Q&A from Assurex Global Webinar "HIPAA Privacy and Security"	April 25, 2013
Question	**Answer**
Q: Are employer administered Cafeteria plans (section 125) that have access to PHI still covered under HIPPA laws?	A: Only the health FSA portion of section 125 plans are subject to HIPAA. One exception is a health FSA plan with under 50 participants that is self-administered by the plan sponsor (i.e., no TPA) is exempt from HIPAA privacy and security rules..
Q: Can an employer allow employees to use the company fax machine to submit claims for HRA & FSA?	A: Sure, but it is all about managing risk. If the fax machine is available to all employees, or at least employees who have no right to access someone else's PHI, then you are leaving yourself open to an unauthorized disclosure (for example, the person faxing forgets and leaves the document in the machine which can be seen by the next person to use the fax machine). Also, many of the fax machines can be both a printer, fax, scanner and copier, which may retain
Q: Can HR update a Manager about an employees LOA status?	A: Yes, as long as health information from any of your health plans is not disclosed, and only the minimum necessary information is shared. For example, a date for return to work may be necessary for managers to manage staff; however, do not give any specifics other than when
Q: Do we now need to issue new business associate agreements in Sept 2013 because the business associate has to report security incidents?	A: The business associate (BA) has been required to report security incidents since April 2005 or 2006, depending on the plan size, and therefore that requirement is already included in most business associate agreements. Employers should make sure that their BA agreements include the following requirements for their business associates: (i) comply with requirements of the HIPAA Privacy Rule applicable to business associates; (ii) comply with the HIPAA Security Rule with regard to electronic PHI; (iii) report breaches of unsecured PHI to the covered entity; and (iv) ensure that all subcontractors of the business associate agree to the same restrictions that apply to the business associate. The 2013 final regulations have a compliance date of September 23, 2013; however, if a BA contract qualifies for transition relief, it can be amended as late as one year after the compliance date (September 23, 2014).
Q: Does a privacy notice need to be provided by a Business Associate? I thought only Covered Entities had to issue them.	A: Only the covered entity, group health plan, provider or insurance issuer needs to re-distribute the privacy notice. Business associates are not required to provide a notice of privacy practices.
Q: If an EE faxes his/her own info to the wrong number, I am not responsible for mitigating, correct? That's up to the EE to decide, yes?	A: An employer would not be responsible for an individual's disclosure of their own Protected Health Information.

Q: If as a company our HR manager helps employees complete enrollment forms, but the forms are sent to a 3rd party broker for imputting and enrollment into plans. What are the PHI privacy requirements or best practices surrounding this type of transaction and sharing of enrollment forms?

A: The employer must have a Business Associate agreement in place with the third party that is handling applications containing employee PHI.

Q: If they are in an EAP because it is offered to all employees automatically from date of employment, do we need to give each of the employees a privacy notice?

A: If the EAP is insured and the employer is receiving only enrollment and/or summary health information the employer may rely on a NPP sent by the EAP vendor. If the EAP is self-administered and/or self-funded the employer plan sponsor is responsible for the distribution of the NPP.

Q: Is "encrypting" or "password protecting" through Excel sufficient for HIPAA?

A: There is no specific "approved method" of securing PHI in HIPAA. Rather HIPAA requires that "appropriate" security measures be taken. However, for purposes of a HIPAA breach, information that is simply password protected is not treated as "secure" but proper encryption is considered secured. Proper encryption protects employers from breach notification requirements if there is an event that involves the loss, or improper disclosure, of the encrypted data.

Q: Is this more geared to employers or vendors (health providers)? It seems like a lot of work for an employer to become compliant with all the rights and authorizations.

A: For purposes of the privacy and security rules, employers (as plan sponsors) and their TPAs normally are not covered entities. However, the privacy and security rules generally do apply to group health plans and therefore, plan sponsors and their TPAs (as business associates) are affected. The nature and magnitude of the HIPAA privacy and security compliance burden imposed on a group health plan sponsor depend on the sponsor's role in the plan's administration; and on whether the plan is fully insured or self-insured. A group health plan sponsor may avoid much of the HIPAA privacy compliance burden if the plan is fully insured and the sponsor has no access to PHI other than summary health information and enrollment information, whereas the sponsor of a self-insured group health plan will have much more responsibility for HIPAA privacy compliance.

Plan sponsors with access to PHI are required to (i) train their workforces on privacy policies and procedures; (ii) establish appropriate safeguards for protecting the privacy of PHI from accidental or intentional use or disclosure in violation of the privacy standards (such as limiting access to information by creating computer firewalls and locking doors or filing cabinets); and (iii) implement policies and procedures designed to comply with the privacy standards, amongst other requirements. Some fully-insured plans only have access to summary and enrollment information, and such plan sponsors are exempted from these administrative requirements.

Q: During open enrollment or when new EE is hired if EE gives enrollment forms to HR manager then HR manager sends to broker, is the employer complying with HIPAA?

A: Health insurance enrollment forms can obviously contain PHI. To be in compliance with HIPAA in general, an employer must have the proper polices and procedures in place so that PHI is only used and disclosed for appropriate purposes as allowed by the law. In the case of sharing PHI with a broker, the employer's plan should have a business associate agreement in place with that organization.

Q: During an Open Enrollment, employees are requested to complete a new set of enrollment application forms. Since the insurance carrier prefers to put the information themselves into the system, they request us to send the original enrollment applications to them by mail. We usually send important documents via certified mail and require signature of receipt. It has not happened before, but what will be our mitigation procedure if these documents are lost in the mail? Is it best to just scan and e-mail the forms to the carrier?

A: Yes, if PHI is lost in the mail the plan is responsible for mitigation and possibly notification under the breach rules. While there is no specific requirement to use certified mail or registered mail, these methods provide the employer with detailed information confirming receipt. Scanning and emailing forms is also permitted, but we would recommend secure email and make sure that you have all the HIPAA Security requirements addressed.

Q: Within the company HIPAA Policy and Procedure, should we define or name the employees who are authorized to receive and maintain PHI for the company or is it assumed that anyone working in Human Resources or Administration is an authorized person and can view PHI of employees?

A: Titles, instead of listing specific individuals, is preferred. This way you do not have to update the policies every time an individual changes positions. It is up to you to determine who has access and to require those that have access to be trained accordingly. There is no requirement to list titles, but it is good practice to document who needs access and who has been trained. It is also common to list titles in the HIPAA plan amendment to your plan documents.

Q: We have a Mother who monitors her daughter's health claims, submitted and paid. The daughter is 26; do we need to get an authorization letter, with the daughter allowing her mother to discuss her information with us and our insurance agents?

A: If the mother is not the daughter's legal personal representative, authorization would be required. Keep in mind, to be considered "valid", authorizations have to be limited in scope. An authorization for "all claims for an unlimited time period" would not be considered limited in scope.

Q: What is a B.A. Agreement?

A: A Business Associate Agreement is a contract between a covered entity and a third party or vendor, and is required when the third party or vendor receives protected health information and provides a service to the covered entity using the protected health information (PHI) and the third party or vendor is not a covered entity. The contract requires the third party or vendor to protect PHI in much the same way a covered entity is required to do.

Q: What's the difference between a privacy official and security official?

A: The Privacy Official is responsible for all PHI, whether a conversation between people(s), written or created, maintained, sent or received electronically. The Security Official is responsible for only PHI created, maintained, sent or received electronically. Many organizations have the same person act as both.

Q: When he talks about distributing Privacy notice, do we need to get employee signature, i.e. receipt acknowledgement?	A: Signatures or receipt acknowledgement is not required for the distribution of notices of privacy practices by health plans.
Q: Would it be a violation of PHI if someone in a supervisory position makes some assumptions about an employee's health condition (i.e. mental condition, medical problems), and tells those assumptions to another employee?	A: While this could be an issue under other laws such as the ACA it is not technically a HIPAA issue because the information did not originate from the employers health plan (the covered entity). Individually identifiable health information becomes PHI when it is created or received ('touched') by a covered entity. Although not entirely clear, a covered entity probably 'touches' health information, consequently making it PHI, when (1) the health information is provided to a business associate of the plan (such as a TPA) so that the business associate can use the information to perform a service for the plan; (2) the health information is provided to an employee of the covered entity (but note that most single employer health plans have no employees of their own); or (3) the health information is provided to the employer/plan sponsor for the purpose of performing a plan administration function (such as deciding an appeal of a claim denial).
Q: Would you please restate the items of the information we should be listing on the accounting documentation.	A: Date of disclosure, individual's name, person or entity PHI was disclosed to, reason or purpose of the disclosure, and a brief description of what was disclosed.