WEBINAR VIDEO TRANSCRIPT

Partnership for Care HIV TAC

Electronic Health Records, Session #3, Community of Practice

24 May 2016

STEVE LUCKABAUGH: Good afternoon. My name is Steve Luckabaugh, and I'd like to welcome you to the electronic health records session number three community of practice webinar. This webinar is brought to you by the Partnerships for Care HIV Training Technical Assistance and Collaboration Center, or HIV TAC. The Partnerships for Care project is a three-year, multi-agency project funded by the Secretary's Minority AIDS Initiative Fund and the Affordable Care Act. The goals of the project are to one, expand provision of HIV testing prevention, care, and treatment in health centers serving communities highly impacted by HIV, two, to build sustainable partnerships between health centers and their state health department. And three, improve health outcomes among people living with HIV, especially among racial and ethnic minorities. The project is supported by the HIV Training Technical Assistance and Collaboration Center, or HIV TAC.

As I say, we have three speakers today. John Cupples from Couples Associates Consulting began his health career in 1974 as the founding executive director of a community health center in Boston, Massachusetts. After many years in hospital management including Brigham and Women's Hospital, Hebrew Senior Life, and Spaulding Rehabilitation Hospital, he returned to Community Health as a consultant to federally qualified health centers. In 2004, John began consulting with the Massachusetts League member health centers with the objective of getting all Massachusetts health centers live on electronic health records. More recently, he and his consulting associates have focused on supporting health centers through the meaningful use population management and HIPAA compliance processes.

In addition to Massachusetts, John has worked with community health centers and related organizations in Utah, New York, Oklahoma, and California. Our first speaker today is Nancy Tabarangao, who served for over 15 years as a senior manager of a community health center in Boston, Massachusetts. There she was integral in key policy decisions and strategic planning and built a track record in successfully improving efficiency, managing costs, implementing health information and accounting technologies, establishing internal controls, and managing multifunctional team projects to improve internal processes and overall patient service.

Since 2003, Nancy has established herself as a management consultant and has applied her project management skills and technical knowledge to health care organizations with focus on community health centers and private physician practices. Working with all levels within these organizations, Nancy is helping management gain operational efficiencies and establish internal controls for effective management. Currently Nancy is working with organizations to optimize

their utilization of electronic health record systems for clinical quality reporting, care management, and improving patient health outcomes. Her efforts are focused on HIPAA compliance, meaningful use compliance, project management, and workflow analysis optimization. Please join me in welcoming Nancy Tabarangao.

NANCY TABARANGAO: Thank you, Steve, and good afternoon everyone, and thank you for joining us on this webinar. Today John and I will be discussing HIPAA and the requirements for electronic protected health information. We'll start with a general overview of HIPAA and then move to discussion of ensuring the protection of PHI and what could happen if PHI is not protected or secured. Today our topics will cover the overview of HIPAA, which will include discussion of the privacy rule, the security rule, the breach rule, and the patient safety role. We'll also explore protected health information or PHI, ways of protecting PHI via risk analysis, breaches, audit preparation, and state law.

OK, so our first polling question for the day is how many of you have at least met stage one meaningful use? The options are yes, no, you're in the process of actually applying for stage one, or you are not sure whether or not organization complies.

STEVE LUCKABAUGH: OK, if you take a minute or so to answer the first polling question.

NANCY TABARANGAO: Great. Excellent. So this means that most of you on the line actually have probably heard enough about HIPAA and security and risk analysis, but for those of you this will also serve as a reminder, a refresher of what is actually required-- help you think through the next stages of meaningful use. Thank you. The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, was passed by Congress to establish a national frame for security standards and protection of confidentiality with regard to health care data and information. The goal of HIPAA is protect patients' confidentiality while enabling health care organizations to pursue initiatives that further innovation and patient care. Before HIPAA, there was actually no universally recognized security standard or basic mandates to protected this health information, or PHI.

There are four major provisions of HIPAA. The privacy rule sets standards for use and disclosure of PHI. The security rules, that's the technical and non-technical security standards for protecting electronic PHI. The breach notification rule-- that's the framework for reporting features of unsecure PHI. And the patient safety rule protects against increased liability risk when reporting patient safety or health care quality issues. In 2009, privacy and security protections were expanded under the American Recovery and Reinvestment Act, or ARRA. And the Health Information Technology for Economic and Clinical Health Act, are HITECH to promote adoption and use of EHR. In the following pages we will provide more detail on HIPAA, but our focus today is on the privacy and security rules which provide the requirements you must follow to ensure data, security, and integrity of e-PHI.

In the second half, we will further discuss our requirements of the speech rule. Under the HITECH Act, rules were established for ensuring protection of e-PHI and assessing security risk

and establishing policies and procedures for protecting e-PHI became core requirements of the EHR Incentive Program and meaningful use. It is worth noting that the audit [INAUDIBLE] meaningful use program sets as a goal that one in four eligible providers participating in the program are to be audited. So far, the primary reason for negative findings has been the failure to comply with HIPAA. And that HIPAA compliance is more closely scrutinize. Sanctions may be and have been imposed for non-compliance.

As just discussed, there are currently four major provisions of HIPAA. the Health and Human Services Office of Civil Rights, or OCR, is responsible for administering and enforcing these provisions. The HIPAA privacy rule protects the privacy of individually identifiable health information or PHI by establishing standards for the use and disclosure of PHI, as well as standards for individual's privacy rights to understand and control how their information is used. The HIPAA security rule establishes a national set of security standards for protecting certain health information that is held or transferred specifically in electronic form.

The HIPAA breach notification rule requires covered entities and business associates to provide notification following a breach of unsecured protected health information. And finally, the confidentiality provisions of the patient's safety rule protects identifiable information being used to analyze patient safety events and improve patient safety. On February 17th 2009, the HITECH Act was signed into law. Through this act, the scope of privacy and security protection under HIPAA were broadened. The HITECH Act was an act of the [INAUDIBLE], as discussed previously, to promote the adoption and meaningful use of health information technology. And it addresses the privacy and security concerns associated with electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rule.

Under the HITECH, that the EHR incentive program was established to provide incentive payments to eligible professionals, eligible hospitals, and critical access hospitals to adopt, implement, upgrade, and demonstrate the meaningful use of certified electronic health record technology. This includes the core requirement to protect the e-PHI as of stage one. This graph depicts the major stages of progression of the meaningful use program, beginning with the HITECH enactment in 2009, initiation of meaningful use stage one in 2011 which focused on capturing and sharing data, progressing to stage two in 2014, which focused on advanced care processes with its decision support, and the introduction of stage three in 2017, which will focus on improved outcomes.

As we move to the HIPAA privacy security rules, you will see that the two go hand-in-hand. The security rules operationalizes the protections contained in the privacy rule. By addressing the technical and non-technical safeguards that organizations called covered entities was put in place to secure individuals' electronic protected health information, or e-PHI. On the one hand, the privacy rule focuses on the right of an individual to understand and control the use of his or her personal information. PHI should not be divulged or used by others against an individual wishes. It also covers the confidentiality of PHI in all formats, including electronic, paper, and

oral. And it assures that PHI will be safeguarded from unauthorized disclosure while allowing the flow of health information to provide and promote high quality health care.

On the other hand, the security rule focuses on administrative, technical, and physical safeguards specific to e-PHI. It protects e-PHI that is created, received, used, or maintained by a covered entity. This includes e-PHI that external or internal, stored or in transit. It also promotes the integrity and availability of e-PHI. Integrity meaning e-PHI is not altered or destroyed in an unauthorized manner, and availability being that e-PHI dot acceptable and useful on demand by an authorized person. In summary, the security rule focus on electronic PHI an assurance that PHI is safeguarded at all times.

The security rule establishes standards for protecting certain health information that is held or transferred, again, an electronic format, such as an EHR. A major goal of the security rule is to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. Covered entities under the security rule include health plans, health care clearinghouses, and any health care provider who transmits health information in electronic in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA. The security rule covers requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the e-PHI.

Specifically, covered entities must ensure the confidentiality, integrity, and availability of all PHI that they create, receive, maintain, or transmit. They must identify and protect against reasonably anticipated threats for the security or integrity of the information. They must protect against reasonably anticipated impermissible uses or disclosures, and they must ensure compliance by their workforce. In addition to the e-PHI safeguards required by covered entities, covered entities must obtain assurances from business associate. Business associates will appropriately safeguard PHI. Business Associates are persons or entities that perform functions or activities that may involve use or disclosure of PHI on behalf of the covered entities.

In other words, business associates are held to the same standard for protection and security of PHI. So this concludes the first half of our presentation. Before we move on to the second half, we can take a few minutes for questions.

STEVE LUCKABAUGH: OK, if anyone has any questions, please type them into the questions pane in the GoToWebinar toolbar. So what security must be observed if data containing PHI is shared with state or local health departments?

JOHN CUPPLES: This is John Cupples. Welcome everyone. The first one is that this involves transmission of protected health information. And the first key thing is that it be transmitted in a secure fashion, and that usually means encrypted or mailed. Mail is considered to be a secure means of transmission. But if it's electronically transmitted, it must be encrypted and there are several ways to do that. Several. And so that's it. A problem or an issue that your IT department is undoubtedly familiar with. But it should be encrypted before it leaves your practice, your

health center. And the keys to unecrypt it would have to be also transmitted to the health department.

And if there's not an agreement with the health department, it varies state by state what health departments can accept as PHI. Talk a little bit more about that in the third section of this presentation when it comes to HIV data. So it gets a little more complicated. We're only talking about federal law so far, and we will refer to-- but basically, it has to be transmitted in a secure format, and that means encryption or via a secure email connection or health information exchange.

STEVE LUCKABAUGH: OK, thank you. I'm not seeing any more questions, so maybe we should move on.

JOHN CUPPLES: So I will continue from this point forward, and we're now going to focus a little bit on what one of the elements of what qualifies protected health information. And basically, as a practical matter, any information that's in an electronic form or paper, or any form of health information system, whether it's paper or electronic that could be used to identify an individual. [INAUDIBLE] the regulations of HIPAA clearly state that for persons who might be easy to identify because of their age, the restrictions get more stringent. For example, anyone over 85, I believe, the zip code has to be deleted.

So these are some common examples. You can see there's common identifiers that all medical practices collect. And any of these clearly qualify as protected health information. In addition, for persons-- elderly persons-- there are additional restrictions on what can be divulged in terms of data [INAUDIBLE]. But this gives you, basically, a good idea of the first things to look for. There are also rules for de-identifying data that should be looked at if you're going to share information for research purposes or with another agency that's not covered a covered or with whom we do not have an agreement.

So basically there are some exclusions. Employer records are excluded unless the employee is a patient, and everything in the medical record becomes protected health information. And education records are also carved out from coverage under HIPAA. They have their own restrictions, but not under HIPAA. We will go to our next poll, which is has your health center been audited for HIPAA compliance? Again yes, no, you're in process right now, or you're not sure.

STEVE LUCKABAUGH: OK, if you'd like to take a minute or so here to answer the poll question, has your health center been audited for HIPAA compliance? Yes, no, in process, not sure?

JOHN CUPPLES: So 25% have been audited which goes along with the national guidelines. 42% not, and I would say most states are still mobilizing to get this done under the Medicaid EHR Incentive Program. Medicare has been more aggressive about its auditing process and it's a few years into the process. And if you're not sure you probably have not been, because you would certainly have heard about it. HERSA also does a quick and dirty audit relating to compliance

with meaningful use and HITECH requirements and HIPAA requirements. So under the security rule, in addition to just being responsible for protecting PHI, you're also required to document that you've carried out certain processes and have instituted those in your organization, including a risk analysis and a management process to ensure that you're managing all the risks related to the protection of protected health information.

And those include administrative factors such as staff education, policies and procedures. In addition there are physical safeguards. For example, restriction on the access and entry to your facility and on the part of your facility that houses your electronic health information record system. Very tight requirements on access and logging of activities in that area. And then finally technical safeguards. You've all experienced that with passwords and that kind of thing, so requirements for levels of technical proficiency including firewalls, that sort of thing. So three major categories of safeguards that go into your risk analysis and management system.

Obviously organizational requirements and policies and procedures have to be well documented, and that's the first thing-- one of the first few things that any HIPAA auditor will look for. So the first thing, obviously, is to make sure your policies and procedures are in place. That's the first piece of documentation that will be looked at, and that they are reviewed on a periodic basis. Annually is a good rule for compliance with the HIPAA security rule. We recommend in constructing your policies and procedures that you actually tie every policy and procedure to one of the HIPAA requirements by direct reference so that there's no doubt that you have complied with every element of HIPAA.

And the other thing that's critical is to conduct periodic risk analyses. And this has been the major reason for failure in audits that have occurred up to this point. This either lack of policies and procedures or documentation that risk mitigation efforts have been put in place and examined on a periodic basis.

So a third poll-- does your health center conduct a security risk analysis at least annually? Yes, no, or not sure?

STEVE LUCKABAUGH: OK, if you'd like to take a moment to answer our third poll-- does your CAC conduct a security risk assessment at least annually? Yes, no, or not sure? We had a question that came in, I don't know if you want to take it. How does HIPAA apply to the deceased?

JOHN CUPPLES: Well, complicated. Generally, it does not. At that point a person's record is not considered a major problem now. That being the case, that data is still very-- some of that data is still worth a lot on the street, so it needs to be properly archived and set aside. And a lot of states have strict rules about archiving records for a significant number of years beyond the termination of care for that patient, whether it's caused by death or the patient resigning from care. So you're still responsible. And those records can-- even though they're in archive, could be considered value.

On the street they have value for false ID and medical fraud. I would as a practical matter they should be covered with the same security as active patients until they're beyond the expiration date that is set by your state.

STEVE LUCKABAUGH: OK, thanks. We have our poll results here.

JOHN CUPPLES: Oh, good. So this is good. Hopefully for those that are not sure, it's a good question to ask. Because if you're not sure or if you're in the no category, that's a vulnerability to HIPAA or HERSA, for that matter-- audit. So as I said earlier, a security risk analysis must be conducted annually, or if a security incident occurs in addition to the annual security risk analysis. An analysis should include, again, a review of your-- the three categories of administrative, physical, and technical safeguards. Documentation of your findings, if there were an incident of documentation of that particular incident, and a plan to mitigate the risks caused by that incident, and documentation that you're maintaining continuous, reasonable, and appropriate security protections.

For example, that your firewall, a very basic one, is in place and operational. That your-- or another one that's overlooked a lot is that your operating systems are up to date. You're not still using XP, for example, from Microsoft. Are you using the latest versions of everything? Let's talk a little bit about breach. And you'll see as we go through these slides that this is a key issue. Everyone is jumping all over this one because the breaches are basically out of control right now and the bad guys are winning. And you'll see some statistics to that affect. So a breach is any disclosure of information or invasion of the information but that's information that compromises the security or privacy of protected health information.

All breaches must be reported to a CMS. A breach of an individual record, for example, must be dealt with within a 60-day period and doesn't need to be reported until the end of-- after the close of the calendar year, no later than 60 days after the close of the calendar year. For breach of more than 500 records, which, for any health center is going to be the case if the system is breached, that has to be recorded within 60 days to HHS. In addition, a breach of that magnitude has requirements about public notification and notification of all the individuals involved. There is a process defined in HIPAA about how to respond to a breach and the steps that must be taken.

The first one in this graphic details this. The first issue is to determine whether it was a valid incident or not in fact, was there an actual breach or not? If so, what is the nature and extent of the breach of the private health information? And if the disclosure was made, say, to another covered entity like a business associate or other medical provider, that's of lesser concern that if it were made to somebody else or another patient and whether the PHI was actually viewed, acquired, and used. So all those go into determining the extent and risk of the breach. And then whether notification is required or not, just depending on the size and the extent and risk involved in breach.

So not every breach rises to the level of being reportable. For example, if a staff member sends a Excel spreadsheet with a PHI on it to a business associate via secure email, that may be a violation of health center policy, and it is an incident that should be investigated, but it may not rise to the level of a reportable breach. Our fourth poll is does your health center conduct annual HIPAA privacy and security staff trainings? Yes, no, or not sure?

STEVE LUCKABAUGH: OK, we'll take a minute here for your fourth poll. Does your CHC conduct annual HIPAA privacy and security trainings? Yes, no, or not sure?

I want to thank everyone who's answering these poll questions. Helps us get a good idea of what's going on.

JOHN CUPPLES: Ah, terrific. Great. I like to see this. And you'll see in the next slide why. The CMS maintains a significant database on what they call their wall of shame. And you can look this up yourself. You'll find the link on the slide. In 2015 there were 268 breaches that involved 500 records or more for a total number of records breached of 113 million, over 113 million. Just to put that in context, that's about one in three Americans had their records breached. And most of those-- and this is the other piece that I found sobering-- and this is something new, in 2015, 111, almost 112,000 of those records were breached by intentional outside hacks. That is to say, people who were intent on hacking health record systems in order to gain the information for whatever use, usually to make money on the sale of that information.

The other causes of theft were minor by comparison, which included actual outright theft by any means, unauthorized access, improper disposal-- the example given was a pile of paper records found in a municipal dump and then otherwise just lost on the part of staff-- lost records. So the key, when you look at this over time, the trend is clearly moving in the direction, and this exemplified in 2015, that hacking by outside sources, well organized sources, is on the ascendancy and is the dominant mode of breach. So having technical and staff training to prevent hacking is critical at this stage in the technology.

Along with the growth and loss of medical records to breaches has been the effort by HIPAA by CMS to enforce HIPAA. And you can see in this graphic and in this slide how that's progressed over the years. HIPAA number of cases investigated has gone from 13, 1,400 in 2004 to almost 450,000 in 2013, and the percent of corrective action, which means fines, has also gone up along with that. Average fine is running between $1,000 and $1,500 per record breached. And so you can see that losing or having 10,000 records breached in a hack of your electronic health record system would be extraordinarily expensive, and a lot of health centers have resorted to purchasing breach insurance.

The key takeaway from this slide is that you're responsible for documenting an adequate documentation if the office of civil rights or Medicaid, the EHR Incentive Program, comes to audit. And there is a six year look back on any item that the auditor might decide to audit. So getting your audit in place is absolutely critical. The other key requirement here is-- a complication, I should say-- is that state law varies from state to state. So it's important-- each

state has its own requirement. And I would urge you to Google your state privacy law as a place to start.

And in some states-- many states-- the privacy laws and rules exceed those of HIPAA, so you might well be subject to even stricter terms and conditions, or at least those that vary from HIPAA. If you would, please, that would be something I would suggest. So next slide, which is three sources, gives you some links to websites that are important for HIPAA understanding, and I would urge you to Google the link to the first one, in particular, which is an overview library of HIPAA information, and then again, also Google your state privacy law to make sure that you're compliant with that.

And one little note, I would make sure that in your policies and procedures you acknowledge that part of your intent is to comply with both HIPAA and your state [INAUDIBLE] policy with regard to privacy. That concludes my presentation, and thank you for your attention.

STEVE LUCKABAUGH: OK, and we have a minute here. We can take a couple questions if we have any. We did have one. Is it considered secure transport if you're uploading data to an SFTP portal but are not encrypting the file before submitting it?

JOHN CUPPLES: It has... and this is something that I'm not an expert in, but I know that technically it's not considered as secure as encrypted transmission or secure email services, which are also encrypted. So FTP has fallen out of favor and one of the first places that it's very useful for large files, but it's not considered-- as I understand it-- as secure as other means. So that's something you would need to check with your IT department on, but I know that from case studies, that's one of the first places that an investigation will begin, is what happened with it FTP? Was that a source of the breach?

DIANA ERANI: Question if I could-- John, do you know if-- I was just struck by the fact that you were talking about disclosure records as a violation. If you have a conversation-- I know in hospitals they obviously say, and even health centers don't talk about patients on the elevator. So I just want to reaffirm that it's-- is it also verbal? Because I honestly-- I won't disclose where, but I was on a meeting today where the chair of the meeting talked about his wife's health condition. And I really realized afterwards, besides that it wasn't appropriate because his wife wasn't in the room giving permission, it was really not appropriate. It wasn't like a personal-- it was-- Yeah.

JOHN CUPPLES: The wording is in any form.

NANCY TABARANGAO: Under the privacy rule.

JOHN CUPPLES: Yeah, in any form. So yes, talking casual or otherwise-- paper, electronic, video broadcast, anything would be covered.

DIANA ERANI: And so that would also mean, too, that you have to not let your guard down. Like you're giving a personal example, you should mask-- you could certainly reflect on a personal example of a health care experience, but you need to still retain some sense of confidentiality of the PHI related to it.

JOHN CUPPLES: Unless you're doing it yourself.

NANCY TABARANGAO: Right, yourself.

JOHN CUPPLES: Yes.

NANCY TABARANGAO: Or unless his wife gave him permission to discuss it.

DIANA ERANI: Right, which wasn't said, so it's...

JOHN CUPPLES: And document it. OK, thank you.

STEVE LUCKABAUGH: All right, our next speaker is Diana Erani, who has spent her career focused on health care operations and management. She's been serving as director of the Massachusetts League of Community Health Centers health center control network, HCCN, since 2013, leading resources supporting the use of data to support quality improvement and primary care and a number of initiatives with the Massachusetts Department of Public Health. Diana is committed to coordinated care and works directly with health information exchange and strengthening e-referral options with community-based organizations to improve coordination of care. She brings a strong commitment to access and coordination of care strength in her role as COO for Baylor College of medicine And Health care of the homeless program at a federally qualified health center in Houston, Texas. In this role she oversaw the implementation of EPIC and data reporting. Please join me in welcoming Diana Erani.

DIANA ERANI: Hello, and good afternoon, everyone. This afternoon I'll be speaking about specifically the transmission of HIV data, and I'll be speaking about the practices in Massachusetts. I realize that not everyone listening is practicing in Massachusetts, but Massachusetts has some of the most restrictive laws in the country so it might be interesting to learn about what we're doing here. For specific questions you would have to contact either an attorney in your state or your state health department for your specific information.

OK, so we just finished talking about HIPAA and now we're going on to the state laws. But how do you know which one to follow? So it depends. If the HIPAA law, which is a more broad federal law, or the state law, which can be a more specific law, you follow one that is more protective of privacy. So in the case of Massachusetts, the state law is more protective of privacy. So that state law will preempt the federal law. OK, here, in case you want to look them up, just to kind of Google why you're doing this-- to check. The HIPAA laws are codified for PHI under 45 CFR, and the Massachusetts laws are codified under mass general law 111.

So here we go. It starts with HIV testing. And I'm not going to read it exactly verbatim. But basically, a health care provider need to do three things when they're testing someone for HIV. First of all, they must get their verbal, informed consent. And second of all, they may not disclose the results of any test without getting the patient's written informed consent. And third of all, they have to identify the subject of such tests to any person without first obtaining their written informed consent with the purpose of the use of that information. So you have to first sit down with the patient and explain, getting their verbal and informed consent, get it in writing and explain the purpose of why you need this information in writing.

And it has to be distinguished from any other medical consent. So that means for practical purposes, that you can't combine it with any other medical consent form. You can't put it just as language in the body of the HIPAA form unless it is separated by something such as a black box-- is what most people do here-- or a separate page. It can't be just a paragraph in the body where people sign at the bottom. It's going to require a separate signature that is easy to distinguish. The exception for this is the Massachusetts Department of Public Health. The State Department of Public Health is allowed to see HIV data.

And it's only the State Department of Public Health. It's not local health department unless there is some sort of legal exception to that. So if you have a state health department, a county health department, and another local health department, such as the city health department or townhouse department-- and some places have more than one in their locality-- it is the state health department that has the exception to most [INAUDIBLE] and also HIV data in Massachusetts where they can see person-specific HIV data. Back to the written consent for the HIV testing. The written consent must be obtained for each requested release of the HIV test results. So again, this is different than HIPAA.

When you sign a HIPAA consent form, that's usually good for a year, and you usually have the date on there and it usually says good until one year from now. But with an HIV test or anything that indicates someone's HIV status, it is only good for one disclosure one time for each time that you disclose their HIV status. The only break you get here is the law doesn't specify who can obtain this release. It doesn't have to be their physician, in other words. It could be anyone in the office. It could be the office staff or a clinical person presenting the person who's receiving the test with the paperwork. So this is a little bit helpful when you are coordinating care or if you're trying to get a social benefit for someone who is HIV positive. It could be a social worker or a case manager or a community health worker that goes ahead and obtains this consent.

The Massachusetts Department of Public Health strongly recommends the use the distinct and separate HIV test results within the general consent document. Like I said before, using that black box. But you also have to state to whom and to where the test results will be released. If you're sharing this information within the same health entity where the person is being treated-- for example, if they're being treated at hospital a and they have both their infectious disease doctor and their primary care doctor in the same hospital, then you do not need to do this. But if you're sharing the information between Dr. Smith at Neighborhood Community

Health Center and hospital A, then you must specify that the HIV result is going to Dr. Smith at Neighborhood Community Health Center on each release of the HIV data.

So what is this HIV data that we're talking about? It's anything that indicates someone's HIV status. So obviously you think of laboratory data, but it's not only the specific laboratory data that's HIV, it's anything related to the HIV in any different type of lab. It's not just yes or no, do you have the virus? It's a medication list of someone that may take medication that someone with the virus would take. It is an allergy list in case they're allergic to one of those medications. It's appointment information in case they have an appointment at an infectious disease facility or with a clinic that traditionally treats HIV.

Its insurance information, and of course it's social history. So what does this all mean for the grant? That HIV data can and should be reported to the Massachusetts Department of Public Health as a condition of participating in the grant as was specified for the people in Massachusetts. That it should not be transmitted for purposes without the written consent of the patient, and that this consent must include the purpose of the transmission and to whom the data will be transmitted each and every time it is shared outside of the health entity. And finally, I did state the obvious, but the privacy laws make care coordination more cumbersome for HIV patients.

But it is the law in our state, it was designed for their protection, and we must be careful to follow it each time. Does anybody have any questions?

NANCY TABARANGAO: So Diana, on this are you saying that for HIV data you to the Department of Public Health they don't need to get consent?

DIANA ERANI: Correct.

STEVE LUCKABAUGH: OK, we can take some questions here if anyone has any questions. Cindy Cabales wants to ask a question. I'm going to unmute her phone. Go ahead.

CINDY CABALES: Yes, this question is, again, begs the topic of future transmission. And I appreciate the answer about the SFTP protocol. That's very helpful to know. In addition, we have to also report certain HIV data to city funders from the Baltimore City Health Department. And in some cases it's our understanding that they are now requesting data that includes PHI where we have the option of loading the data to a CD and then either hand delivering it or mailing it to the Baltimore City Health Department.

If we opt to report the HIV test data that way, how should we go about securing the CD, or do we need to clear that with the Baltimore City Health Department first? Thank you.

JOHN CUPPLES: I think the best practice would be to encrypt the CD and send the keys separately or securely to the Department of Public Health or whatever that government agency is. So again, taking best practice precautions, it would be generally recommended in a situation

like that. If for some reason that CD were lost or went astray, it would be considered breach if it were not encrypted. It would be considered breach in any event, but under the guidelines you could-- as soon as you said that it was encrypted, you're fine. You're covered. So I would say encrypted.

CINDY CABALES: Great. Thank you. I have one more question. So the next question, just to summarize, in general it's ideal to encrypt a file before you transmit it regardless of the transition process unless you have a secure HIE. The next question, then, is with regards to HIV data and the relationship we have with public health reporting, I'm a little bit confused on the point with regards to HIV data. I understand that for surveillance purposes the state needs to understand things like identifiers, names, dates of birth, HIV status. We have another agency-- a local agency-- that's also asking for information about last CD4 count and last kept appointment and the next kept appointment.

How do we know if that's actually permissible, or what would determine if that goes beyond what's required in terms of our disclosure?

DIANA ERANI: There should be some kind of agreement or some kind of legal agreement that you could ask them to show you to make sure that it's OK to send them that kind of information. They're probably making sure that the patients are in care, or if they're not in care that they become in care, but they have to have the authority to ask that. So that they should either have some kind of ruling that gives them the authority, but you can ask them for it if you're not sure.

JOHN CUPPLES: And on your end, the documentation to demonstrate that you released it in a way that was permissible under HIPAA and whatever your state privacy law is.

[INTERPOSING VOICES]

CINDY CABALES: I'm sorry. To your point, in terms of a requirement, is a grant-- basically an agreement through a grant funded project sufficient, or do we have to actually look for more like a state statute or something?

JOHN CUPPLES: That sounds like it's treading on legal opinion. I would get a legal opinion before proceeding too much further.

NANCY TABARANGAO: I would also add that it would also be dependent on what are they asking for. Are they asking for aggregating numbers? So you have 50 HIV patients and some of them have been tested, or they actually asking for patient level identifiable data?

UNIDENTIFIED PARTICIPANT: They're asking for patient level for CD4 last appointment and next appointment.

UNIDENTIFIED PARTICIPANT: And that certainly requires some legal advisement.

CINDY CABALES: OK, thank you.

STEVE LUCKABAUGH: OK, if anyone else has any questions--? Up on your screen right now is the registration link for session number four. If you would like to write that down real quick and we can get yourself registered for session number four, which is Tuesday June, 28th at the same time. I'm not seeing any questions here. If our speakers have any closing thoughts?

JOHN CUPPLES: It's been our pleasure.

UNIDENTIFIED PARTICIPANT: Thank you very much.

STEVE LUCKABAUGH: OK, I'd like to thank you for participating in today's webinar. We hope that you're able to find the information provided useful as you continue your P4C project and ask that you take a few moments to complete the feedback survey that you will receive when you close out of this webinar. You also receive it via email. Today's webinar was recorded, and the audio and video versions of the entire webinar, are as well as the slides from today's webinar, will be available on the P4C website within the next few weeks. Copies of our prior P4C webinars are currently available on the website on the P4C Resource Materials page at http://www.p4chivtac.com You will need to log in to access materials. If you need login credentials, send an email to be p4chivtac@mayatech.com.

Thank you again for participating in today's webinar, and thank you to our presenters for those excellent presentations. If you have any additional questions for the P4C project or for any of our presenters, please email us at p4chivtac@mayatech.com. Take care, everybody, and we'll see you next time.