TIC International Corporation
Benefit Administrators and Consultants

2015-04

February 6, 2015

CLIENT BULLETIN

The "Hack" at Anthem and the HIPAA Privacy Rules on Breach Notification

In light of the recent breach of information at Anthem, the following information is provided concerning the *HIPAA Privacy Rules* (("Privacy Rules") on reporting a breach. The data breached appears to be the personal identifiers that would be in "enrollment data", which is considered Protected Health Information (PHI). See 2002 *Privacy Rule Preamble* at 67 FR 53182, 53207-08. **We are not declaring this to be a HIPAA Privacy Rule Breach, but will provide information applicable as if it were such a breach.**

THIS BULLETIN IS NOT "LEGAL" ADVICE AND HEALTH PLANS WHOSE INFORMATION HAS OR MAY HAVE BEEN AFFECTED BY THE DATA BREACH AT ANTHEM ARE ADVISED TO SEEK LEGAL COUNSEL ON THE PROPER COURSE OF ACTION UNDER THE PRIVACY RULE OR STATE LAW.

In this newsletter, the "covered entity" is the group health plan, which includes multiemployer group health plans. Anthem would generally be a "business associate" to health plans for which it processes claims and provides other administrative services which use PHI, but Anthem could be a covered entity also. Business Associates must inform covered entities of breaches.

In this case, for self-funded plans that use Anthem as a business associate to process claims, etc., while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Plans should review their business associate contracts to see which party has the duty of providing the notice to individuals, as well as any notices that are required to be given to the media and reporting the breach to the Secretary Health and Human Services (HHS). Hereinafter, the Secretary of HHS will be referred to as "the Secretary."

Even if a plan's business associate contract has delegated the duty to make the required breach notifications to Anthem, plan administrators may wish to consult Fund Counsel on whether the Fund may wish to voluntarily provide breach notifications to its members, as well as reporting the matter to the media and the Secretary. In addition to any Privacy Rule breach notification rules, there may be

Prepared for TIC by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

state laws concerning the breach of PHI or breaches concerning Social Security Numbers that may apply. Plans should consult their Fund Counsel for advice on the affect of state breach notice laws. Information on state breach laws can be found at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Information Available From Anthem

Anthem has created a website – www.anthemfacts.com, and a hotline, 1-877-263-7995, for its members to call for more information. Anthem has also posted some Frequently Asked Questions (FAQs) on the breach http://www.anthemfacts.com/faq. Anthem's website states that *Anthem will notify individuals whose information has been accessed and provide credit monitoring and identity protection services free of charge*. Individuals may also contact the three major credit reporting firms and have a fraud alert placed on their report which will provide alerts if someone tries to open accounts in a person's name. The three major credit reporting firms are: Experian, (888) 397-3742; Equifax, (800) 685-1111; and, TransUnion, (800) 888-4213.

Before discussing the *HIPAA Breach Notification Requirements*, it is helpful to recall how protected health information (PHI) is defined, as well as how a "breach" of PHI is defined and the corresponding "notice" duties of "covered entities" and "business associates" if a "breach" occurs.

What is PHI?

The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). Enrollment data is considered PHI.

In essence, the *Privacy Rules* say the unauthorized access of PHI in a manner not permitted by the *Privacy Rules* which compromises the security or privacy of the PHI is **presumed to be a breach unless** the covered entity demonstrates that

there is a **low probability** that the PHI has been compromised **based on a risk assessment of at least the following factors:**

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The *extent to which the risk to the protected health information* has been mitigated.

(*emphasis added*)

Breach Notification Requirements

Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Covered entities include multiemployer group health plans.

Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.

The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate.

Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like the individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary of HHS

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of the breaches of unsecured PHI. Covered entities will notify the Secretary by visiting the HHS web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) by filling out and electronically submitting a breach report form.

If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

Notification to Covered Entity by a Business Associate

If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

Administrative Requirements and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of "breach."

* * *