JSI RESEARCH & TRAINING INSTITUTE, INC
DATACHATT WEB CONFERENCE

HIPAA and Data Sharing
Denise McWilliams, AIDS Action Committee
June 24, 2008

TRANSCRIPTS

Operator: Welcome to the National Training and Technical Assistance web conference sponsored by HRSA's HIV/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: I want to welcome you all to the first web conference through the National Training and Technical Assistance Cooperative Agreement. I'm Mira Levinson, Project Director for the Cooperative Agreement and I will be the moderator for today's call.

The topic of today's call is HIPAA and Data Sharing. HIPAA, the Health Insurance Portability and Accountability Act, was enacted by the US Congress in 1996. This Act included a number of provisions which addressed the security and privacy of health data, and it has resulted in guidelines and policies to protect and regulate use and sharing of protected health information, or PHI. The goal of today's web conference is to provide an overview of HIPAA and to help participants understand how HIPAA regulations impact data collection, data sharing, and reporting of Ryan White HIV/AIDS Program data. If you haven't already, please download the materials for today's call. The links for these documents appeared on the original registration page and will also be posted on dataCHATT, which is our website at dataCHATT.JSI.com, along with an archived version of today's web conference, which will be posted as soon as it becomes available.

Our presenter, Denise McWilliams, joins us from the AIDS Action Committee of Massachusetts. The AIDS Action Committee is dedicated to stopping the spread of HIV/AIDS by preventing new infections and optimizing the health of those already infected. They provide free confidential services to over 3,500 men and women already living with HIV/AIDS, and they conduct extensive educational and prevention outreach to those at risk of infection. Our presenter 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 worked for and directed several HIV/AIDS organizations including the AIDS Law Project, the Justice Resource Institute's Health Law Institute, and the Boston AIDS Consortium. Denise 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. She currently serves as General Counsel for AIDS Action.

Following Ms. McWilliams' presentation we'll have a question and answer period. If you have questions in the meantime you may type them into the ChatBox on the right-hand side of your

screen and they will be addressed during the Q and A. After the presentation is finished you may also dial the operator if you prefer to ask your question by phone.
Before we begin I'd like to review a few additional technical details. All participants are currently in listen-only mode so you don't need to mute your individual phone lines. If you have any technical difficulties during today's conference please dial 1-4 to reach the operator or type your problem in to the ChatBox on the right side of your screen. Now I'll turn it over to our presenter. Denise, please go ahead.

Ms. Denise McWilliams: Thank you. Good afternoon everybody. It's a pleasure to join you, at least digitally, for the following presentation. We're going to be talking today about the interplay between HIPAA and the Ryan White HIV/AIDS Program. Before I start that, though,—I'm being a typical attorney with a malpractice policy behind me—I want to throw out a few disclaimers so you know exactly what we're talking about.

First off, nothing I'm saying to you should be taken as legal advice that's directly relevant to your own situation. Those of you who have been trained in chemistry will be familiar with the phrase that "small changes can have enormous consequences." That's also true in law. Very small changes to your organization—how you collect information, who you serve, and how you're funded—could totally change the answer. It's simply not possible for any attorney to speak to over a hundred people and be able to answer a question without getting more details about the situation that has arisen.

The second thing I want to talk about is that all of these cases are highly idiosyncratic. Again, this is in light of my first comment. However, they can also change from day to day because of changes in the law, because of a change in an emergency situation, and because of a change in funding. They can change because your organization has changed its corporate structure or perhaps has merged or entered into a business agreement with another corporation.

This leads me to the third point. Any time you have a question about whether or not a piece of information is restricted from freely flowing throughout your system you really do need to find and consult your own attorney. There is nothing like having your own lawyer who has only your interests at heart to really sit down and work through the issues you're presenting.

With those disclaimers out there I want to talk about what is HIPAA anyhow. As Mira said, HIPAA is the Health Insurance Portability and Accountability Act. It had four main purposes when it was first enacted. The first purpose was to improve the availability and the continuity of health insurance. The second was to present fraud and abuse. The third, which I think is somewhat ironic given the amount of concern and conversation that's gone on, is to simplify the administration of medical records and medical billing systems. The fourth was to promote the use of medical savings accounts.

Clearly over the years what has become most key for people is the privacy end of HIPAA; and I believe that's the piece that most affects you. But it's important to remember that the privacy actually stems from a desire to simplify the situation; and the purpose or the goal was to reduce costs by standardizing the exchange of information while at the same time protecting people's privacy as well as the security of health information.

HIPAA is a floor, it's not a ceiling. HIPAA establishes the bare minimum that companies, providers, entities, and organizations are required to meet in dealing with the health information of people in that system. The ceiling is really imposed by your state law, and states vary wildly in terms of applying privacy and confidentiality around medical information. States can increase protection from HIPAA, but they cannot decrease the need for protection that HIPAA affords people. Some state—my own, for example, Massachusetts—have gone a long way towards enhancing the privacy protections of everybody. Many other states rely solely on HIPAA to present what the barriers or the standards are for this sort of thing.

The guts of the HIPAA rule for our purposes today, if you will, are the privacy rules. The privacy rule is a national standard that's composed of three separate elements. The first of these are the individual rights of people whose data we're talking about or people whose information is being sought to be shared. The second piece of the national standard is guidance on the exercise of those rights. In other words, how do individuals take steps to protect their own information? The third piece is a distinction around the uses and disclosures that require the authorization of the subject of the information before it can be used for other purposes. I want, at this point, to be clear that there is a distinction between authorization and consent that we will be going into more in the second session.

We are going to talk primarily in this session about things like: What is a covered entity? Is the information we're talking about covered by HIPAA? If it is covered, what are the standards that apply, how do I hold it, and what do I do with it? In the second session we're going to look at the issues around disclosure, data sharing, what sort of authorizations or consents are required for further use of the information. I looked at some of the questions that some folks have submitted for this session and I'm going to hold those questions until the second time around because they really do deal with disclosure issues. I am hoping it might be helpful to have the overview before we actually delve into the details.

The question of whether or not HIPAA applies really stands on the answer to two other questions, the first of which is: is it a covered entity? The second is: is the information we're talking about covered by HIPAA? Covered entities are among the following, these are the ones you'll most commonly see: health plans, healthcare clearinghouses, healthcare providers, hybrid entities, and technically business associates aren't covered entities on their own, but they are through contract. Because so much of Ryan White services depend on contractual agreements between other organizations I decided to include business associates within this category.

A health plan is broadly defined to be a payor or a provider/payor of health care. This is not a definition that includes employer-sponsored group plans or government programs whose main purpose is not to provide or pay for the cost of health care. So those two other categories are not covered entities under HIPAA. Broadly speaking—and again this is broadly speaking—payor or provider/payors are, in fact, covered by HIPAA.

A clearinghouse is an entity that translates into a standard format the health information that they receive from providers so that it can then be transmitted electronically to payors in a fairly uniform system.

The next entity, which I think covers a lot of folks who might be on this call, are health care providers. Health care providers are broadly defined to be persons in facilities that provide care and services, as well as supplies. Among the services that we talk about—this, again, is an illustrative list, it's not an exclusive list—are preventive, diagnostic, therapeutic, rehabilitation, and counseling assessments or procedures regarding the physical/mental condition or functional status. This covers traditional as well as alternative providers. For example, MDs, ODs, acupuncturers, in some cases even perhaps massage therapists would be covered under HIPAA depending on how they get paid for their services.

Whether or not a person or an entity is a health care provider is answered by applying this three-part test: Does the person or organization furnish, bill, or receive payment for health care in the ordinary course of business? If that answer is yes, the next question is: Does this person or organization conduct covered transactions? We'll talk a bit more about that in a moment. Thirdly, is health information transmitted electronically in connection with any of the covered transactions? The answer to all of those questions has to be yes for a health care provider to be covered under HIPAA.

Hybrid entities are somewhat of an odd bird. They're a single legal entity. So it's a single corporate structure that is covered by HIPAA, but it engages in covered as well as non-covered functions. If you're a hybrid entity you are permitted to designate which components of yours are covered components subject to the privacy standard, but you are required to erect firewalls between your covered and non-covered components. If a hybrid entity fails to do this they can well find themselves having to justify why their entire course of business is not subject to HIPAA. So the firewalls are a key function in maintaining your status as a hybrid.

Business associates are a person or an organization to whom a covered entity discloses PHI so that a function for the covered entity can be performed. For example, if somebody does your billing for you, if somebody does your quality assurance, if somebody does your filing but it's a separate entity—it's not an employee or an agent within your corporate structure—that would be a business associate. But it has to be outside of your corporate structure. To engage with a business associate and to safely share information with that associate without incurring liability you have to obtain satisfactory assurance that the PHI will be appropriately safeguarded. Simply put, you need a contract, and the contract should detail that it is to cover the protection of PHI and these are the ways in which your business associate is going to safeguard that information from further impermissible disclosure.

Covered transactions really are simply health claims or the equivalent of a health claim, the enrolment or disenrollment information, payment or remittance advice, referral certifications/authorizations, coordination of benefits, or premium payments can all be considered to be health claim or the equivalent to a health claim.

The next piece—and this is always the one that's a little bit surprising to folks—is whether or not the information is transmitted electronically. It isn't what we might think of as necessarily sending the information out over the Internet to a recipient third party. It can also be information that's kept on your own intranet or in your private network. Even so simple a transmission as saving it to a CD to file in your own internal structure is sufficient to bring the information

within the ambit of HIPAA. These days virtually all of us will probably have our information transmitted electronically according to this definition.

The Protected Health Information, which I've been referring to as "PHI" without telling you what is meant, and I apologize for that—is actually defined to be information that's individually identifiable and is transmitted or maintained by electronic media or any other form or medium, and that includes paper. So if you have information that I can look at and I can say, "Okay, that's Mary Smith," and you transmit it or maintain it in any format at all, besides your memory that I know for your purposes of malpractice you don't do, that is going to be covered and considered to be protected health information. Most educational records are not considered to be protected health information because they're covered by a separate federal statute. If you're looking at an educational record that is not something generally you need to work about in terms of the HIPAA requirements. Similarly employment records are not considered to be protected health information. As an example of that if there is a Worker's Compensation claim and a person submits the medical records relevant to that Worker's Compensation claim to their employer – that has taken it out of the ambit of protected health information, changed it into an employment record, and the employer and the employer agents are not bound by the strictures of HIPAA.

Information that is not considered to be PHI is any information that has been coded, encrypted, or from which the identifying information has been otherwise eliminated. So if you have a record and a person's name and other identifiers have been removed or if the information has been encrypted such that it is not easily accessible to somebody—and "easily" is obviously a term of art—that's not considered to be PHI. Another way information is taken out of the category of PHI is if there is a low probability of identifying an individual according to documented scientific methods. These are typically statistically analyses done of the types of information that various organizations have, and a determination is made—and there's a standard for this—as to whether or not that will be considered to be PHI.

One of the things I want to talk about are some examples for people to respond to to get a sense of whether or not these are PHIs, covered entities, or electronic transmissions. Let's take, for example, a situation where you have a grantee funding an NGO to run the local ADAP Program. The NGO reports back to the grantee on utilization. I'm going to ask people to please look at the right-hand side of your screen and you're going to see a bar saying, "Raise Hand." I'm going to ask people to raise your hand if you think that NGO would likely be a covered entity under HIPAA. The question is: is the NGO a covered entity under HIPAA? Raising your hand is a yes. An NGO is a non-governmental organization and generally a non-profit organization. The question again is: if a grantee is funding an NGO to run the local ADAP program and the NGO reports utilization back to the grantee, is the NGO—a non-governmental organization or a non-profit—considered to be a covered entity for the purposes of HIPAA? I'm going to give you another moment to chime in here. I'm sorry, I didn't realize you folks can't see this. So far out of 134 folks we've got 60 coming in saying yes, an NGO is a covered entity. I'm just going to wait another moment. Okay, the total we have now is 68 folks—oops, somebody just changed their vote—67 folks think that this is, in fact, a covered entity. I would be inclined to agree. It think that that NGO is most likely going to be a covered entity because it does, in fact, provide a service. It would either provide funding for the service or the actual premium in some cases. In some states I think they actually do provide drugs directly. So I would probably be a covered

entity, and particularly because it reports back to the grantee on utilization. So you're going to have some way of storing the information, maintaining the information, and then sending it back to somebody else, most likely electronically. So I think that likely will be a covered entity.

Let's try the next example. You have an AIDS service organization (ASO) that provides housing, counseling, and case management services to folks living with HIV and AIDS. They report back to the grantee on the client's CD4 counts and viral load. The information is stored on the ASO's intranet, which is the internal network, but it's mailed in a hard copy. The first question I'm going to ask is: how many folks think that this ASO is likely to be a covered entity? Okay, we have 80 people who are saying this is likely to be a covered entity. I'm going to agree with that. There is a slight chance that it might be a hybrid entity that would require a few different things—the erection of the firewalls, for example,—but because it is, in fact, providing health care services, as that broad definition I gave earlier applies, and because they're reporting back on health care information, specifically the CD4 counts and the viral load, and because it is stored electronically on the intranet, all of those examples are things that would push one into the direction of finding this to be a covered entity.

Keeping with the same example, the question I want to ask now is: do they actually serve or do they actually transmit PHI? In other words, how many people would find that the CD4 counts and the viral load is protected health information? Again, raise your hand if you think it is protected health information. [Pause] Okay, 79 people are chiming in saying that they believe that that this would be protected health information. It's a little bit more complicated because the question would be: how does that get reported? If that gets reported in a way that the individual can be identified it is likely to be found to be protected health information. If, on the other hand, it is a situation where the information is aggregated and it's not possible to look at the report—or it's not reasonably possible—to look at the report and make a determination it is likely not going to be protected health information. So it really depends on whether or not those reports can be teased out so that individuals can be identified.

The third example we'll talk about is you have a health center—clearly a covered entity, it provides health care in the normal course of business—that contracts out their billing to a third-party vendor. How many people would find that third-party vendor to be a covered entity? Again, hit the "Rise Hand" button. [Pause] We have 74 people who have said that they find that the third-party vendor is likely to be a covered entity. Again I would agree with that. It's billing for payments for health care services provided to another party. Another thing to consider is that if, for whatever odd reason inherent to the way the contract is set up, if that’s not considered to be a health care entity it would likely be found to be a business associate of the health center, and that the information that they transmit, maintain, and utilize would then also be covered under HIPAA under the business associates which calls into play the obligation to provide specific contractual agreements and assurances about how the information is going to be maintained.

We have gone through the information that we've prepared for this. I think now I'm going to take a look at some of the questions that people have specifically asked.

Ms. Levinson: We're going to go to the question and answer session in just a moment. Before we begin I want to tell people about a few important resources.

First, as a reminder, in case you joined the call a little late, please be sure to go and download or order HAB's resource guide, "Protecting Health Information Privacy and Complying with Federal Regulations." Details on many of Denise's points can be found in this document, and you'll also find recommendations which you may find useful. Second, as Denise mentioned, she will be back next month to talk more about HIPAA and Data Sharing in Part II of this presentation. During that session Denise is going to cover additional information such as how to deal with data that is sent from a contracted provider, paired to a grantee, or to HRSA. Please join us on Thursday, July 24 at 2 PM for that session.

Third, in the next few days we're going to post an archived version of today's presentation along with a frequently-asked-questions document that we will create based on questions that were submitted during today's call and during the registration process including both those that are answered during this call as well as those that we may not be able to get to. I apologize, that is 2 PM Eastern Time for that call on Thursday, July 24. If you'd like you can check our website, dataCHATT.JSI.com, in the next few days to access the archived materials and you may wish to forward that link along to others that you work with or that are providers with you who you think may benefit from this presentation.

One last point before the question and answer session: at any point after this you can click on the "Polls Panel," that is going to appear in just a moment here. It's going to be opening on you right-hand side. Once that polls screen opens, you'll see a few brief questions. We'd like it very much—there it is—if you could just take a moment to answer those questions before leaving the session.

Let's get started with the question and answer session. Note that there are two different ways to ask questions. First, as we mentioned earlier, you can type your question into the ChatBox on the right side of your screen and I'll pose it to Denise. Second, you may ask your question by phone. The operator will now give instructions for dialing into the queue. While we're waiting we're going to take a few questions from the ChatBox and also from some pre-registrants.

Operator, can you give the dial-in instructions?

Operator: Yes, 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 acknowledging your request. Your line will then be [inaudible] access from the conference to obtain information. If your question has been answered and you would like to withdraw your registration please press the star followed by a zero. If you're using a speaker phone please lift your hand set before entering a request. We are ready for the first question.

Ms. Levinson: While we waiting for the first question to queue up we're going to take a few questions that have come in through the registration process. Several of the questions were submitted by CAREWare users. Those participants asked about HIPAA compliance in terms of the data sharing options available in the CAREWare software. Because it came in early in through the registration process, HAB was able to pose that question to John Milburg. He's going to be posting some information about this issue on the TARGET website. So please check the

TARGET website for further information about CAREWare and HIPAA compliance in terms of data sharing options and other aspects. We will also post that information in our frequently asked questions or a link to it.

Denise, are there any other of these questions that you have not yet covered that you would like to go to before we go to…

Ms. McWilliams: One question I would like to respond to, the question was asked by a participant: If you assume there are 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 their client's information? Again, you have sixteen providers on a single server. If they wanted to share client-level data between or among themselves would they have to have each client sign a consent form for them to share their clients' information? The answer to that will really be found in the legal entity that the provider is. If each of the sixteen providers are separate legal entities—they are their own corporation, they're their own governmental entity, etc.—they will then have to have the consent form their clients to share the information among themselves. If the sixteen providers are all the employees or the agents of one single organization/corporation, they will not have to get that level of informed consent from each client. So it depends on what is meant by "sixteen providers". If they're one corporation you do not need separate consents; if they're multiple corporations you do.

Another question that was asked is: Can a health care organization share data for the purposes of health care delivery without the need for an additional release of information or formal consent? In absence of an emergency, assuming the health care organizations are different legal structures, you need to obtain the consent from the subject of the information for that information to go back and forth; again, absent an emergency.

I want to say that at the outset, I've been looking at HIPAA for years now and my conclusion is that it permits you to pretty much share the information however you want to share it in some specified way. Sometimes it's consent, sometimes it's authorization. There is a variety of exceptions that you can use for public health purposes, emergency purposes, etc. If there is a belief that the information needs to be shared there is generally a way to do it even if a consent or authorization is the mechanism you have to go to. I frequently have had people tell me that they can't share things even with the client's consent. That's simply not true.

Another question is: Is it necessary to obtain consent to share clinical data every time you refer a patient to another provider for treatment? Generally authorizations or consents, well written ones, will have a time period involved. So, Dr. A refers to Dr. B John Smith and John Smith consents to this referral and the sharing of information for a period not to exceed thirty, sixty, ninety days, six months, or a year. So you don't have to have a separate consent every time the person returns to the same provider, but you do have to have within the consent some understanding of how long the consent is good for. Similarly, if you're referring the patient to a different provider and the different provider is outside of each corporate structure—or, in other words, each corporate structure is unique to that provider—you would then need to obtain consent each time you refer it out.

Ms. Levinson: Why don't we see if we have any callers in queue? Then we can take some of the questions from the ChatBox and a few of the other registration questions. Operator?

Operator: As a reminder, to register for a question please press the one followed by the four on your telephone. There are no questions on the phone lines, ma'am.

Ms. Levinson: That's fine. There are tons of questions coming in through the ChatBox. I think you can take a look at them as we go instead of me fielding them.

Ms. McWilliams: Okay, one of the questions is: As a provider don't we have both a legal and an ethical obligation to protect client's information by considering how someone who comes in contact with it will use? As an example, will the recipient of the information take the database that might lead them back to a location for those clients and cross match it to Medicaid's data that then might link the user to a specific client in the Medicaid database? That's a tough question. I actually think you do have a legal and ethical obligation to always take into account the protection of client-level information. I think the question of how can you cross match different fields of information to identify any given individual is a highly technical one and the law is very slow to catch up on this. I believe that there are standards—so many fields are in common—that information is no longer considered to be sufficiently protected; in fact, HIPAA actually talks a little bit about that. As an attorney, I would say look to see whether or not the databases you're looking to meet the technical standards for preserving confidentiality. In other words, do they have sufficiently few enough fields in common that it is a safe assumption that the individual not be identified? If the answer to that question is no, you have a problem because that information cannot be held confidential.

Going back to the ASO example, somebody has asked: Is it allowed for the ASO to share the information with another ASO, perhaps a food bank provider, for the purposes of the second ASO to maintain up-to-date records on clients? With the consent of the client involved, absolutely. I would argue that you cannot share that information without the consent of the client. But as long as people consent to that information going back and forth there's no barrier to it.

Someone's asked the question about whether the proposed HRSA Unique Records Number Format—which is the first and third letter of the first name, first and third letter of the last name, a six-digit date of birth, and a gender code—is considered adequate de-identification to collect and track client-level data. That fortunately is not a legal question; that's a technical question. I would have to defer to someone who is versed in the understanding of encryption and codes to know whether or not that passes the standard that has been set for preserving people's confidentiality and privacy.

Ms. Levinson: This is one of the questions that we'll certainly take back and pose to HAB so that we can try to get you responses on all of the questions that are coming in so that we can post them.

Ms. McWilliams: I'm not sure I fully understand the next question, it is: If you have a client, who we will call B, sign two releases, but client A signed all sixteen so that all sixteen recipients

of the release have access to client A's data, how is client B protected? The answer I'm going to give I don't think fully answers what the person is trying to get at so if you want to take a second crack at this, I'm sorry I'm not quite getting your point. Client B is protected because they have only agreed to choose discrete releases of the information, and they're neither bound nor affected by the sixteen that client A has signed. If I'm missing your point please feel free to send that in again.

Someone has asked: Please discuss network releases within a group of providers, all Ryan White providers. Again I would refer back to the legal structure of the entity of the network. If you're dealing with separate corporate structures, if everybody is their own separate incorporation, the information cannot be disclosed across the network without the separate consent of the client. If, on the other hand, the network is, for instance, a string of health care centers that are all operating the aegis of Health Care for Us, you could do that with a single release because you're all within the same corporate structure. There's also an issue here though that, although you can do it, you have to ask yourself do you want to do it because one of the keys in making an assessment of whether or not you have an unauthorized disclosure is, how well have you protected the flow of information within your structure? I had a case a couple years back with a local hospital that had a totally open client health record system so that the secretary of the cardiologist could, and did using her own password, go into the health record of a person living with HIV in a different part of the hospital in a different clinic—this person happened to be her sister-in-law—and discover my client's diagnosis and condition. I argued—unfortunately not successfully at that time, but I think this law has advanced a bit—that that was too wide open an architect to be used to justify the actually protection of somebody's confidentiality. Generally the shorthand version of this is the information is restricted to those who actually have a need to know. Again although you might be technically protected by the use of your consent disclosures if, within that circle of people protected by the consent, there's not thought and care given to how to protect the information from straying to an unauthorized disclosure situation you still could find yourself in an exposure situation.

Can a consent for a hospital system cover all the clinics within it? Yes, it can, again informed by what I just said. But as long as it's all within the same corporate structure and people really are restricted primarily to folks who have an actual need to know you can do it that way.

Can a grantee have a business associate agreement that covers fifteen or more agencies to share data? Properly drafted, absolutely. You would want to make sure you have it drafted by somebody with experience, that everybody understands what they are signing, and that the agreement accomplishes the goals that you all have in mind. But a business associate agreement could absolutely accomplish that.

The question has been asked: Is there a HIPAA condition or coordination of care that would allow getting a consent from every client in the system of care? I'm not exactly sure what that is asking. I'll take a crack at it, but if you could, please help me figure out what this means. I'm reading this to mean to allow the exception from obtaining a release from every client. I'm not aware of that. I'll be happy to look into that, but I thought that coordination of care still requires you have consent except, again, if you're in an emergency situation.

Do we have to obtain written consent to make a referral within our provider network of business associates when we have written agreements addressing HIPAA? Depending, again, on what's told to your clients, to your patients, and what they've agreed to, and depending on what your corporate structure is, you may or may not have to obtain written consent. In other words, if you are all operating within the same legal structure you can make a referral within that legal structure without getting a separate consent each time or as a business associate. Whether or not your written agreement relieves you from that obligation would really depend on what the written agreement accomplishes.

Is a state department of health-run ADAP exempt from HIPAA rules? No, absolutely not.

Would a non-covered entity be able to release PHI to a third-party contractor for a purpose allowed under HIPAA? If it's a non-covered entity HIPAA doesn't apply. You would again have other safe searches that you have to take into account. You might also have contractual obligations with the person. But, don't forget, HIPAA requires that an entity be determined to be a covered entity one way or the other under the definitions that we went through earlier.

Is the inclusion of date of birth identifiable and does it make the ID number identifiable? Again that's more of a technical question, not a legal one. I really don't have an opinion that I would dare to offer on that.

Overnight medical records are faxed to our clinics. Are contract maintenance staff held to the same HIPAA standards for privacy? That's an interesting question. I'm going to a different direction with this, which is that they are your agents, they're in the building, and they have access to information by virtue of the fact they might be in the building when there's not a whole lot of outside supervision. You would have other obligations around preserving the confidentiality of those records, specifically do these people need to see these records? If they are, in fact, maintenance staff it's hard to imagine why they would have a legitimate purpose to share or have access to that information. I would argue there that the maintenance staff may or may not be held to the same HIPAA standard, depending on their understanding is of their involvement with your organization, but the organization would clearly have the obligation to protect that information from invasion by people who shouldn't be authorized to see it because they have no legitimate purpose for it.

Ms. Levinson: Let me just interrupt briefly to say that we've reopened the poll with the evaluation questions. Please remember to leave your feedback during the rest of this call. We had a little technical problem, but it's back up. If you could take the time to answer those questions any time during this call, that would be great. Let's check with the operator to see if anyone else has dialed in. Operator?

Operator: Yes?

Ms. Levinson: Has anyone else dialed into the queue?

Operator: No, we still have no questions, ma'am.

Ms. Levinson: Okay. We'll take another question from the ChatBox.

Ms. McWilliams: The question is: Many universities have taken HIPAA as an indication that providers and their employees who use their databases with PHI to participate in activities might wind up publishing as advocate statements. For example, fifty-five percent of people with something in our network have this type of problem; they have to have IRB approval to participate in that type of activity. Is this rational? I never answer questions about whether or not something is rational. I restrict myself to whether or not it's legal or required. The reality is that IRB approval really speaks to whether or not something is a research activity. HIPAA will allow some exceptions to consent issues when it's done for the purposes of research, but HIPAA in and of itself does not create any sort of standard, entry-level requirement, or barrier as to when an organization should get their IRB approval. That really is a question of whether or not it's a research topic involving human subjects. So they sort of run on parallel tracks.

Can a third-party insurance carrier notify an employer of the diagnosis of AIDS in an employee? That's actually a more complicated question. Notifying an employer really depends on the purpose of the notification is. It's one thing if the insurance agent calls John, the chief CEO, and says, "My God, do you know that you have somebody with AIDS in your organization?" That clearly would be prohibited. If, on the other hand, the third-party insurance carrier is, for example, the administrator of a self-insured organization—in that case because the employer is, in fact, providing health insurance and paying for it—he or she can indirectly learn the medical status of many of their employees. If, for example, they actually get a report on pharmaceutical utilization that could be another indirect way that people could get information about the specific diagnoses of the employees. A lot of employers are rightfully nervous about this because even though it becomes, then, part of an employment record and it's not covered by HIPAA you still have the same issues around privacy that most states regulate. By that I mean that even if it's not covered b HIPAA that doesn't men you're off the hook. It means you still have to look at whether or not that information should be held in a private, confidential, secure manner. If the answer to that is yes and you haven't taken the proper steps to safeguard that information you will be held liable for inappropriate disclosure separate and apart from any HIPAA considerations. There is one famous case, I think it was in New Hampshire, of a gentleman who'd made a Worker's Compensation claim because of stress-related issue. The person who did the evaluation wrote back a very extensive report to the employer including several pages recounting the gentleman's unfortunate experience as a child with sexual abuse. The employer just folded that into the regular personnel file and, of course, it rapidly became well known throughout the entire company, what was going on with this guy. The employer there was held to have substantial liability, separate and apart from HIPAA, because he simply didn't hold sensitive private information in a responsible manner.

Ms. Levinson: I think that's it for our questions. Sorry, there's one more coming in. Let me point out in the meantime that you'll see the polling box on the bottom. It is asking you if you responded to the evaluation questions at the very beginning of the call please resubmit. That would be very helpful. Let's take this next question.

Ms. McWilliams: Since many non-governmental organizations utilize volunteers where do they fall into this? Are there any legalities that prevent volunteers from accessing PHI? If they are

allowed to access PHI, I would presume that there should be a signed confidentiality agreement. Yes. Generally a volunteer is considered to be an agent of an organization. If the volunteer has some legitimate need to have access to what would otherwise be protected health information they would be covered the same as any employee. As an attorney I generally recommend that all organizations have their volunteers, and their employees, sign confidentiality statements so you can establish that people understand what their obligations are around maintaining the privacy and the confidentiality of discreet information. But the fact that a person is a volunteer does not really alter the equation very much. It really just depends on, do they have a legitimate reason to access PHI? If they do, they're subject to the same obligations that the employees would be.

Next question would be: If a client agrees to a consent to be cared for by a network of separate legal entities at the outset of care will a network release listing all of them be adequate for PHI sharing? In my opinion if it's properly drafted, yes. I don't think you need to have a separate informed consent for each individual entity, but I think they do have to be listed in a clear reasonably readable fashion. Everybody remembers the old mortgage agreements and the car sales places where you had point-two font. Obviously it has to be legible to most people.

Referral of our patients to outside agencies may automatically disclose HIV status due to the nature of our clinic being the only ASO in the area. We should look to our contracts for specific language protecting PHI? That's a tough one. I frequently face this with my clients working with the AIDS Action Committee. What I generally say to people is that we are happy to take information and put it on benign stationery. We have a rental assistance program that we call The Rental Assistance Program. But we also, in our information disclosure, say to the client we cannot guarantee that people will never know you're getting services from AIDS Action. In fact, if that happens they're going to assume you're HIV positive or make certain assumptions about your HIV status. I think the only way to really handle that is by disclosure and to assure the client that you will take whatever steps you can to protect their confidentiality. But even then you simply cannot guarantee that somebody would not find out that this is the organization doing it.

Ms. Levinson: We have time to take about one, possibly two more questions.

Ms. McWilliams: We currently use CAREWare on a shared network server with no data sharing across providers. Is it a HIPAA violation for providers that share common clients to be allowed to share data? Again with the consent of the client it's fine. I would suggest that without the consent of the client it's not appropriate.

The next question is: What is the liability or the responsibility of the former employees of a covered entity over PHI? The fact that you leave the employ of an agency and you take with you, obviously at a minimum, your memory—at least those who are younger than I may take most of their memories—you still have the obligation to hold that information confidential and private. In most cases you can be found personally liable for failure to treat that information in the appropriate manner.

Ms. Levinson: I think we're going to bring the call to a close in just a moment. I can see that there are a few additional questions that have come in. If you have additional questions you can

either put then into the ChatBox now or if you think of them later please feel free to email them to dataCHATT@JSI.com and we'll add those questions to our FAQ document that we're going to prepare following this call.

I would like to thank Denise McWilliams very much for joining us today. And I'd like to thank all of you for listening and participating in today's call. Please remember to complete the evaluation questions in the poll box and mark your calendars for Part II of this HIPAA and Data Sharing conversation scheduled for Thursday, July 24 at 2 PM Eastern Time. Registration information will be posted on the TARGET website starting on Monday; and a link to information about this conference and an archive of today's session will be found on our website, dataCHATT.JSI.com.

Thank you again for joining us. Goodbye.

Operator: That does conclude the conference call for today. We thank you for your participation and ask that you please disconnect your lines.

[End of Recording]