WEDI Strategic National Implementation Process (SNIP)
Privacy and Security Workgroup

Breach Risk Assessment Issue Brief

Breach Notification Decision Process

1/1/2014

Workgroup for Electronic Data Interchange
1984 Isaac Newton Square, Suite 304, Reston, VA. 20190
T: 202-684-7794//F: 202-318-4812

CONTENT

I. Introduction

The Final HIPAA Omnibus Rule updates the Breach Notification decision process by introducing several new concepts or requirements including:

- A Breach is presumed to have occurred when first discovered. It is up to the covered entity or business associate to demonstrate a low probability that PHI has been compromised.
- A new four-factor risk assessment must be used to establish the probability that PHI has been compromised; all four factors must be considered and documented unless the covered entity proceeds directly to the appropriate notification of individuals and HHS.
- Notification requirements remain the same as established in the Interim Final Breach Notification Rule.

II. Purpose of this Issue Brief

The following decision process can be used to guide efforts in establishing probability and requirements for notification. This is based on the Breach discovery:

1. Is the data "protected health information" ("PHI")? (See 45 C.F.R. 160.103)

If the data is not PHI, stop here. No further action is needed from a HIPAA Breach Notification standpoint.

2. Is the data "unsecured PHI"? (See 45 C.F.R. 164.402) PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in HHS' guidance? (Guidance published: 74 Federal Register, Pages 4270, 42742) NOTE: This applies to electronic and hard copy PHI.

If your review determines with complete assurance the PHI is secured (for example a laptop was lost or stolen that had data encryption enabled and there is no evidence the encryption key has been compromised), and you can document that the method for securing the PHI was enabled as of the breach, you can stop here. Document your review and the finding that the breach did not involve "unsecured PHI". Document any remedial actions such as training or revision of policy and procedure to reduce the likelihood of another possible breach from reoccurring.
If not, proceed to the next steps.

3. Determine and document whether the incident falls under one of the exceptions of the breach definition:

a. Unintentional access to PHI in good faith in the course of performing one's job and such access does not result in further impermissible use or disclosure.
b. Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate or affiliated organized health care arrangement (OHCA).
c. When PHI 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.

If the disclosure falls into one of these exceptions, notification is not necessary. You can stop at this point. It is suggested you review the pre-amble of the Interim Final Rule for further examples of the above exceptions. Be certain you have adequately documented the exception determination!

If the disclosure does not fall into one of these exceptions, proceed to the next step.

Note: If your organization decides to proceed immediately to notification, the four-factor risk assessment is not necessary. Document your actions for notification, and conduct the appropriate follow up remedial actions described below.

III. Documentation

A completed risk assessment is necessary after discovering a breach of unsecured protected health information (PHI). To determine probability of a compromise to the PHI and whether breach notification is required, the HIPAA Breach Notification Rule requires consideration of <u>at least four factors</u>:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

a. Identifying financial and demographic data: Social Security number, credit cards, financial data
b. Clinical data: Diagnosis, treatment, medications
c. Behavioral health, substance abuse, sexually transmitted diseases

2. The unauthorized person who used the PHI or to whom the PHI was disclosed.

a. Does the person have obligations to protect privacy and security?
b. Does the person have the ability to re-identify the PHI?

3. **Whether the PHI was actually viewed or accessed.**
    a. For example, was a stolen laptop later recovered and IT analysis found that PHI was never accessed, viewed, transferred or otherwise compromised, although opportunity existed?

4. **The extent to which the risk to the PHI has been mitigated.**
    a. Can the person who received the PHI provide satisfactory assurances that the PHI will not be further used or disclosed or that it will be destroyed?
    b. What level of effort has been expended to prevent future related issues and or to lessen the harm of the actual breach?

IV. Next Steps

Work with your legal counsel/risk management team per your Risk Analysis/Risk Management internal protocols to confirm the probability the PHI has been compromised and if such probability requires notification.

6. **Can it be concluded that there is a low probability that the information has been compromised?** If so, notification is not necessary. Complete your documentation and retain for future reference or investigations.

For a medium or high finding that data has been compromised, work with legal counsel/risk management team/Privacy/Security Officers to complete the appropriate notification steps for each individual affected. These should be thoroughly documented in your organization's Breach Reporting/Notification Policy and Procedure.

V. Remedial Steps

Remediation must be considered even for a low probability breach determination-as any breach discovery is also a HIPAA security incident that requires response and reporting.

- **Is there a system or procedure in place for discovery of breaches? Does this apply to both covered entity and their business associates?**

- **Has the entire workforce been trained in the need for prompt reporting of privacy and security breaches? Are meaningful sanctions or consequences applied for untimely reporting of breaches? Is documentation maintained of the training and the sanctions?**

- **Is there a procedure in place to remediate the cause of the breach, if possible and demonstrate that it is not likely to re-occur?**

WEDI Note: As a best practices Project Management step, it is recommended that you conduct a post review. Use the opportunity to gather those who

participated in the breach assessment and determine if processes should be revised to make the overall identification, reporting and assessment more efficient for future issues.

VI. Acknowledgements

The Breach Risk Assessment Brief provides an overview of the changes as part of the Final Rule for Breach Notification and is meant to help organizations develop their internal plans for how their organization will follow specific protocols in the event of a breach situation. It is recommended that each organization consult published guidance from the U.S. Department of Health and Human Services and/or obtain additional consultation or legal guidance to make a final determination of what their federal/state (if applicable) compliance posture should be relating to Breach review and notification.

RESOURCES: Health and Human Services, Office for Civil Rights, Breach Notification: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Breach - The term ‘‘breach’’ means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (HITECH Act, Section 13400, Public Law 111–5, Feb. 17, 2009.) Regulations: “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. (45 C.F.R. 164.402)

We would like to acknowledge the work of the WEDI co-chairs of the Privacy and Security Workgroup to produce this document: Mark Cone; Lesley Berkeyheiser; David Ginsberg; and Joe McClure, Esq.; as well as Ruth Anne Carr, J.D. while participating as Chair of the Breach Notification Sub-workgroup.

Disclaimer

Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the WEDI Strategic National Implementation Process (WEDI SNIP).

Document is for Education and Awareness Use Only