PARKER SMITH & FEEK
An IMA Company

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

# HIPAA Breach Notifications: Group Health Plans

There has been a prevalence of cyberattacks and data breaches on health plan-related companies recently, and we expect more of these in the future. When a HIPAA breach occurs in relation to an employer's group health plan, HIPAA breach rules must be followed.

This article expands on the employer's role once it has been notified of a HIPAA breach by its insurer/carrier, business associates (i.e., TPA), or other health plan partner.

Under HIPAA regulations, an employer's group health plan is a covered entity required to follow HIPAA breach notification rules. However, an employer is not required to duplicate the efforts of other covered entities or business associates.

## WHAT DO EMPLOYERS NEED TO DO ONCE IT IS NOTIFIED OF A HIPAA BREACH?

It depends on whether the employer's plan is fully-insured or self-insured.

**Fully-insured plans** will not have any additional obligations because the carrier/insurer itself is also a covered entity required to follow the breach notification rules. The letter from the carrier/insurer to the employer should describe its findings and how it will notify the impacted members.

**Self-insured plans** have more responsibility as the sole covered entity and plan sponsor. However, some large health plan vendors may handle the majority or all of the responsibility of a HIPAA breach.

*continued >*

## WHAT SHOULD A SELF-INSURED PLAN SPONSOR DO ONCE IT HAS BEEN NOTIFIED OF A DATA BREACH?

First, determine if the vendor will handle any of the HIPAA breach responsibilities on behalf of the group health plan.

Many large vendors who experience a breach will send a communication to the employer describing what happened and what steps they've taken to mitigate the damage. They will either automatically notify or offer to notify the affected individuals, with or without an offer of identity theft protection, and in a lot of cases, will also offer to notify the required government agencies.

If the employer is satisfied that the vendor's response fulfills the breach notification rules, the employer is not required to take any additional steps, although, they are free to communicate information regarding the breach to their employees themselves if they so choose.

In any event, the plan sponsor should keep records of due diligence by documenting the data breach notification, and the findings below and assess whether there is ongoing risk in doing business with the health plan vendor.

**This assessment would include the following:**

+ Did the vendor conduct a thorough investigation into the breach to identify the cause?
+ Did the vendor take appropriate steps to mitigate the harm caused by the breach (providing additional training to staffing, implementing stronger security measures)

Note: the notification from the vendor to the Plan may include this information.

If the vendor won't handle the HIPAA breach responsibilities, the self-insured plan sponsor must take action.

The primary responsibilities of the self-insured plan sponsor after notification of a HIPAA breach from one of its health plan partners include ensuring the following is determined:

+ Whether there was unauthorized acquisition, access, use or disclosure of protected health information (PHI);
+ Was the PHI that was accessed unsecured, i.e., not encrypted or otherwise unusable, unreadable, or indecipherable to unauthorized persons; and
+ Does the use or disclosure compromise the security or privacy of the PHI taking into account (a) the nature and extent of the PHI involved; (b) the unauthorized person who used the PHI or to whom the disclosure was made; (c) whether the PHI was actually acquired or viewed; and (d) the extent to which the risk to the PHI has been mitigated.

If there was a breach, then notice of the breach must be provided to affected individuals. In addition, notice must be provided to the media if more than 500 individuals' PHI was involved, and to the U.S. Department of Health and Human Services (HHS), either immediately if more than 500 individuals were involved or at the end of the year if less than 500 individuals were involved. States may also have their own breach notification requirements.

## DOES THE PLAN SPONSOR HAVE A FIDUCIARY DUTY SPECIFIC TO HIPAA BREACHES?

It's not specifically called out in the ERISA fiduciary rules, but there may be some overlap between HIPAA and ERISA responsibilities since ERISA fiduciary duties generally require broad compliance on behalf of the plan.

It seems plausible that not following the HIPAA breach notification rules could be a breach of fiduciary duty under ERISA. Further, continuing to use a vendor despite indications that their data is not secure could also constitute a breach of ERISA fiduciary duties.

If the nature of the breach indicates the vendor is not taking their HIPAA privacy obligations seriously, there may be a fiduciary obligation to terminate the relationship or take steps to ensure the vendor makes improvements.

## SUMMARY

Fully insured plans should save the breach notification from the carrier/insurer in their files as documentation. The notification should be thorough in documenting the cause of the breach, any mitigation efforts, and confirmation that a notification will be sent to impacted individuals.

Self-insured plans have more responsibility and should work with their vendor partners to ensure HIPAA breach rules are followed.

## AUTHOR

**MICHELLE CAMMAYO**
Compliance National Practice Lead
*michelle.cammayo@imacorp.com*