Q&A from Assurex Global Webinar "HIPAA Privacy and Security for Employers in the Age of Common Data Breaches"	April 30, 2015
Question	**Answer**
Are there templates available for NPP that we can look at?	A: Yes HHS has published model HIPAA NPPs for both providers and health plans that can be found at http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
Are you recommending our company to create a summary plan document that outlines what our company does in regards to Hila? Does there need to be a section in the Personnel Policy about HIPAA? I thought we removed that section last year?	A: We would not describe it as a "summary plan document", rather we believe the rules require an employer sponsored health plan to have written policies and procedures which the employer (plan sponsor) follows regarding the privacy and security of plan PHI.
As a level 1 employer, which of the many steps/requirements that were presented here are we required to do?	A: If an employer has no access to PHI other than summary health information and enrollment data the only privacy requirements which apply to plan or plan sponsor are the prohibition against retaliation and restrictions on asking members for a waiver of HIPAA rights. However HIPAA Security requirements may still apply if any PHI (including summary and enrollment data) is in electronic form.
Can you give any websites to get templates for written policy for HIPAA? And other forms?	A: HHS has a site devoted to general information about HIPAA for covered entities at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html. However, HHS has not published sample policies and procedures. Benefit Comply offers a HIPAA compliance web based tool which includes model policies and procedures. More information can be fond at http://benefitcomply.com/hipaa-compliance.
Does the NPP have to actually be sent or can a link on the company intranet be provided via email during open enrollment to cover the 3-year requirement?	A: Simply posting the NPP reminder on a website would not generally be sufficient. An HHS FAQ described different methods a covered entity could use to distribute the NPP reminder. • sending a copy of the actual notice of privacy practices to participants • mailing a reminder that the notice of privacy practices is available, with information on how to obtain a copy • including in a plan-produced newsletter or other publication information about the availability of the notice of privacy practices, with information on how to obtain a copy Informally, representatives of HHS also have commented that the notice of availability could be provided by email under the same standards that apply to electronic provision of the notice of privacy practices—specifically, the individual must have agreed to electronic notice (and not withdrawn agreement), and if the covered entity knows that the email transmission failed, it must provide a paper copy.
He mentioned reoccurring training, but how often should the employee receive reoccurring training?	A: HIPAA does not specify how often employees with access to PHI must be trained. At a minimum these employee should receive training when first hired or transferred into a position that involves the use of PHI, then receive updated training whenever an employer's HIPAA policies or procedures change, or applicable laws or regulations change.

I often receive PHI from medical providers over the fax machine. What is my obligation to stop this infraction by the physician office? If a company send personal medical records via standard emails (which to me is not HIPAA compliant), what do you do? Report the company? During transfer of emails, information could have been intercepted which is a breach and could possibly in the future look like the company I work for caused the breach when in fact we didn't.	A: Technically it is correct that your firm is not in direct violation of HIPAA if another firms improperly sends PHI to you. On the other hand, the reason HIPAA exists is to protect member and patient PHI. In the case of business partners who use practices that put the PHI of your employees or members at risk it may be prudent to discuss this situation with the other entity.
If enrollment data under ACA requires SSN is that not PHI?	A: Yes - individually identifiable health plan information such as SSN that is part of a health plan record would be considered PHI.
if someone has a fully insured med plan, but has a self funded HRA... does this kick them into Level 2?	A: An HRA is simply a type of self-funded plan for HIPAA purposes and an employer sponsoring an HRA should have HIPAA policies and procedures in place.
In regards to a separate file for PHI, if an employer has a separate file for employment/personnel, benefit, workers' comp, and medical with anything PHI related would go in the benefit file (all files separate access from each other) would that be sufficient? Is it ok to keep health plan info in the employee file or should it be kept in a medical or confidential file? With saying that all PHI needs to be filed separately, does this mean that all applications for Health, dental, life insurance etc. need to be filed separately, or just claims associated with them? As well as short/long term claims?	A: The requirement to keep PHI separate varies from employer to employer. HIPAA requires that access to PHI be limited to only those employees who have a specific reason allowable under the rules. In some cases certain employees with legitimate access to other medical related information such as workers comp data, may not have a role with the employer and the plan that would permit access to PHI. In other cases the same employees may have roles that permits them to have access to various types of medical information including PHI. The key here is to limit access, and sometimes the only way to do that is to segregate the data.
Is health information on enrollment form considered Level 1 - such as for pre-existing conditions? We are fully insured with no HRA, but some of our insurance enrollment forms ask about medical history including specific diseases/conditions. does this make us level 2?	A: There is some debate regarding this point. Some advisors believe that detailed health information on an enrollment form is still considered enrollment data. We believe it would be prudent for any employer who collects medical information for enrollment purposes to be considered a level 2 employer and develop full HIPAA polices and procedures.
Is there a particular entity or agency you can recommend to "certify" a Privacy or Security Officer for their firm?	A: There is no official entity that certifies HIPAA compliance. There are vendors that supply some kinds of certifications of completion, but these are simply for documentation purposes and are not recognized in any way by HHS.
Payment is not referring to premiums is it? What about information included in the enrollment form? Is that still Level 1?	A: Plan payment related information regarding an individual's health plan premium, and data on enrollment forms is generally considered enrollment related PHI. However, remember if an employer only has access to summary health information and enrollment data their HIPAA privacy obligations are limited.
Should the privacy & security official(s) be designated in the HIPAA policy/procedure or elsewhere?	A: Yes these officials are typically designated in a plan's HIPAA policies and procedures.

So when sending out an rfp and we have names on a census should we take them off because they are not necessary for quoting? Does that fall under Minimum Necessary?	A: Yes - that would be a good example of applying the minimum necessary principal if the names are needed to accomplish the purpose for which the PHI is being used.
What about receiving vendor invoices that list each employee's name and the premium amount associated - is that PHI?	A: Yes individual employee plan cost information provided by the carrier is a form of PHI.
What if the PHI indicates that an employee is breaking a state or federal law? Hypothetical: If claim data showed a surgeon was HIV positive, and state laws prevented HIV positive people from performing medical services, can the information be used by the employer to remove the doc?	A: HIPAA regulations allow for the use and disclosure of PHI in various situations such as when necessary for public safety, when requested by law enforcement, and other situations. An employers HIPAA policies would typically include provisions that define how the employer would handle PHI in these situations.
When employees receive a fit for duty evaluation under Workers Compensation does PHI information under consideration?	A: No - HIPAA does not apply directly to workers' compensation coverage,. and health information collected by the employer as part of the administration of workers compensation would not be considered PHI.
where can you get training for HR, Accounting, and IT members? Are there HIPAA classes to attend for new employees coming aboard handling PHI	A: A good resource for online HIPAA training is Bridgefront. More information can be found at http://www.bridgefront.com/solutions_education_hipaa.php.
What agency is responsible for enforcement?	A: The privacy and security requirements of HIPAA are regulated by the Department of Health and Human Services (HHS)
Work at small company, employees were used to receiving an annual "Christmas Card" list of employees Names and Addresses. Is it okay to send these out?	A: General employee information unrelated to health plan data such as names on a Christmas list is not considered PHI and would not be subject to HIPAA rules.
You state that you must document the training. Is any competency based documentation required (i.e. quiz on the training)?	A: No HIPAA does not contain any specific training structure, format, or documentation. Employers should document training for use in a participant lawsuit or audit by a regulatory agency.