Q&A from Assurex Global Webinar "Key Principles of HIPAA Administration and Compliance"	March 29, 2018
Question	**Answer**
If we send out a copy of the Notice of Privacy Practices annually with enrollment mateirals is that sufficient?	Sending the NPP annually will satisfy the requirement to provide a reminder of the availability every 3 years. However, it is still necessary to ensure that the NPP is provided to new enrollees and to anybody who requests it.
What is required for training on HIPAA Privacy?	There is no prescribed format or required frequency for HIPAA training. Typical trainings provide a background of HIPAA and its major regulations; a definition of PHI; common use and disclosure issues; and an overview of general security principles.
How do I evaluate a vendor that says they are "HIPAA compliant?"	If the vendor will be performing plan administration functions (e.g., claims processing or enrollment activities) and will be accessing protected health information (PHI) as part of its services, then it the employer should ensure that a Business Associate Agreement (BAA) is put in place with the vendor prior to sharing any PHI. It should not rely on a claim by the vendor that it is HIPAA compliant.
What determines "some" EAP plans that are under HIPAA?	Most EAPs are considered group health plans and subject to HIPAA privacy and security requirements. Some EAPs that only provide referrals or that meet the exception for small, self-administered group health plans, might be exempt. But it is most common for EAPs to be subject to HIPAA.
Are doctors' notes submitted by employees subject to HIPAA rules?	In general, information provided directly by an employee to an employer is not considered protected health information (PHI) for the employer. But it may be subject to other confidentiality requirements, so employers should handle such information with care!
Are voluntary worksite benefits i.e. short-term disability, group accident, subject to PHI?	Disability and accident benefits are not subject to HIPAA. Some voluntary plans (e.g., critical illness policies) may be subject to HIPAA, depending on their structure. It's necessary to look at voluntary benefits on a case-by-case basis to determine whether or not HIPAA applies. If you're not sure, check with the carrier who issues the policy for a determination.
Can all of these HIPAA requirements be included in the plan 'wrap' document(s)?	Probably not - the requirements really should be outlined in a set of policies and procedures, which is different in form and scope from a wrap document.
Does HIPAA apply to workers comp matters as well?	No. HIPAA does not apply to workers' comp.
For fully-insured plans that are subject to only limited privacy and security obligations (no health FSA or HRA), what are those limited obligations versus all of the HIPAA requirements for self-funded plans?	Employers sponsoring fully-insured plans who only have access to enrollment/disenrollment and Summary Health Information must comply with the requirements under the Privacy Rule to refrain from intimidating or retaliatory acts, and with the prohibition against requiring an individual to waive their privacy rights. In addition, there is no broad exemption from the Security Rule's requirements (although as a practical matter, compliance for such plans may be simplified).
How does HIPAA apply to an on-site medical clinic that does more than occupational health (e.g. can visit a doctor for an illness)?	Most on-site clinics will be considered health care providers if they conduct electronic transactions. In addition, many on-site clinics will meet the definition of "group health plan." While HIPAA lists on-site clinics as one of the excluded categories of benefits for purposes of privacy and security, it's unclear what the exact boundaries of the exclusion are). The safest approach is to treat any on-site clinic as a plan subject to HIPAA, or to seek advice from legal counsel for a more fact-specific anlysis.

I have a question about submitting a new health enrollmen application to our provider through gmail. I understand that basic gmail accounts are not HIPPA compliant. Are we not meeting security compliance by using gmail?	This is something that should be evaluated as part of the organization's security risk analysis. While there isn't a requirement that PHI only be transmitted by encrypted means, it is a best practice - and it's likely that, in the event of an audit or inquiry, OCR would expect to see encryption controls in place.
If a small employer uses an insurance broker, do they replace the employer as the responsible party in a sef-funded Health Plan?	No. If the broker is accessing PHI for purposes of assisting with plan administration functions, it would be considered a Business Associate. But the plan itself is still the Covered Entity (and the plan sponsor is ultimately the entity responsible for making sure its plan is in compliance).
If we are putting our required notices in an enrollment guide and notifying colleagues during open enrollment that the notices are in the guide on our intranet - is that sufficient?	Specifically with respect to the Notice of Privacy Practices (NPP), simply posting the NPP on a central intranet site would not meet the delivery requiremnets. NPPs must be individually mailed to the individual entitled to the notice. They may be combined with other materials in a single mailing, however. And with consent, the NPP may also be sent via email.
What about IT employees who help with document management and have access to all server folders and documents?	Generally, IT employees who have access to applications/folders that contain ePHI should be identified accordingly in both the plan amendment and the policies and procedures as requiring access to PHI for plan administration functions
What constitutes "agreement" to electronic notification? Is a signature needed? Can it be added to a personnel policy that transmission is electronic unless otherwise requested in writing, then the employee signs that?	There is no specific set of parameters for consent to receiving the Notice of Privacy Practices (NPP) electronically. The allowance for electronic delivery of the NPP has been given informally by HHS, and the only requirement is that the employer have and document some sort of "proof" of consent (which should include waiver of the right to receive the NPP in paper form). HHS has indicated that such "proof" may itself be electronic.
When we add a newhire for our dental plan, the carrier wants us to email the enrollment form to them. Is that compliant? They don't have a secure email system.	Emailing a blank form shouldn't be a problem under HIPAA. Even with respect to a completed form, there isn't a prohibition against emailing PHI. However, a best (and the safest) practice is to ensure that email transmissions of PHI are encrypted.
Ok, again, Sarah just said that only the benefits department employees should have access to PHI. However, most companies have benefit admin systems and payroll systems and the HR generalist staff has to have access to these systems. Again all the HR generalists can see is benefit enrollment information and payroll deductions for health benefits. Still it is PHI. What to do?	Any employees (HR staff, benefits staff, etc.) who require access to PHI in order to carry out plan administration may be granted access, but the plan sponsor should ensure that it is clearly identifying the roles/responsibiltiies that require such access, and that the titles/departments of these individuals are identified in the required plan amendment.
Is one "HIPPA compliant" the same as another "HIPPA compliant?"	HIPAA compliance may look different for different types of entities (e.g., covered entities that are providers; covered entities that are health plans; covered entities that are insurers; and business associates). But in a general sense, compliance with HIPAA means ensuring that the requirements of the Privacy, Security, and Breach Notification Rules are appropriately addressed.
Please confirm who the plan sponsor is.	The plan sponsor is the entity who is offering/making available the plan. In most cases, the plan sponsor is the employer.

Is it acceptable to have employees sign an authorization to allow assigned PHI personnel to help them with claims at annual renewal in case it comes up over the course of assisting throughout the year?	Yes, as long as the authorization meets the required content requirements.
Who normally serves as the Security Official? Not the Privacy Officer, correct? What background/experience do they have?	Normally (but not always) the Security Official is a senior member of the IT Department. Anybody can act as Security Official, although it helps to have an understanding of the organization's technical infrastructure and existing security controls.
I have been advised that employees' benefit elections and benefit premiums are PHI. Many HR generalists have access to this information through access to payroll systems to view employee deductions and benefit enrollment systems where they can view employees' elections. Are these items considered PHI and if so, does the privacy officer have an obligation to provide HIPAA training to the HR generalist staff as often as it should be provided to the benefits department staff who work with PHI on a regular basis?	There is some gray with respect to enrollment information. The regulations exclude from the definitinon of "PHI" any individually identifiable information that an employer holds in its personnel records in its role as employer. But benefit elections and premium information are likely originating from the health plan records, and would therefore be considered PHI. Therefore, the general requirements for PHI would apply to individuals who have access to such information.
Does this "Privacy Official" need to be assigned in company's with less than 50 employees?	Yes - HIPAA will apply to employers of any size. The only exception is for group health plans that: 1) Have fewer than 50 participants; and 2) are completely self-administered (i.e., do not use a third party administrator). In most cases, employer do not self-administer their own plans.
Is the NPP sent from the insurance company?	The insurance company will often issue an Notice of Privacy Practices for a fully-insured plan, but two notes of caution: First, if the employer also sponsors a self-funded plan (e.g., a health FSA), it is responsible for issuing the NPP for that plan. And the carrier's NPP may not accurately describe the employer's actual processes. Therefore, even if the employer only has a fully-insured plan, it may still be a good idea to review the carrier's NPP, or develop an NPP that the employer is sure accurately speaks to its operations.
What is an OHCA?	"OHCA" stands for "organized health care arrangement." A plan sponsor who has several different plans (e.g., medical, dental, vision, Rx, etc.) may designate these various plans as a single "OHCA" and therefore develop just a single set of policies and procedures; designate a single Privacy and Security Official; develop a single Notice of Privacy Practices, etc. In other words, the plan sponsor doesn't need to develop procedures with respect to each different plan; it groups its various plans together into a single plan, or OHCA.