JSI RESEARCH & TRAINING INSTITUTE, INC
DATACHATT WEB CONFERENCE

# HIPAA and Data Sharing: Part II
# Denise McWilliams, AIDS Action Committee
# July 24, 2008

## TRANSCRIPTS

**Operator:** Ladies and gentlemen, welcome to the dataCHATT Technical Assistance web conference sponsored by HRSA HIV and AIDS Bureau. The topic for this afternoon's session is HIPAA and Data Sharing. Please note that this session is being recorded. During the presentation the phone lines will be muted. After the presentation we will then open the lines for questions. At this time I will hand the call over to Mira Levinson. Please go ahead, ma'am.

**Moderator Mira Levinson:** Thank you, and hello everyone. Welcome to today's call. This is the second web conference through the Ryan White Data TA and Training Cooperative Agreement. I'm Mira Levinson, Project Director for the Data TA Center and I will be the moderator for today's call.

The topic of today's call is HIPAA and Data Sharing, Part II. Part I provided an overview of HIPAA, the Health Insurance Portability and Accountability Act, and the types of entities and transactions that are covered by it. Today we will focus on the types of information that are covered by HIPAA and the impact of HIPAA on data sharing practices, such as data collection, data management, and RDR data reporting.

If you haven't already please download the materials for today's call. The document you'll need for today's call is the same as the one from the Part I call. Our speaker will be referring to specific sections of this document during today's call so you may find it helpful to print out a copy and mark it up with your own notes and questions or to reference the presentation, particularly since the text as referenced on the slides is small.

The links for getting those documents appeared on the original registration page, and they'll also be posted on our website, dataCHATT. You'll see [the address] in the lower right-hand side of the slide, that's www.datachatt.jsi.com. There will also be an archived version of the last call and one of today's call as soon as that become available.

Our presenter, Denise McWilliams, joins us from the AIDS Action Committee of Massachusetts. She was also the presenter for the first call. She has spent more than twenty-five years working to improve the lives of people living with HIV/AIDS and has litigated precedent-setting cases in discrimination, privacy, and access to treatment. She has engaged in successful lobbying campaigns on both the state and federal levels seeking to secure the rights of and necessary benefits for people living with HIV/AIDS; and she currently serves as General Counsel for AIDS Action.

Following Denise's presentation we'll have a question and answer period. If you have questions at any time during or after the presentation you may type them into the “Chat” Box on the right-

hand side of your screen. Those questions will be addressed during the question and answer period. After the presentation is finished you can also, if you prefer, dial the operator to ask your question by phone.

Before we begin I want to remind you that you are all in listen-only mode so you don't need to mute your individual phone lines. If you have any technical difficulties during the conference today you can dial “one, four” to reach the operator or just type your problem into the “Chat” box, as people are already doing, on the right-hand side of your screen. Now I'm going to turn it over to our presenter. Denise, please go ahead.

**Ms. Denise McWilliams:** Good afternoon, everybody. Today we're going to focus a little bit more specifically on the impact of HIPAA on the reporting of client-level data to HRSA. There are two things I want to say in advance. First, again, this is a general overview, this is not legal advice. This is in no way a substitute for consulting with an attorney who is licensed to practice in your own state. Secondly, HIPAA creates a floor. HIPAA is the minimum requirement that you have to adhere to actually respect your clients' privacy. Many states have more stringent privacy protections, and the more stringent protections need to be looked at to see whether or not they are preempted by the Ryan White CARE Act. Those are the two general caveats I want to give to you.

As you might recall from the first call, HIPAA doesn't just apply across the board to everybody who holds onto any sort of personal information. The first question to ask is whether or not the entity holding the information is what's called a *covered entity*. That's a three-pronged test. If you look at page four of the handout from HAB, which is the "Protecting Health Information Privacy and Complying With Federal Regulations" you'll see that the three-part test is: one, is the person or organization considered to be a health care provider?; two, does the person or organization conduct public transactions?; and three, does the person or organization transmit health information in electronic form in connection with any of these transactions? If the answer to all three of those questions is yes, you are a covered entity.

The next step of the analysis is whether or not the information is protected health information. Again referring back to the document I just referenced—which I won't reference again because the name is way too unwieldy—you'll see, on page six, that protected health information is health information that is individually identifiable and is created or received by a covered entity. If you're thinking that's a little circular you're correct, it is. But that's the step you must be going through when you're making these determinations.

The major part of our discussion today will be on the use and the disclosure of protected health information. That is covered under a section of HIPAA that's called the "Privacy Rule." The privacy rule is the standard that directs the circumstances and the conditions under which PHI can be used and can be disclosed. Now, there are a couple of different ways to think about this. The way in the pamphlet I'm going to be referring to is, I think, the easiest. They speak in terms of required disclosure and permissive disclosure.

Required disclosures are the disclosures that the privacy rule requires. Those are to two basic places, one of which is to subject individuals. In other words, if we're talking about my health

information and I want it, I get to see that with a few very specific exceptions. Secondly, the statute requires that reports be made to the Office of Civil Rights of the Department of Health and Human Services to ensure compliance with HIPAA. Those are required disclosures. They do not require authorization.

Permissive disclosures are disclosures that the subject individual must authorize unless the use and disclosure is permitted by the privacy rule. If you look at page fifteen of the document that will give you much more detail about what these disclosures and uses are. They are, for example, the first one is the treatment and health care operations. You may use and disclose protected health information for this without the person's individual authorization. You can also use it under the public priority purposes of—skipping ahead to number three; and the number two, uses and disclosures to which the subject individual can agree or object. What that means is not that the person has to do so in writing, but that before the information is used, the individual has to be given an opportunity to agree or object and this can be done verbally.

The third category is public priority purposes. Those can be found on page sixteen of the information. That refers to things such as public health reporting, public health oversight, and use and disclosure required by law. I'm sorry, let's go back to treatment and start from there. I apologize for this. If you turn to page fifteen you are going to see the treatment options. They deal with the provision for coordination of the management of health care related services by one or more health care providers. That includes management by a provider with a third party, consultation between providers, and referral from one provider to the other. As you will see, you do not need an authorization for each and every one of these disclosures.

Second is payment. That's the information a provider must send to third-party payors to receive reimbursement. Again, that is not information that requires specific authorization in advance. Health care operations includes, but is not limited to, quality assessment and improvement, performance reviews, resolution of internal grievances, as well as some fund-raising activities. The individual can agree or object to the inclusion of the patient's name in a facility directory—by that they mean those indexes you can call and ask for the consideration of a particular patient—disclosure to family members, and certain notifications that have to be made, such as death notifications. If you want a complete listing to see some of the most commonly-occurring episodes please take a look at 45 Code of Federal Regulations, §164.510 for the complete listing; and also take a look again at page fifteen for a little bit more explanation of what I just said.

The public priority purposes is the situation that I talked about briefly earlier. They include, but are not limited to, the uses and disclosures required for health oversight and correct public health purpose. For example, in Massachusetts under some circumstances a mandated reporter would be required to report information that would otherwise be considered to be PHI if the subject individual poses a direct threat to somebody else's well being. Most states have similar sorts of provisions. For health oversight it would be situations such as quality assessment, quality management, and compliance in areas of contractual relationship. For a public health purpose it's typically the situation for things like contact tracing, disease reporting, etc.

All other disclosures require authorization; and those authorizations must be written in plain language, it has to describe the specific information to be disclosed and/or used, and it has to

identify the recipient of information. The authorization must contain an expiration date and it must also describe the subject individual's right to revoke the authorization in writing.

As we all know, client-level data will soon be required by HRSA before receiving Ryan White funding. There are three separate ways to think client-level in connection with HIPAA. They are as follows: that it is permitted because it's a health oversight or a public health purpose; it is a limited data set; or de-identified information.

Regarding health oversight or public health purpose, we spoke a bit earlier about health oversight being things such as quality assurance. Public health purpose would be linking people's health outcomes with the various services provided. Under either of those categories HIPAA would likely allow the reporting of client-level data. Secondly, it's a limited data set. For a limited data set for HIPAA purposes is a set that has not been completely de-identified, but certain identifiers have been removed from the report.

The de-identifying information is probably, I think, the one most likely to be applicable here because HRSA is putting a great deal of time, energy, and resources into developing a unique client identifier to be used in connection with this sort of reporting.

What de-identify technically means is that all information that could identify an individual has been removed, coded, encrypted, or otherwise eliminated from PHI. This doesn't have to be perfect. It does not have to be a code that can never be broken under any circumstances. Folks frequently go to that standard when they're looking at computerized electronic reporting. What you need to keep in mind is that even in the times when we were just using paper files there were always ways that paper files could be inappropriately used: people don't want file cabinets, file cabinet keys are missing. It doesn't have to be a perfect system. What it has to be, though, is a system where documented methods established that there is a low probability of un-identifying an individual. No way am I qualified to speak to the technical aspects of the code that HRSA is using except to say that, as it has been described to me, it seems likely that it would, in fact, be shown to give a low—in fact, a very low—probability of identifying an individual.

Again, I would urge people to consult with their own technological consultants as well as their attorney to confirm that that is, in fact, true when their finished product is put out for use. Remember that this is a broad overview of the topic. It's important to consult an attorney to look at your individual situation because you don't just have to worry about HIPAA. You have to worry about your state laws and your state regulations. Also keep in mind that although there might be state laws that would go against this sort of procedure it frequently is a requirement of your contract, and you can contractually agree for different things. This is why it really is key to find your own attorney with whom to discuss these things.

**Ms. Levinson:** Thank you very much, Denise. We are going to move on to the question and answer session in just a moment. Before we begin I want to take a moment to tell you about a few announcements.

First of all, if you haven't already, please download or order the resource guide that Denise has been referencing. Information about how to download or order copies can be found on our

website, again you can see it in the lower right-hand corner of your slide, www.dataCHATT.JSI.com.

As I mentioned earlier, an archived version of Part I of this web conference is already available on the dataCHATT website and a "Frequently Asked Questions" document is coming soon. If you'd like, you can pass that along to your colleagues if you would like for them to be able to hear the Part I of this session. As soon as it's available we will post an archived version of today's presentation. The "Frequently Asked Questions" document will summarize questions from both Part I and Part II of the web conference.

The next web conference in this series, which will probably be in late September, will focus on using contracted providers' data for ongoing program management. Once the date and time is set the call will be announced in a HAB Information e-mail and on the dataCHATT and TARGET Center sites; registration will be available through the TAGET site, as well.

Now we're going to begin the question and answer session. As I mentioned earlier there are two ways to ask questions. You can type your question right into the “Chat” box on the right-hand sided of your screen or you can ask your question by phone. The operator will now give instructions for dialing into the telephone queue. While we're waiting we'll take some questions from the “Chat” box and also from the registrations that have come in before the call. Operator?

**Operator:** Thank you. Ladies and gentlemen, if you would like to register a question please press the one followed by the four on your telephone. You will hear a three-tone prompt to acknowledge your request. Your line will then be accessed from the conference to obtain information. If your question has been answered and you would like to withdraw your registration you may press the one followed by the three. Once again to register you need to press the one followed by the four. Please go ahead.

**Ms. Levinson:** Thank you. As a reminder we're going to focus our attention on HIPAA and data sharing on today's call. A discussion about operations and HIPAA will be presented as part of a separate call later on in the fall. We have some questions that came in as part of the registration process for the Part I call and also a couple for today's call. Denise is going to now take a few of those. We were able to address most of them last time, but as you know we tabled a few for today. Go ahead, Denise.

**Ms. McWilliams:** The first one I want to address is the question about whether a client release of information is required if sharing data among the parties for the purposes of quality management. Again, most likely the answer to that is, no, it's not because that would fall under the category of health care operations, which would be a permitted disclosure for which it is not necessary to get individual authorization.

The next question is: We have sixteen providers on a server. If they want to share data amongst each other does each client have to sign a consent form for them to share that client's information? I'm assuming that the sixteen providers are all separately incorporated organizations. With that assumption I would say, yes, they do have to get a consent form for the

purposes of sharing that client's data, assuming that it is for the purposes of services and doesn't fall under one of the other exceptions.

Next question: Is it necessary to obtain patient authorization to share clinical data every time you refer a patient to another provider for treatment? No, that falls, again, under the treatment payment and health care operations permissive use and disclosure to which you will reference on page fifteen of the document; and individual authorizations are not necessary for releasing information for the purpose of affecting a referral.

**Ms. Levinson:** We have a few questions that have come in through the "Chat" box. Let me just find out from the operator if anyone has dialed in by phone. Operator?

**Operator:** We have no questions at this time.

**Ms. Levinson:** Okay, we'll go to the "Chat" box. I think we can take two questions.

**Ms. McWilliams:** The first question is: Is a date of birth with patient initials in an e-mail HIPAA compliant or too disclosing?

**Ms. Levinson:** That's a good question.

**Ms. McWilliams:** My initial response is that most likely it would be HIPAA compliant, but it would depend pretty much on the purposes. I'm hesitating with this because, again, this would have to be analyzed from a technological viewpoint because I know there are certain sets of data that if you bring them together it's reasonably easy to break that code and determine who the individual is. I would assume that, for most purposes, a date of birth and initials does not provide sufficient information. But you should probably have that seen by your own EMR, Electronic Medical Records Consultant just to be sure I'm correct about that.

The next question is: Unless a state law prohibits sharing client-level data in either a limited data set or a delimited manner—which I'm assuming meant de-identified manner—then the grantee is permitted to share their data set. I would say that's correct: that that is, in fact, the case.

**Ms. Levinson:** We can skip the next one.

**Ms. McWilliams:** Okay.

**Ms. Levinson:** We're going to work on that and see if we can explain it in just a minute.

**Ms. McWilliams:** Please explain the distinction between consent and authorization under HIPAA. The authorization is the situation that I talked to when I referenced you to page seventeen where it speaks specifically to what an authorization needs to include. Typically a consent is a more informal, less regimented sort of approval for the sharing of data. The authorization has very specific requirements. This is on a slide that was presented earlier, written in plain language, contains the information to be disclosed or used, identifying the person

disclosing and receiving the information, the expiration date, and—etc., etc. That's on page seventeen, and that's what is the authorization.

**Ms. Levinson:** We're providing a little information in the "Chat" box to the user that was looking for information about how to download or order the materials. To provide clarification, there are two ways. You can download and print out the materials yourself, and there are hard copies also available for order from the HRSA Clearinghouse. You can go to the website or you can call 1-888-ASK-HRSA. Those are free to be ordered, and they're available in both English and Spanish.

**Ms. McWilliams:** The next question is: We have a multi-disciplinary care team of providers from multiple organizations to care for clients. Do clients need to sign a release for each provider to allow multiple providers to discuss treatment and care options for each client? Again, that falls into the category of permissive use and disclosure. It's considered to be a treatment issue and individual authorizations are not required.

Isn't this question about coordination? I don't understand what that means. Would you expand a bit on that, please? While we're waiting for that there are a couple questions that came in with the registrations. I'm going to go to those questions now.

The first question is: What are the HIPAA implications of requiring names, dates, and reporting of client-level data for Parts A and B grantees to understand utilization trends and unmet needs? There's going to be a follow-up call to this one that's going to talk about the operational aspects of HIPAA and the client-level data. A lot of these questions will be covered in much more detail then. My understanding is that HRSA is not going to be requiring name-based reporting. CDC is requiring it, but that's a different issue. HRSA is going to be using a unique identifier.

The second question is: How do you meet HIPAA requirements on a centralized server housing information from twelve organizations with over ten thousand clients? That actually is more of a technological issue. The HIPAA requirements, I think, are pretty clear to be what we just described. It really is a question of how you set up the different, I'm going to call them, accounts for each of the providers in the organization to make sure that each provider and each account does not have open access to the other accounts on the server.

The third question is: I assume that HIPAA is the overall privacy law and that state laws that are stricter remain so. If that is the case how do you keep up-to-date with the various state privacy laws? There's a couple of ways to do this and it depends on the state you are in. In Massachusetts, we have a trial law library website into which people can sign and get updates on the various laws that are being passed. Virtually all the state legislatures, at this point, have websites where you can check on legislation. Probably the easiest thing to do is to keep in touch with your local ACLU, American Civil Liberties Union. These are the folks who are typically very much on top of state privacy law. Another place to look to is an organization called the Electronic Freedom Foundation. I believe their website is EFF.org. They do a very good job of doing annual surveys and summaries of the state of the law around privacy in the various states. There is another organization called EPIC. I'm blanking on what that acronym stands for. I believe it's the Electronic Privacy Information Center. Their website is EPIC.org. Similarly, they

do a very nice job of surveying the state of privacy laws across the country and reporting them. Those are some of the places you can go to. Again, you can always find a local, neighborhood attorney and ask to be updated. Most of us do get these updates pretty regularly. I have worked with one organization where a guy was sending out updates to a variety of organizations that I've worked with in the past.

**Ms. Levinson:** We have no other questions in the "Chat" box. If any of you have anything you'd like to add please do. Operator, do we have anyone in the telephone queue?

**Operator:** We have no questions at this time.

**Ms. Levinson:** Okay. If you come up with any additional questions you'd like to have us include in the question and answer document that we'll be developing you can e-mail those to us at dataCHATT @jsi.com or you can also submit your questions through our website.

It's time to bring the call to a close. I want to thank Denise McWilliams for joining us today. And I'd like to thank you all for listening in and participating in today's call.

Please look to the right-hand side of your screen. You'll see in just a minute that a "Polls" bar will be added. There it is. There are a few brief questions there. Please take a moment to answer those questions before leaving the session. Don't forget to check dataCHATT, the TARGET Center site, and the HAB emails for information on our third web conference as well as archived materials from both Part I and Part II of the HIPAA and Data Sharing call. We will e-mail all of you registrants from the Part I and Part II calls when the archived version of the Part II call is up. Thank you again for joining us. Goodbye.

**Operator:** Ladies and gentlemen, this does conclude the conference call for today. We thank you all for your participation and ask that you please disconnect your lines. Have a great day, everyone.

**[End of Recording]**