COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

PARKER | SMITH | FEEK

Q&A FROM ASSUREX GLOBAL WEBINAR

HIPAA PRIVACY AND SECURITY MISTAKES EMPLOYERS MAKE

FEBRUARY 28, 2019

Q. What is the standard for proper encryption? Where do you find that info?

A. There is no specific standard for encryption; however, HHS references certain encryption standards that, if implemented, will render ePHI "secure" for purposes of its breach reporting requirements. More information may be found here: https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

Q. Is it best to get a BA template from an employment attorney ?

A. As long as a Business Associate Agreement meets the required content specifications, it will be valid. For these purposes, the templates available online may be sufficient. But an employment attorney (or other advisor) may be helpful for ensuring that the discretionary provisions are tailored in a manner that is most beneficial to the employer.

Q. As you know, in today's world many self-insured plans bolting other services and vendors onto their health plan, such as cost transparency vendors, concierge/advocacy services, telehealth, data analytics vendors, etc. While these services are not specifically cited in a health plan document, do you feel these are services that should all still be subject to Business Associate Agreements and other HIPAA security requirements?

A. If any vendor is performing services related to the administration of the employer's health plan, and requires access to PHI in order to perform those services, then it would be considered a business associate, and a business associate agreement would be necessary.

Q. How often do you suggest Plan sponsors conduct a risk analysis?

A. In general, plan sponsors should conduct a risk assessment on a regular, periodic basis (e.g., every year or every three years). In addition, the risk analysis should be revisited and updated when there are operational, infrastructure, or regulatory changes that affect the content of the most recent risk analysis.

Q. Can you help us better understand what a "properly encrypted mobile device" is?

A. There is no single standard for encryption, but HHS generally recommends following NIST standards (https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html)

Q. Should the NPP be stand alone or included in an employee handbook?

A. The Notice of Privacy Practices must be individually delivered to the individual entitled to the notice. However, the covered entity may include the NPP with other written materials that are mailed to the individuals or the plan sponsor could include the notice with an SPD or with enrollment materials. The NPP can also be provided by email, if the recipient has agreed to receive an electronic notice and that agreement hasn't been withdrawn. However, if the covered entity knows that the email transmission to an individual has failed, it must provide a paper copy of the notice to the individual. (Remember that a reminder of the availability of the notice must also be issued at least once every 3 years!)

Q. If we have one health plan for Tribal Government & Casino's - should we have multiple Privacy Officer's or is one sufficient?

A. The regulations require designation of a single Privacy Official for a plan. However, the Privacy Official may delegate its duties. Therefore, if there are multiple entities participating in a plan, it may make sense to have delegates at each entity, who can carry out the day-to-day responsibilities of the Privacy Official at their respective locations.

Q. Is the wellness vendor a Business Associate?

A. If the wellness program is part of the employer's group health plan (e.g., if the incentive is tied to the health plan premium), or if the wellness program is itself a stand-alone health plan, then it would be subject to HIPAA, and a Business Associate Agreement would be needed with any vendors accessing individually identifiable information in connection with administration of the wellness program.

Q. As a Healthcare Provider, can we "piggyback" our EE healthplan BAA with our agency-wide BAA agreements for our email provider, shred company, etc.?

A. A health care provider is a covered entity. Separately, a health plan offered to a provider's employees is a covered entity. Each of these covered entities have separate obligations under HIPAA, and would each need to enter into Business Associate Agreements with their respective vendors. If a single BAA is used, then it should clearly identify both covered entities, and any differences in services provided/expectations of the Business Associate with respect to each entity should be clearly outlined in the agreement. The vendor would need to agree to being "lumped" into a single agreement listing others since, presumably they each get a signed copy listing each vendor and some might prefer that their contract not be known to others. From these perspectives, it may be administratively easier to use two separate BAAs.

Q. So do I need BAA with all our insurance companies, like Medical, Dental, Life, etc.?

A. Assuming the plan in question is subject to HIPAA, the answer will depend on whether the insurance company is acting as an administrator for a self-funded health plan or not. When insurance companies act as TPAs, then they are considered business associates. But in the case of a fully-insured plan, the insurance carrier is a covered entity in its own right, and no business associate relationship exists between the fully-insured plan and the insurance carrier.

Q. Does lost or stolen equipment count as a breach?

A. This will depend on whether the equipment stores or accesses PHI, and whether the equipment is appropriately encrypted. A lost device that is used to store or access PHI could be considered a breach if it's not encrypted.

Q. Does information from a drug screen for hire requirement needs to be treated as PHI?

A. If an employer is obtaining drug testing information as part of its hiring process, then it is acting in an employer capacity; not in a plan sponsor capacity. The hiring process is not related to administration of the employer's health plan. Therefore, drug testing results obtained as part of the hiring process would not be considered PHI in the employer's hands.

Q. Is medical information related to a workers compensation claim PHI? If not, does a company still have the same obligations to protect and limit access to this information.

A. Worker's compensation is not a group health plan subject to HIPAA. Therefore, individually identifiable information related to a Worker's Compensation claim would not be considered PHI. But other confidentiality laws may still apply.

Q. I have been under the impression that HHS had no authority to regulate businesses. I thought that their scope was health care plans, health care clearinghouses and health care providers who accept Medicare/Medicaid.

A. Technically, the health plan sponsored by the employer is the covered entity (i.e., the legal entity subject to HIPAA). Therefore, OCR is regulating the health plan sponsored by the employer rather than the employer itself. (Although, as a practical matter, the employer as plan sponsor is the entity responsible for ensuring that its health plan is in compliance.)

Q. Is a disclaimer recommended when using email to transmit PHI?

A. A disclaimer might be a good idea for general due diligence, but it won't provide any protection if an unencrypted message containing PHI is sent to or accessed by an unauthorized person.

Q. Is a billing statement with the employee's name and plan design listed considered PHI?

A. Yes, this would be considered PHI. However, for an employer sponsoring a health plan, it is only PHI in the employer's hands if the employer is obtaining the statement via its health plan records. A billing statement provided directly to an employer by an employee would not be PHI in the employer's hands.

Q. Are there specific steps for an employer to designate it's plans an OHCA?

A. Typically, designation of an OHCA is done as part of the plan sponsor's written policies and procedures.

Q. We sometimes fax health enrollment forms. It is my understanding that our fax machine has a hard drive that keeps the data for a certain amount of time. Do I need to have a BAA with the vendor that services the fax/copy machines, since the workers have access to those hard drives? Or is this going too far?

A. It is not going to far - this is exactly the type of information that must be protected. Vendors servicing the hard drives would be considered business associates, and an agreement would be necessary.

Q. Why would you share PHI with a payroll vendor?

A. Payroll vendors might receive information related to premiums, or health FSA elections, both of which would be considered PHI.

Q. Apart from breaches/violations, should we be reporting anything in terms of HIPAA to HHS on an annual basis?

A. No annual reporting is required, other than of breaches affecting fewer than 500 individuals. (Larger breaches require reporting within 60 days.)

Q. We are a small company under 25 employees, do we need to conduct a risk analysis?

A. Yes, if you sponsor a group health plan that is self-insured or that is administered by a third party administrator, the plan would be subject to all of the HIPAA privacy and security requirements, including the requirement to conduct a risk analysis.

Q. For the risk analysis, do we need to keep a physical copy of the analysis? Do we need to submit copy online?

A. The risk analysis should be maintained in written or electronic form for at least six (6) years from the date of creation or the date last in effect (whichever is later). It does not need to be distributed, but those who are responsible for risk management should have access to it.

Q. What about a 3rd party IT Dept.? They have access to our system - should we have a Business Associate Agreement with them?

A. Yes - a third party IT Department would be considered a business associate if it has access to systems/files/folders/applications that store or transmit PHI.

Q. Is the tier and plan that someone enrolls at considered PHI? Like Delta Dental Base plan vs. Delta Dental Buy Up Plan and if they are Employee + spouse vs. Employee + Family, etc.?

A. Yes, enrollment information is considered PHI. (There is some gray with respect to enrollment forms that the employer collects and transmits to the carrier or TPA. Technically this wouldn't yet be considered PHI. However, once the enrollment form is received by the carrier/TPA, it will become PHI. Therefore, it is generally safest to treat all enrollment information as PHI.)

Q. Can you provide a website/resource for the risk analysis audit?

A. OCR's Risk Assessment Tool may be found here: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool