of the release equals $75, and multiplying this amount by the number of breaches affecting 500 or more individuals (56) equals $4,200. It should be noted that this amount may overstate the actual costs of issuing a notice to the media. The regulation requires a release only in the jurisdiction or State where 500 or more individuals are affected. As the example in the discussion of § 164.406 discussed above in Section IV illustrates, a breach may affect a total of 500 or more individuals but may affect fewer than 500 persons in each State or jurisdiction where the affected individuals reside. In that case,

the covered entity does not have to issue a notice to the media, but must take all the other steps required of a breach of that size.

There is the possibility that a breach may affect 500 or more individuals in several States or jurisdictions. In such situations, the covered entity has the choice of notifying the media in each of the several States or jurisdictions; or it may choose to notify the national media with the expectation that the local media in each jurisdiction will pick up the information. We expect the covered entity to select the most efficient means for informing the media.

The report to the Secretary of HHS that must be sent contemporaneously to the sending of the notices to the affected individuals will contain essentially the same information as the notice sent to the affected individuals: (a) information regarding the nature and cause of the data breach, (b) the number and contents of the records breached, (c) the number of individuals affected, (d) steps the entity took to notify affected individuals and the degree of success it had in reaching affected individuals, and (e) steps taken to improve data security.

We anticipate the time and cost to prepare the report will be the same as that required for issuing a notice to the media. The cost for reporting the 56 breaches affecting 500 or more individuals based on the 2008 data is $4,200.

Cost of Investigating a Breach

As a prerequisite to issuing a notice to individuals or to the media and the report to the Secretary when a breach occurs, the covered entity will need to conduct some form of investigation to determine the nature and cause of the breach. We anticipate that most breaches involving fewer than 500 records or individuals will be relatively easy to

investigate and may involve a day of investigation to determine the cause and the extent of the breach. An office manager's time at $50 per hour multiplied by 8 hours equals $400 and multiplied by the number of breaches affecting fewer than 500 individuals is $20,000. We note that this estimate includes the time required to produce the documentation required by § 164.414(a).

For breaches involving 500 or more individuals, the breach investigation may take considerably longer and involve significantly greater costs. The FTC, in its proposed rule (74 FR 17921 and footnote 27) estimated 100 hours at a cost of $4,652. We accept this cost for investigating a breach as an upper bound, but we expect that the average investigation will take half the time and cost approximately $2,300. Based on the Ponemon report cited above, the most frequent cause for data breaches was a lost laptop computer accounting for 35 percent of all data breaches. While system failure was the second most frequently cited cause of data breaches accounting for 33 percent, the combined loss of laptops and other data bearing equipment accounted for almost 50 percent of data losses. For these reasons, we believe that estimating the average time and cost for breach investigation as being half the amount FTC estimated is a reasonable assumption. Multiplying our cost estimate by the number of breaches of 500 or more individuals protected health information yields us $128,800.

Cost of Submitting the Annual Breach Summary to HHS

Under § 464.408, covered entities must maintain a log of all breach events. Once per year a covered entity that has experienced a breach must submit a summary of its log to the Department. Since the material for the submission has already been gathered and organized for the issuance of the notices to the affected individuals, we expect submitting

the log summary to the Department will require at most an hour of office staff time once per year. At $30 per hour multiplied by the total number of breaches reported for 2008 (106) equals $3,180.

3. Benefits

We were not able to identify any studies that pointed to quantitative benefits arising from the notification of health data breaches. On an intuitive level, however, it seems that notifying affected individuals of compromises to their protected health information would help in two ways. It would alert them to the possibility of identity theft resulting from the exposure of identifiers such as credit card numbers, date of birth, and social security numbers associated with the individual's name. The other benefit of notification is enabling an affected individual to mitigate harm to his or her personal reputation that may result from the exposure of sensitive medical information.

With respect to the mitigation of financial loss, in the study cited previously[16] Turner presents evidence suggesting that 69 percent of individuals who were able to take action within 6 months of the breach to their financial information to mitigate damages suffered no out-of-pocket expenses. This compares to 40 percent who took action after 6 months. In cases where affected individuals who were able to take action within 5 months of the breach such as monitor their credit card statement and notify credit bureaus, the value of the fraud exceeded $5,000 only in 11 percent of the cases. For those who did not take steps to mitigate the damage for 6 months or longer, the amount of fraud exceeded $5,000 in 44 percent of the cases. From this evidence, it appears that there are some tangible benefits to notifying individuals as soon as possible after a breach of protected health information occurs. We did not, however, find a clear connection

[16] "Towards A Rational Breach Notification Regime" by Michael Turner; Information Policy Institute.

between the breach of protected health information and the amount of financial loss or its frequency.

The harm to a person's reputation or standing in the community resulting from the release of protected health information could be substantial and could have financial and economic consequences. We lack data on the frequency and extent of damages from the inappropriate release of sensitive medical information. Notifying a person of unauthorized access can, however, enable a person to take measures to reduce the damage. Notification can enable them to prepare psychologically and take actions to prepare for the consequences. The individual also may take steps to prepare others for the possible consequences.

Benefits to the HIPAA covered entity will rest with the actions it takes to prevent data breaches. As our analysis demonstrates, the costs of notification for an entity may be significant, although in the aggregate in terms of overall health care costs, they are extremely small. Nevertheless, we believe that the costs of the interim final rule are avoidable if either before a covered entity experiences a breach or following one, the entity adopts measures to strengthen its data security. As pointed out, the most frequent form of data loss is the result of lost or stolen laptops and data bearing media such as hard drives. If the data on these devices is encrypted, then under the interim final rule definition of a breach, the event would not require the covered entity or the business associate to notify affected individuals.

Because much of the harm resulting from breaches of protected health information may come from the pain and suffering individuals' may sustain to their reputations and standing in their communities, the benefits that reductions in the number

of breaches and number of individuals affected is hard to quantify while the costs of the rule are identifiable and specific. For these reasons, we are unable to estimate the net benefits of the rule. Yet we believe by providing an incentive to reduce the number of breaches of unsecured protected health information, the rule will help increase confidence among members of the public in the security of their protected health information. To whatever extent greater trust can be fostered between patients and health care providers, the better the communication and the higher the quality of health care delivered.

D. Regulatory Flexibility Analysis

The RFA requires agencies to analyze options for regulatory relief of small businesses if a rule has a significant impact on a substantial number of small entities. We are implementing this interim final rule as required by section 13402 of P.L. 111-5. The objective of the rule is to establish uniform requirements for HIPAA covered entities and their business associates to notify individuals whose unsecured protected health information may have been improperly accessed or used.

In Table 2 above, we identified the type and number of HIPAA covered entities to which the interim regulation applies. For purposes of our regulatory flexibility analysis, it is our practice to assume that all health care providers and suppliers meet the definition of a small entity. Ninety percent of small entities either meet the Small Business Administration size standard for a small business or are nonprofit organizations. Approximately 71 percent of health insurance carriers and third party administrators meet the SBA's small business size standard. Although we do not have separate revenue data for health insurance carriers and third party administrators, we believe that the majority

of the third party administrators meet the SBA standard. Approximately 22 percent of pharmacies meet the SBA standard for a small business.

Based on the analysis of data breaches for 2008, we do not expect the interim final rule to have a significant impact on a substantial number of small entities. We estimate that the average cost per breach will cost $160.616. Second, the rule will apply to entities that, in many instances, already have obligations to provide notification of data breaches under most State laws covering medical breaches. Therefore, the Secretary certifies that the rule will not have a significant impact on a substantial number of small entities.

VI. Paperwork Reduction Act Information Collection

In compliance with the requirement of section 3506(c)(2)(A) of the Paperwork Reduction Act of 1995, the Office of the Secretary (OS), Department of Health and Human Services, is publishing the following summary of a proposed information collection request for public comment.

Because this rule will go into effect 30 days following publication, we have submitted a request to OMB for review of these information collection requirements on an emergency basis, pursuant to 5 CFR 1320.13. We are providing an abbreviated comment period of 14 days. Interested persons are invited to send comments by [INSERT DATE 14 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] regarding this burden estimate or any other aspect of this collection of information, including any of the following subjects: (1) The necessity and utility of the proposed information collection for the proper performance of the agency's functions; (2) the accuracy of the estimated burden; (3) ways to enhance the quality, utility, and clarity of

the information to be collected; and (4) the use of automated collection techniques or other forms of information technology to minimize the information collection burden.

To comment on this collection of information or to obtain copies of the supporting statement and any related forms for the proposed paperwork collections referenced above, e-mail your comment or request, including your address and phone number to Sherette.funncoleman@hhs.gov, or call the Reports Clearance Office on (202) 690-6162. Written comments and recommendations for the proposed information collections must be directed to the OS Paperwork Clearance Officer at the above email address within 14 days.

Abstract: 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) requires the Office for Civil Rights to collect information regarding breaches discovered by covered entities and their business associates. ARRA was enacted on February 17, 2009. The HITECH Act (the Act) at §13402 requires the Department of Health and Human Services (HHS) to issue interim final regulations within 180 days of enactment to require HIPAA covered entities and their business associates to notify affected individuals and the Secretary of breaches of unsecured protected health information. Section 164.404 of this interim final regulation requires HIPAA covered entities to notify affected individuals of a breach of their unsecured protected health information without reasonable delay and in any case within 60 days of discovery of the breach, and, in some cases, to notify the media of such breaches pursuant to § 164.406. Section 164.408 requires covered entities to provide the Secretary with immediate notice of all breaches of unsecured protected health

information involving more than 500 individuals. Additionally, the Act requires covered entities to provide the Secretary with an annual log of all breaches of unsecured protected health information that involve less than 500 individuals. Finally, covered entities must maintain appropriate documentation under § 164.530(j) to comply with their burden of proof under § 164.414.

The estimated annualized burden table below was developed using the same estimates and workload assumptions in the impact statement in section V, above.

Estimated Annualized Burden Table

Type of Respondent	Number of Respondents	Average Number of Responses per Respondent	Average Burden Hours per Response	Total Burden Hours
Individual Notice—Written and E-mail Notice (investigation; drafting, preparing, and documenting notification; and sending notification)	**106**	**27,253**	**1/60**	**48,147**
Individual Notice—Substitute Notice (posting or publishing notice and toll-free number)	**70**	**1**	**668**	**46,760**
Media Notice	**56**	**1**	**1**	**56**
Notice to Secretary (Notice for breaches affecting 500 or more individuals and annual notice)	**106**	**1**	**22/60**	**39**
TOTAL				**95,002**

LIST OF SUBJECTS

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Investigations, Medicaid, Medical research, Medicare, Penalties, Privacy, Reporting and recordkeeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Reporting and recordkeeping requirements, Security.

For the reasons set forth in the preamble, the Department proposes to revise 45 CFR subtitle A, subchapter C, parts 160 and 164, as follows:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

1. The authority citation for part 160 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-8; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(note)); 5 U.S.C. 552; and secs.13400 and 13402, Pub. L. 111-5, 123 Stat. 258-263.

2. Revise §160.101 to read as follows:

§160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171 through 1179 of the Social Security Act (the Act), as added by section 262 of Public Law 104-191, section 264 of Public Law 104-191, and section 13402 of Public Law 111-5.

3. In §160.202, revise the second paragraph of the definition "Contrary" to read as follows:

§160.202 Definitions.

* * * * *

Contrary * * *

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Pub. L. 104-191, or section 13402 of Pub. L. 111-5, as applicable.

* * * * *

4. In §160.534 add paragraph (b)(1)(iv), and revise (b)(2) to read as follows:

§160.534 The hearing.

* * * * *

(b)(1) * * *

(iv) Compliance with subpart D of part 164, as provided under §164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

* * * * *

PART 164—SECURITY AND PRIVACY

5. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d-1320d-8; sec. 264, Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320-2(note)); secs. 13400 and 13402, Pub. L. 111-5, 123 Stat. 258-263.

6. Revise § 164.102 to read as follows:

§164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and section 13402 of Public Law 111-5.

7. In §164.103, add in alphabetical order the definition of "Law enforcement official" to read as follows:

§ 164.103 Definitions.

* * * * *

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

* * * * *

8. In §164.304, revise the definition of "Access" to read as follows:

§ 164.304 Definitions.

* * * * *

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.)

* * * * *

9. Add a new subpart D to part 164 to read as follows:

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

Sec.

164.400 Applicability.

164.402 Definitions.

164.404 Notification to individuals.

164.406 Notification to the media.

164.408 Notification to the Secretary.

164.410 Notification by a business associate.

164.412 Law enforcement delay.

164.414 Administrative requirements and burden of proof.

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

Authority: secs. 13400 and 13402, Pub. L. 111-5, 123 Stat. 258-263.

§ 164.400 Applicability.

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

§ 164.402 Definitions.

As used in this subpart, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

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

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information 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 not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information 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.

Unsecured protected health information 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 under section 13402(h)(2) of Pub. L. 111-5 on the HHS web site.

§ 164.404 Notification to individuals.

(a) *Standard*-(1) *General rule.* A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), 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 (determined in accordance with the federal common law of agency).

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) *Elements.* The notification required by paragraph (a) of this section shall include, to the extent possible:

(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 protected health information that were 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 toll-free telephone number, an e-mail address, Web site, or postal address.

(2) *Plain language requirement.* The notification required by paragraph (a) of this section shall be written in plain language.

(d) *Implementation specifications: Methods of individual notification.* The notification required by paragraph (a) of this section shall be provided in the following form:

(1) *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. The notification may be provided in one or more mailings as information is available.

(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 (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) *Substitute notice.* In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information 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 there is insufficient or out-of-date contact information 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 where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) *Additional notice in urgent situations.* In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

§ 164.406 Notification to the media.

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in §164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.

(b) *Implementation specification: Timeliness of notification.* Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

§ 164.408 Notification to the Secretary.

(a) *Standard.* A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) *Implementation specifications: Breaches involving 500 or more individuals.* For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.

(c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a 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 the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS web site.

§ 164.410 Notification by a business associate.

(a) *Standard.* (1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (1) of this section, 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 (determined in accordance with the federal common law of agency).

(b) *Implementation specifications: Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

§ 164.412 Law enforcement delay.

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

§ 164.414 Administrative requirements and burden of proof.

(a) *Administrative requirements.* A covered entity is required to comply with the administrative requirements of §§ 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) *Burden of proof.* In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

§ 164.501 [Amended]

10. In §164.501, remove the definition “Law enforcement official.”

11. In §164.530, revise paragraphs (b)(1), (b)(2)(i)(C), (d)(1), the first sentence of paragraph (e)(1), (g)(1), (h), the first sentence of paragraph (i)(1), (i)(2)(i) and add paragraph (j)(1)(iv) to read as follows:

§164.530 Administrative requirements.

* * * * *

(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2)*** (i) * * *

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

* * * * *

(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

* * * * *

(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies

and procedures of the covered entity or the requirements of this subpart or subpart D of this part.* * *

* * * * *

(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

* * * * *

(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under §160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. * * *

(2) Standard: Changes to policies and procedures.

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

* * * * *

(j)(1) ***

(iv) Maintain documentation sufficient to meet its burden of proof under §164.414(b).

* * * * *

Dated: August 6, 2009

Kathleen Sebelius,

Secretary

[FR Doc. 2009-20169 Filed 08/19/2009 at 4:15 pm; Publication Date: 08/24/2009]