HIPAA & HITECH Compliance for CBO-Health Care Partnerships

Aug. 16, 2017

Good afternoon everybody. Thank you very much Steve. What an introduction [Indiscernible]. We are going to get started. I know that HIPAA is one of those issues and that is pretty significant on the healthcare and integrated care front I. I know that in number of the community based organization I am I have worked have raised this as a they consider a barrier to their healthcare integration and I'd like to certainly work with you to minimize those barriers as it relates to your capacity to support covered entity for some of these healthcare organizations compliance with HIPAA and mitigate some of the risk here today our learning objectives are to provide you with some key components of the HEPA and HITECH act to help you understand were going to focus primarily today on Ray privacy and security rules the both the HEPA and HITECH act contain other provisions most notably the additional fraud and abuse standards for Medicare and Medicaid in healthcare in general and as well the transaction standards and Meaningful Use for electronic health records. We are also going to discuss very clearly what the roles of covered entities and businesses you are as described in the regulations I and provide you with an understanding of why this is a factor for you as you are doing more outreach for the sustainability of community-based services by contracting with health plans and other payers. We are also going to review some mechanics of some privacy and security compliant programming just to give you a heads up that my experience has been that most of you have already launched into this. You have some standards, some basis for creating privacy and security regulation problem driven by just good business practices or cases by your contracts with state or federal agents these.

The last piece of this is my goal is to try to keep your head from exploding as you download all the information but I do want to assure you that we you will recover if your headaches I certainly did. We are going to talk a little bit just about the healthcare environment. One of the challenges I think are community-based organization as you reach out to the healthcare industry weather is hot it'll health plans other kinds of [Indiscernible] ACL is that there is a massive and complex that rules and regulations the federal level and it weighs down into the state level fact is been documented that the healthcare industry probably the second or first was heavily regulated industry in the country. Those of you who are not familiar with my work [Indiscernible] archery listen to about HEPA because I am still a recovering health and privacy officer was responsible at the onset of HEPA privacy way back in the day forgetting my health plan ready and implementing HIPAA privacy and security at our healthcare organization . Part of the challenge in healthcare regulations is understanding where do you fit in as community-based organization. Unfortunately none of the HIPAA rules a regulation even a definition of covered entities and business associates addresses media based organization and your services. It does cover some of the relationship you are contracting with the health plan for certain kinds of care management or clinical services and/or you utilizing PHI protected health information as part of your business with the healthcare organization potentially fall under the the business associate relationship. The idea opportunity for you in terms of engaging the healthcare organization is to understand what some of their headache some other points of pain are and that helps you adapt your business program business strategy is that your more effective partner.

Again the ideal partners for the industry healthcare industry of those were knowledgeable supportive and can help mitigate risk and reduce the potential for somebody to have to spend time behind bars. The legislation [Indiscernible] again there's many different kinds of healthcare legislation is [Indiscernible] the top about what kind of service and treatment has to be provided for anybody was in the emergency room also addresses issues like [Indiscernible] showed up in the emergency room because I thought I was having a heart attack not having a heart attack that six hire burrito you had that that you home so may have some liability with copayments for hospital treatment but [Indiscernible] provisions then Apollo provide you with some option for appealing. This also huge issues around fraud waste and abuse legislation particularly in the Medicare and Medicaid program but today going to speak specifically in this alphabet so about hit by the health insurance portability and liability act and the health information technology for economic and clinical health act. We will start with HIPAA .

HIPAA was originally health insurance portability act which was enacted in 1996 and signed by President Bill Clinton title I of HIPAA or the original have a was about protecting employer-sponsored health insurance. That was the opportunity for you to bridge your insurance and not be locked out new insurance coverage if you move to a different employer had employer-sponsored plan as long as you do not have a gap of coverage are more than 63 days [Indiscernible] because of pre-existing conditions. HEPA -- HIPAA to window is really about beginning the when extension of patient protection is were defining the regional have been act which was called Kennedy Kestenbaum window really does focus on critical issues around his of these use of electronic transaction healthcare it was important for the government to establish some regulations the kind of tenderized those transactions were process also an opportunity to standardize protections privacy and security protections for consumers are HEPA is up to each state and sometimes within the state teacher covering entity to design how they were going to meet privacy and security. The other piece that HIPAA privacy offered was access to your health records for consumers something that was that again formally available across the country the federal statutes established some options for access to your healthcare record picketing think of HEPA window title to which was enacted in 2003 also known as the administrative [Indiscernible] rule although never in the history of government regulations have administrative [Indiscernible] been further from what ever covers I [Indiscernible] trotting the electronic interactions between healthcare organizations particularly 834 regulations the standard about how enrollment of people is process into a health plan. 837 is how healthcare claims are processed to and covered entities are not going to talk about that they were going to focus primarily on the [Indiscernible] but I've given this presentation before folks have raised the question about the unique [Indiscernible] identifier for the NPI that is also pretty hit the regulation and was created to help help the government track provider is the kind of providers who are available in many states and at the federal level cannot transact or engage in business the federal government Medicare/Medicaid in some cases state Medicaid programs unless you have a unique national identifier and NPI number.

As I mentioned before HIPAA also addressed additional standards healthcare fraud and abuse. Title to privacy will protected individual rights providing his of disclosure and or access to healthcare data and the security rule is really operationalize the privacy regulations establishes the safeguards of the protection of what the elements of protected health information or PHI and

that the individual healthcare data security rule is also most civic to electronic PHI are E PHI -- or E PHI.

The privacy rule in short know it's not short defines individually identifiable health information that the critical element for you to understand those of the elements that make up what are called protected health information or PHI. Identifies roles and responsibilities of covered in these and business associates and for the most part community-based organization or a subcontractor to a health plan consider the latter of business associates. It also addresses allowable disclosures your healthcare operation also referred to as treatment payment healthcare operations or TPL and it establishes the penalties violations in the Department of Health and Human Services office of civil rights that so that is the organization the government organization responsible for for the overs right and management of HEPA privacy and security regulations. Insurance the privacy requires that a covered entity or business is may not use or disclose protected health information wire other I [Indiscernible] healthcare protected health information elements and that the individually identifiable health information data that is collected or owned or managed for use in any way by covering entity or its business associate and is transmitted or maintained in any form way [Indiscernible] anything that you have electronically fusing hieroglyphic using our chat all of that contains any of the individually identifiable health information is considered protected under HEPA -- HIPAA [Indiscernible] limited to the past present or future physical and mental health condition of an individual health services are paid for what kind of services are paid for for that individual and the record has been created by healthcare provider. The other piece the high-tech rule did for the HIPAA enhancement that it requires the protection and security of PHI for a 50 years after the death of the healthcare consumer question I. [Indiscernible] individually identifiable health information these are some of the elements Social Security number, medical records some of you may recall that in the past some insurers particularly [Indiscernible] insurers utilizer Social Security number as part of your member ID number. The practice was struck down under the introduction of -- for the enactment of the HIPAA privacy rule is medical record numbers are phone numbers anything related to your name address code or County, your city none of that information can be disclosed without proper authority. Your email address back from a facility any photographs of you any photographs of part any parts of you that might be -- to identify you metric identifier this was added under the high-tech rule because the high-tech rule focused more on some of the new electronic and technical data utilized in healthcare transactions.

Voice and fingerprint your if your health plan or your hospital allows you to access your medical records through voice or fingerprint options that information has to be protected. Your genetic information with your predispose to curly hair or baldness is protected under HIPAA . [Indiscernible] I have shoe says on here because this actually happened somewhere but I won't disclose it to think about a small community where almost everybody knows each other unity of maybe thousand, 1200, 4000 people there is a person in the community who show signs with Evan team -- 17 1/2 there was nobody else in the community what I shoe size that came near 17 1/2. Every time that person went to the doctor or went to a hospital and engaged in healthcare that information because part of problem within his feet aspect that information about his size 17 shoe was considered protected information because if -- allowed people to immediately identify who that healthcare consumer was. Fertile of this and I are thinking how do we transact any business can we allow to use this information at all certainly the rule provides for that.you are

allowed to use the information is for shared information to a covered entity and business associate or between other covered entities. Is allowable for treatment payment in healthcare operation and the private financial kind of transaction are covered under treatment payment in healthcare operations mail. You may also utilize the identified PHI aggregate information for public health research and other kinds of I the identified you can't attend the person is say researcher public health and are trying to identify how many Medicaid beneficiaries are actually being treated for HIV that you're allowed to extract that information but not extract or share any of the information that identified [Indiscernible] those individuals are in of course there is a requirement share PHI is required for law enforcement. There are also very specific standards about the kind of disclosures to law enforcement agency that are required as a business associate any petition directly to you disclosure of PHI for data that is owned by the covered entity that needs information I have collect data and/or uploaded as a result of your contract with the healthcare organization all all of this request need to go to the covered entity the cover entity on the information and is therefore responsible for the disclosures.

Oh there are also other allowable disclosures, disaster relief. Let's think of Katrina and the need to very quickly and easily share information about people were who were under treatment and those circumstances you are also allowed to provide for public health reporting comedic will disease notification -- communicable disease and notification [Indiscernible] the safety threat to law-enforcement you may be required to disclose information -- PHI about that individual. Again, I encourage you to refer those increase back to the covered entity home your contracted -- with whom you are contracted. One of these covered entities and one of the business associates? Covered entities of the first-tier folks were considered responsible for the protection and they compliance with the HIPAA privacy and security regulation will responsible to ensure that the identified business associates and execute business associate agreements are also responsible for ensuring that issue notice of privacy practices and most of you have seen those you get them annually renew or change your health insurance coverage every time you go through a hospital emergency room very likely getting us the privacy product is simply the organization description of how to use this in transact her PHI under the allowable regulations for HIPAA. Most of those are standard documents government did establish the template for the use of that kinds of covered entities include plans insurance HMOs physicians providers players sponsored health care organizations [Indiscernible] Medicare, Medicaid, veteran and armed services insurers. Business associates are those contracted with covered entities for the execution of some kind of business related to the cover allowable uses of PHI treatment payment in healthcare operations in your doing those services under a contract with covered entity. [Indiscernible - multiple speakers] you are also responsible for performing the services function that is defined in that contract with the use of PHI according to the contract and the business associate agreement that you execute. [Indiscernible] associates are responsible for for [Indiscernible] to the covered entity and that has to be done within 60 days of you discovering the breach.

The business associate agreement why is required there is a contract that is going to engage the use of PHI and is under one of the treatment payment in healthcare operation provisions by covered entity and a business associate. One of the things that you will find is that some covered entities have not yet required their community-based organization partners to execute a business associate agreement. There are varying levels of agreement about whether or not some of the services that you may be providing -- let's say you are doing referral services or support you

don't have full access to PHI some covered entities help plan NCOs are not asking you to execute a business associate agreement. Most of them well just as a CYA for them and if they don't ask is your transacting business you should raise the issue of whether or not the business that your be engaged in for your contact requires a business associate agreement.. Business associate agreement is not required between certain kinds of covered entity the health plan at the hospital to have a contract health plan is utilizing the hospital to deliver services for its enrollees know business associate agreement is required because they're both covered entities they both have to follow the same rules and regulations. The thing goes for a contract between a health plan and an individual physician or provider group they're both covered entities and their sharing information for treatment payment in healthcare operation. Again the business associate is going to issued by the covered entity you will not initiate execution of a business associate to cover entity's responsibility to identify you a as a business associate and then have you execute a business associate agreement will always be a contract attached to the business associate which is defining the services that are being delivered in engage in treatment payment in healthcare operation. The businesses that agreement binds you the business associate to comply with the covered entity's privacy and security rule as well as the HIPAA rule so in many cases just as an added protection and this often happens with covered entities may have had a citation from the office of civil rights on a HIPAA privacy violation in the ad national requirements for security and protection the PHI in their own contract.

This is why it's important for you to have a very strong HIPAA compliance program . The business associate agreement some of the elements we should see in that is establish the permitted and required uses of PHI uses and disclosures of the information that you're allowed to utilize as a business associate. It allows you to use and disclose the PHI for the proper management and administration of your covered entities contract and and it may not give you any authority and even if it does explicitly state can do whatever you like with this information we don't care don't do it. The agreement should also be very specific about not allowable use or disclosure of the information in violation of the HIPAA privacy rule .

A big picture and factor in adhering to have a privacy use and disclosure standards is another subtext in the privacy rule called minimum necessary disclosure. This is a pretty big deal. As we get further in the presentation you will see that failure to implement minimum necessary disclosure procedures is one of the significant me cited for violations by the office of civil rights. The minimum necessary disclosure is a key element of the privacy rule that limits unnecessary or inappropriate access to use and disclosure PHI. It creates entities using PHI must document policies and procedures how you will address the necessary standards such as identifying the person or class of persons within your organization them a nexus of the PHI carry out their job duties [Indiscernible] you will define this is the level of access they will have to an individual's PHI information. That information may be brought and you may determine that they have access -- full access drivers on the other hand we do have access to a person medical history their Social Security number or any of those details that are necessary for the expectation is that you're going to set up classes of individual relate to to those classes of individual with the level of PHI information that they can have access to that there authorized to have access to because if you find out for that a driver has been getting access to Social Security information or other information you strict and five or [Indiscernible] for the individual classes of work. Again, and Arthur a care management person is probably going to have access to information like medical

history maybe Social Security number that caseworker is working in conjunction with the Medicaid agency to support a person's reauthorization for Medicaid etc.. One of the things that I've had ways with some community-based organizations as how much information does her finance department need. How much access to PHI does her finance department need for after all they are doing the billing, the monitoring and auditing their processing claims and maybe doing some of the reporting. My recommendation to you is everybody in your organist station every [Indiscernible] you need to define what level of access -- what the minimum necessary PHI need to transact their business that includes her finance folks to they made all access to Social Security numbers or photographs of folks medical conditions and those kinds of things in order to transact business related to billing and payment. That's up to you to decide based on how your organization is structured.

Your we are going to talk know about the security rule which is also part of title II and as I mentioned security rule basically provides operational direction for the implementation of the privacy rule. The security rule higher requires or assures of the confidentiality integrity and availability of all the PHI can that's electronically created PHI that's received created maintained or transmitted by covered entity fully protected identifies and protects against reasonably anticipated threats to the security or integrity of EPHI. It also protects against reasonably anticipated and permissible uses or disclosures of PHI the security rule also heavily emphasizes a development of staff compliance program policies and procedures that outline for your staff staff or volunteer how your protecting the PHI what your expectations are for their performance and support for meeting privacy and security requirements also. Also provides the ministry to full technical and physical safeguards that must be adhered to the development and use of protected health information in security rule also heavily emphasized is that you designate a security officer, probably whoever is the head tech for your IT department to, your CIO or somebody like that.

The security rule identifies a variety of security standards establishes required and addressable implementation specs. The required specification you must have incorporated you must implement to must operationalize and again those are things like minimum necessary necessary safeguards necessary safeguards how much access people in your organization have to PHI based on the need to that access to execute their job and there also addressable educations. There a lot more flexible and think of you simply ability how and how you meet the privacy and security requirements for workspace security I always. I always -- the first you recommend everyone go what we need to do with the low hanging fruit. The low hanging fruit is all of your computer screens need to be facing away from public view whether it's in a cubicle or whether it's in somebody soffits your computer screen should always be facing away from public view people walking down the hall people office when you have outside yes folks everybody in your organization should not have full access and you have full access at your desk should make sure that you not providing public access. That they flexible opportunity under the security rule.

The administrative safeguards can designate a privacy officer as well as the security officer. Adoption I ran privacy procedures that address things like access the PHI is restricted to only those employees who need to complete their job function and its we get into that will based access information that I previously discussed expectations a policy and procedures are going to establish internal audit to identify and correct potential breaches of PHI and you're going to

document instructions for addressing and responding to any security breaches you. The other piece that the HIPAA security regulations require is that you document and execute sanctions for PHI policy procedure violations expectations just that you have something in your policies and procedures that says if you intentionally violate HIPAA roles and sometimes if you unintentionally do it as I left my handheld device in the trunk of my car when I went to the mall and the complainant client PHI in my car was stolen it's not locked that information is now in the public domain intentional or unintentional your policies and procedures must identify potential sanctions for employees who violate the HIPAA privacy rules .

You must establish comprehensive and ongoing training. My recommendation is always within the first 90 days of hire as you create your on boarding boy employees HIPAA training thorough HIPAA training and expectations for your organization needs to be included in that. You should also do annual training for everyone that includes your board all of your executives your staff and any volunteers that you have five maybe providing some support to provide some access to PHI. Another huge factor is how you manage your vendors lots of you are utilizing vendors for delivery of meals or transporting clients appointment in a variety of ways. Your vendors were going to have access here PHI here's we might want to create your own draft of a business this is an agreement and bind your vendors line complying with HIPAA privacy rules and regulations because there vendors are the source of a HIPAA privacy and security breach they need to know that they must reported to immediately and if that branch involves information that is owned by the covered entity you need to respond to them 60 days to notify them the vendor compliance is a huge issue because they potentially are a risk anyone to help mitigate any and all risk of inappropriate use and disclosure of PHI.

Disaster recovery planning is another factor that is heavily identified in HIPAA and it really is about how do you ensure that you have access to PHI without a member access to their PHI in the circumstances of the disaster exists client and the client needs to access their records for treatment. It's also your responsibility to coordinate with covered entities expectations for disaster recovery and a number of state unit on aging and other available organizations Medicaid for and also require disaster recovery provisions in contracts with organizations. Technical safeguards are those things that really me to how you are protecting electronic health information as it housed in your computer system looks at things like how do you control access how do you sure that your the janitor can't walk through while cleaning up your office hit a button and suddenly access to PHI is available. And asks that covered entities implement technical policies and procedures and again this is a part of your overall HIPAA policies and procedures in your IT people are probably already implemented a number of these things for instance the use of encryption as you are transacting information that contains PHI whether or not your computers go blank all if you're involved in using computer and you walk away from your desk and you gone or stop using it for more than a minute or two to system automatically shut down that you have to reload your password in order to re-access the system. And also asks for audit control. They want to ensure judgment you want to ensure that your monitoring how your protecting PHI are the policies and procedures and the technical safeguards that you have in place working to help mitigate potential breaches. This is particularly true as you talk about not just EPHI but your hardcopy. And a lot of cases you are so very heavily paper hardcopy oriented point for you to ensure that our safeguards cover not just electronic PHI but your hardcopy PHI. The integrity controlled these addresses the fact that you need to implement policies and procedures that you

don't properly alter or destroy PHI. The very significant revisions in the security and the high-tech rules about the maintenance of the integrity of PHI that it cannot be inappropriately altered or destroyed except by the provisions that are established security and high-tech rules. Are also responsible for ensuring that you have are not improperly altered or destroyed any PHI

Transmission security is when a covered entity you need to ensure that your technical security measures are ensuring ensuring that as you utilizing EPHI is being transmitted to an electronic network that using certain safeguards to reduce the unintended access of that information by a recipient. In some cases authenticating for the beneficiary the recipients are of the information this is a huge issue as a relates to fax information somebody puts in one room digit in somebody's PHI is now on a fax machine at McDonald's versus Dr. feel good. The lead for you to ensure that your authenticating how information is processed in any electronic media is a critical aspect of the transmission security. Again, the encryption rule is heavily emphasized here how you transact that information electronically through the computer and the authentication of entities with PHI a shared.

The physical safeguards rail around how are you and your facility providing additional protection around access to PHI for ensuring that you're not going files that have PHI and open public areas not in your reception area but it someplace that you don't have a lot of heavy public traffic again turning that computer so that its way facing away from public view. It also talk about workstation insecurity devices. One of the challenges again as we become more sophisticated needs more laptops in these handheld document is no handheld technological supports important to make sure that your HIPAA privacy and security protections apply to those devices as well. Again, do you have the ability when you utilizing handheld information but he says to you was stolen out of my car can you lock it down from your IT department within moments of notice. Can you ensure that all of the documents whether it's laptops and handheld devices have password on them and that those passwords have to be utilized people not sharing passwords the maybe sharing these devices. You need to have a policy and procedure to address the transfer removal this puzzle and reuse of electronic India to ensure the appropriate protection of the PHI and again the specific standards were highlighted in enhanced and the passage of the high-tech act.

The high-tech act apparently the government did not feel that HIPAA rules and regulations that they pass the high-tech act pick the high-tech act was enacted as part of the American recovery and reinvestment act and was added to [Indiscernible] as part of title III effective date of to the line when it was enacted and full complaints required by all participants between 2010 and 2013 depending on the class of eligibility defined in the law. Again the high-tech act strengthens privacy rule protection and here's why this is important to for those of you are wondering why my sitting listening to this one beautiful Wednesday afternoon instead of being out on the golf course because the high-tech act is coming after business associate. The original HIPAA privacy rule predominantly applied to covered entities in terms of the government auditing the right monitoring the government's ability to [Indiscernible] because in many cases the breaches of privacy is pretty recurring business associate level the high-tech act provided the government with the opportunity to hold business associate agreement hold business associates excuse me equally accountable the covered entities within their contracted. It also expands the standards for reporting unintentional disclosures and will cover some of that. The high-tech act also some of

your probably failure with further advancement of use of electronic health record in Meaningful Use which a lot of providers took advantage of some of the Meaningful Use to upgrade and enhance their electronic health record.

The big deal in the high-tech act it's about reporting breaches in the high-tech and establishes some new security breach notice requirements first and foremost again business associates and covered entities maintain unsecured PHI and cover breach of this information I have to notify the individuals who were affect did and you must notify the office of civil rights. You should as part of your notification be prepared to include to the government be prepared to include detailed identification of how the breach occurred why it occurred and what corrective action measures are putting in place up to and including sanctions against the individuals responsible creation of new protection and security measures and retraining for staff. The business associate must provide notice of data breaches for protected health information that is owned by the covered entity within 60 days of you becoming aware that the breach has occurred the business associate and covered entities must identify each individual protected health information with illegally accessed and then the covered entity is responsible for issuing the notice to each one of those individuals and I'm sure by now many of you who have had and thumb or some of the other healthcare organizations with had math the breach of the last five years are in receipt of one of those notices that says I your PHI has been breached and here's what were doing to protect it.

For breaches the HITECH act requires that for breaches that involve more than 500 consumers information there must be a report of the breach in the media. For those folks particularly for Medicaid population or for folks who are snowbirds I'm in Florida notice about XYZ health plans breach occurred is going to my winter home I will see it for six months but this also requires that there's a public notice generally published in a newspaper that identifies how the breach occurred what it was what they're doing safe that information. The high-tech act is also very specific about the destruction of PHI because one of the many cases was breaches the result of folks thinking that they had properly destroyed PHI and they hadn't. The destruction of PHI whether it's paper, film, other hardcopy must be shredded or destroyed so that the PHI cannot be read can't be reconstructed this what does the government provide for folks provide office machines instant income because now everybody's got have massive numbers of shredders on their property. Electronic media must be cleared purged or destroyed and consistent with the specific NIST standards and you got the link there so that the PHI cannot be retrieved. What has happened as we discovered nothing on your computer can never be really a race so the standards provide for the destruction of PHI in specific formats that help ensure that it can be reconstructed so that folks can collect the information and use it for nefarious means

---

You should also be prepared to follow any instructions from the covered entity about any need to destroy PHI here's the part you've been waiting for when it comes to have a privacy and security the best defense is a strong offense. Your organizational personnel policies and procedures meet corporate HIPAA privacy protection and sanctions. Needs to be incorporated as part of your organizational every day business needs to be part of how you manage personnel as a relates to integrity of the relates to anything else you very important that folks see this as an integral part of how your organization is structured and operates. As I mentioned HIPAA enforcement is the responsibility for the title to the HIPAA act by the U.S. Department of Health and Human Services the office of civil rights. There responsible for establishing provisions for oversight and

monitoring of the HIPAA rules the responsible for the review in responding to have the complaints. There is a responsible for investigation of those complaints and for levying compliance and sanctioning corrective action requirement and breaches are discovered and they also [Indiscernible] monitoring penalties. For the most part the most common penalties are corrective action plans and/or increase reporting and more monitoring for the government which everybody welcomes. More recently you have seen article and will back heavy monetary penalties and it's important to understand that these penalties can be in two forms civil and criminal and here's another incentive individually you you can be prosecuted for HIPAA violations as well as organizationally heavily fined for HIPAA violation is not something that any of us can afford but it's also something that we need to make sure that we defend against some of the most common citations of HEPA breaches of course the misuse of disclosure of PHI failure to establish adequate protection for health information like not having policies and procedures that help people the society to PHI.

Patients unable to access their health information again before HIPAA there was no universal rule that said have access your information are still some folks who may or may not follow the rules about providing patients with access your permission if you get a request for access to information is a business associate that should be referred to the covered entity because again that date some by the covered entity certain policies and procedures that they need to follow verification of her the petitioner is first and foremost before that information is disclosed. Using or disclosing more than a minimum necessary standard business transaction that as we we talk about minimum necessary it's important for you to identify has how much access to PHI your maintaining in your organization and make sure that I will [Indiscernible] today need to be name the date of birth and [Indiscernible] sometimes becomes a routine part of a member file pick the lesson the failure to establish safeguards of electronic protected health information I share two things with you it's the encryption of the information and under no circumstance is PHI to be texted, under no circumstances any form of identifiable individual health information to be texted or used in the text at all.it is an instant violation sections will be applied.

Again, just a couple of issues around the civil penalties. I'm not going to read through all of these but the government is a little bit flexible and understanding that in some cases because the truth would privacy rules of you policies and procedures can be so very complex there are going to be unintentional disclosures of PHI pick the big issue here is how quickly you identify how quickly remedy it and quickly reported. There's willful neglect and there's not willful neglect so if you've got somebody who should by virtue of not shutting down there workstation or not liking up files that have PHI in them on a routine basis that could be considered not willful neglect but it certainly something that we want to address. One of the recommendations I have for folks is to look at the establishment of some [Indiscernible] and Lieutenant in your organization call them switches folks to help you with the auditing and monitoring of [Indiscernible] practices in your organization so maybe on a weekly basis certain supervisor is responsible for running file the fax machines and department to make sure that there is no PHI left asked overnight that you haven't been the recipient of the PHI because of the styled number should be yours misdialed number that shouldn't be yours. [Indiscernible]

I you do not interested in joining oranges the new black you went to implement the best and most effective HEPA policy and security rules and regulations in your organization. That's a lot of law

that's a lot of legislation that's a lot of how are we going to manage this? The good news is that for the most part most of you are already doing this because it's just good business practice but also because he been required to do so for your contracts at the state unit on aging or with the Medicaid agency or some other covered entity within your state or local areas. One of the things that you want to consider is you moving forward with HIPAA compliance is the establishment again of an environment that emphasizes rocksolid compliance administration. Be documented in policies and procedures what the expectations are who has access to what when it's appropriate to use or disclose it when it's not appropriate to use or disclose it searches your when there is an appropriate use and disclosure of of PHI the strong privacy and security infrastructure training is critical it's not enough just to have policy and procedures and handed to focus need to be able to demonstrate in this is really weren't if you do ever have a violation one of the things OCR will take a look at some credence for you is if you have established a strong and comprehensive HIPAA privacy program your organization that includes routine and ongoing training and communication tier staff have you established a good auditing process in your organization so that your privacy and security officers have contributed to the development of some routine auditing whether it is on a daily basis like pulling information off the fax machine or ensuring somebody walking by and ensuring that all cabinets that contain PHI are locked and secured the end of the business day the reporting aspect failure to report breaches within the designated time constitutes an additional violation of HIPAA privacy the reporting [Indiscernible] is imported FSIS with your staff and others the imported reporting.and there's also timely corrective action how quickly do your work to clear the breach whether it was some kind of electronic failure, whether it was just kind of personnel mishap it's important for you to be able to document in a timely manner identified and corrected the breach pick

---

You need to again embed privacy and security into your human resource administration. Is part of how supervisors will do dishes this stuff should have some provision for staff managing PHI responsibly. The next piece is just the discussion of some more options for you establishment of those privacy and security official role some folks panic and go wait a minute this is an unfunded mandate where my supposed to get the money for hiring a privacy and security officer. In many cases, again your IT CIO could be a designated security officer someone in your personal department might be able to manage your chief operating officer might become your privacy officer. I also encourage the establishment of a compliance committee that includes representatives from your board from your executive team and staff before would help ensure that your in a routine basis reviewing some of the audits and responsibility of monitoring what's happening regarding your compliance with the program and also can make recommendations you. They also can help you Inc. to see privacy regulations. One of the issues that you need to be cognizant of as well HIPAA privacy and security requires at minimum you have to meet the standards it does allow for folks to introduce standard that are on a higher level than the HIPAA privacy and security requirements. States often have more restrictive privacy requirements when it comes to disclosure of information like mental health substance use disorder and other kinds of disability condition they need to be cognizant of that when you're creating your HIPAA privacy policies and procedures . You need to define your organization's expectation about how employees board volunteers and subcontractors are going to adhere to your HIPAA privacy standards outlined in the [Indiscernible] got flexibility to a stop on the hand but the expectation is forever reported violation there is going to be some kind of action by the organization to help provide the care and really stick for compliance. I again would encourage you to always practice

him him necessary disclosure no texting of PHI at all and it's important for you to be comfortable with the fact that not going to know anything all you guys out there guys out there that information for you in the bibliography there also a number of organizations certified organization available on the Internet I can provide you with the standard it will trade for HIPAA . There organizations in some cases when a covered entity has been sanctioned by your by OCR office of civil rights for a HIPAA violation . One of the requirements and the corrective action plan is that they have to post their policies and procedures in a public place maybe on their website so that they can demonstrate that they do have appropriate policies and procedures those are good resources for you.

Will I've also included in this very tiny grade #I believe Steve is also made this available in that resource box for you just some [Indiscernible] quick and dirty [Indiscernible] this is by no means a comprehensive list because again for regulations that span about 800-0900 pages and that's just title II doesn't even cover the high-tech at peace there is no such thing as quick and dirty but it's an oxymoron going to go with this there couple things is you're looking at your own HEPA monitoring and monitoring of your organization have policies and procedures that authorize members of your workforce to access PHI and describe the types of access that are permitted again that's defining has access and what level of access based on their need to use it for their job. Does your organization have formal policies and procedures to support 20 workforce members employment is terminated and/or relationship the business associate is terminated picked this is one of the hot buttons -- folks to get terminated can still access their email or information that has protected health information contained and it will. Somebody is gone there should off immediately and that includes people who maybe on long medical leave should ensure that their access to information is restricted or limited until they're back at work. Same thing goes for when you're terminating a contract with a vendor has been utilizing PHI to transact the business that's defined in your contract ensures they are provisions in your vendor contract that calls for the turning over many hardcopy documentation to you at the conclusion of that business relationship and then provisions for how you expect them not to inappropriately disclose any electronic PHI.
