GROOM LAW GROUP CHARTERED

BENEFITS BRIEF

February 6, 2015 www.groom.com

Authors: Sravya Boppana, Mark Nielsen, Vivian Hunter Turner, Christy Tinnes

If you have questions, please contact your regular Groom attorney or one of the attorneys listed below:

Sravya Boppana
sboppana@groom.com
(202) 861-6338

Jon W. Breyfogle
jbreyfogle@groom.com
(202) 861-6641

Thomas F. Fitzgerald
tfitzgerald@groom.com
(202) 861-6617

Tamara S. Killion
tkillion@groom.com
(202) 861-6328

Christine L. Keller
ckeller@groom.com
(202) 861-9371

Mark C. Nielsen
mnielsen@groom.com
(202) 861-5429

Seth T. Perretta
sperretta@groom.com
(202) 861-6335

Christy A. Tinnes
ctinnes@groom.com
(202) 861-6603

Vivian Hunter Turner
vturner@groom.com
(202) 861-6324

Allison Ullman
aullman@groom.com
(202) 861-6336

Health Data Breach: What HIPAA Requires

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted by Congress to protect the security and ensure confidentiality of health information. Over the last five years, there have been several alleged breaches of health care information potentially affecting millions of individuals that have been reported by major news outlets, including recent reports involving Anthem.

Depending on the nature of the data affected, a breach of health information may require health plans to take certain actions, including notifying affected individuals, and potentially, the Department of Health and Human Services ("HHS") and the media.

The article below generally describes HIPAA obligations and sets forth some considerations for employer plan sponsors when faced with potential a breach of health information.

Background

HIPAA protects the security and confidentiality of health data by imposing obligations on covered entities[1], such as health plans (including self-insured group health plans). In their role as covered entities, health plans must comply with HIPAA's requirements to ensure that health information remains secure and, if health information is breached, follow certain breach protocols set forth under HIPAA.

In reality, access to health information is not always limited to the health plan itself. To assist with business functions, health plans contract with other entities such as third party administrators (who process claims and make available networks of providers) ("TPAs"), law firms, consultants, and actuarial firms. Depending on the nature of services they provide, these other entities may have access to health information that is protected under HIPAA, known as Protected Health Information ("PHI"). To ensure that PHI is protected, HIPAA requires that health plans enter into business associate agreements with service providers that may have access to PHI. Business associate agreements generally provide that the business associate will comply with the requirements of HIPAA and require the business associate to impose the same compliance obligations on any sub-contractor that the business associate may engage to help with plan-related activities.

Breach

As noted above, HIPAA requires covered entities to comply with its requirements – including privacy and security rules. As such, if there is a breach in violation of HIPAA, the covered entity (*e.g*, an employer-sponsored self-insured health plan) is responsible for compliance

[1] Health care providers, health plans, and health care clearing houses are covered entities under HIPAA.

with HIPAA's security breach rules. This is the case regardless of whether the breach is by the health plan itself (the covered entity) or by one of its business associates. Similarly, depending on the nature and impact of the breach, HIPAA may require the covered entity to provide certain notifications of the breach to affected individuals and HHS. Again, the health plan (as the covered entity) is responsible for this reporting regardless of whether the breach is by the covered entity or its business associate.

As the covered entity would not otherwise know whether a breach has occurred at the business associate level, HIPAA requires that a business associate notify the covered entity of potential breaches within 60 days of discovery. The covered entity is then responsible for any subsequent reporting, as described in the next section.

Though HIPAA places the responsibility following a breach upon covered entities, there is nothing in HIPAA precluding covered entities from stating in the business associate agreement who is responsible for making a breach determination, or delegating applicable reporting obligations to their business associates. Indeed, through the business associate agreement, covered entities and business associates frequently address which party is responsible for costs of reporting, notification, and/or providing any additional protections (*e.g.*, credit monitoring).

For example, a health plan could enter into a business associate agreement that allocates responsibility to the TPA to determine whether a breach has occurred and to perform required reporting of the breach. However, if the TPA does not comply with its obligations, then, under HIPAA, the health plan would be ultimately liable.

Reporting

A breach is a "reportable breach" under HIPAA if there is 1) an acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA's privacy and security rules that 2) has compromised the security or privacy of such PHI. If a breach meets these requirements, a covered entity must report the breach to the individuals affected (as well as HHS and the media, if applicable) unless the covered entity can demonstrate that there is a low probability that PHI has been compromised. HIPAA requires that the determination of a reportable breach include consideration of:

1. The nature and extent of PHI involved;
2. The unauthorized person who used the PHI or to whom disclosure was made;
3. Whether PHI was actually acquired or viewed; and
4. The extent to which risk has been mitigated.

A covered entity must document its findings in a risk assessment, even if it determines that a reportable breach has not occurred. And if there is a reportable breach, then the covered entity must:

- **Notify the individuals whose PHI is at issue** no later than 60 days of after discovery of the breach. The HIPAA security breach regulations include specific content for this notification.
- **Notify HHS** within 60 days of discovery if the breach involves 500 or more people. If the breach involves less than 500 people, the covered entity must record the incident on its breach log and file the log with HHS annually by March 1st.
- **Notify the media** if the breach involves more than 500 residents in a state.

GROOM
LAW GROUP
CHARTERED

High Level Takeaways for Health Plans

In the event of a reported breach by a business associate, the health plan should take steps to determine if the plan itself may have liability or exposure as a result of the breach.

As a best practice, health plans could prepare a checklist of steps to take in the event of a breach, including documenting that the relevant notifications are being provided by the health plan or the business associate and monitoring the ongoing activities and remediation steps of the business associate that caused the breach.