JSI Research & Training Institute, Inc
Ensuring the Privacy, Confidentiality, and Security of Your Clients' Data
National Training and Technical Assistance Cooperative Agreement
January 26, 2009

Operator: Welcome to the dataCHATT Technical Assistance web conference sponsored by the HRSA HIV/AIDS Bureau. The topic for this afternoon's session is "Ensuring the Privacy, Confidentiality, and Security of Your Clients' Data". Please note that this session is being recorded. During the presentation, the phone lines will be muted. After the presentation, we will open the lines for questions. At this time, I will hand the call over to Mira Levinson. Go ahead.

Mira Levinson: Thank you. Hello, everyone. I want to welcome you all to today's web conference. I'm Mira Levinson, the dataCHATT Project Director and I'll be the moderator for today's web conference. The topic of today's call is Ensuring the Privacy, Confidentiality, and Security of Your Clients' Data. The goal of the web conference today is to discuss necessary steps you need to take to protect your client's data. We will feature practical strategies for safeguarding this data with an emphasis on accessing, storing, sharing, and releasing data.

Today, we'll hear from Debbie Isenberg, an HIV data specialist. Debbie will talk about many procedures and processes for improving the security of your data, but we want to emphasize that this is not an instruction manual or to-do list. Instead, her presentation will discuss different approaches for keeping your data secure. We encourage your program or organization to determine your own data security needs and priorities.

If you haven't already, please download the material for today's call. Links to these materials were posted on the original registration page and are also available on the dataCHATT website, which is written out at the bottom of this slide, dataCHATT.jsi.com. One of the links wasn't working for a little while. I think it changed, but it has now been corrected if any of you had any trouble earlier.

We've posted two types of documents for today's call. The first is titled "An Introductory Resource Guide for Implementing the HIPAA Security Rule". This helpful document breaks the Security Rule into manageable categories and provides key activities and questions for each one. The second resource we've posted includes two examples of business associate agreements, one from the American Medical Association and another from the Department of Health and Human Services. Both sets of documents provide specific data security information including examples of secure data sharing relationships.

Our presenter, Debbie Isenberg, joins us from the Massachusetts Department of Public Health, Bureau of Infectious Disease Prevention, Response, and Services where she is the Director of Research and Evaluation in the Office of HIV/AIDS. Debbie has more than fifteen years of experience in the field of HIV, specifically in the areas of data management, data systems development, evaluation, applied research and quality management. She has worked with federal, state, local government and community partners on a variety of studies focused on using data for planning and evaluation purposes.

At the end of the presentation, we will have a question and answer period. If you have questions at any time during or after the presentation, you may type your questions into the "chat" box on the right-hand side of your screen and they'll be addressed during the Q&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. First, all participants are currently in listen-only mode, so you currently don't need to mute your individual phone lines. If you have any technical difficulties during today's web conference, please dial one-four to reach the telephone operator or type your problem into the "chat" box on the right side of your screen. Now, I'll turn it over to our presenter. Debbie, please go ahead.

Debbie Isenberg: Thank you, Mira. It is a pleasure to be talking with you today about the topic Ensuring the Privacy, Confidentiality, and Security of Your Clients' Data. As Mira mentioned, I work at the Massachusetts Department of Public Health where I am a Part B grantee. I also have experience working with Part A, C and D grantees regarding client-level data. What I will be sharing with you today are my experiences as well as best practices regarding privacy, confidentiality, and security.

First, to provide a little context, as Mira mentioned, while I'll be providing examples and ideas, not all of these may apply to your organization. You may also need to prioritize what is feasible with the resources that you have and know that improving the security in your organization is an ongoing process. Ideally, by the end of today's presentation, you may have identified one or two things that you would like to change, but understanding that you would not change your whole process at this point in time.

I'd like to review the training objectives for today's presentation. First, I am going to define the differences between privacy, confidentiality, and security and then discuss strategies for ensuring the security of your clients' data. Finally, today's presentation will provide a forum to discuss existing challenges to data security and explore potential solutions.

The terms privacy, confidentiality, and security are often used interchangeably, but they do each have a distinct definition. Privacy is related to an individual's rights to control the access to his or her personal health information, while confidentiality relates to the obligation of the entity or agency to protect data or information. This includes not disclosing the identifiable information to unauthorized persons or to unauthorized processes. Security is ensuring that data, and this is electronic or paper, cannot be accessed, read, or compromised by any individuals without authorization.

A way to think about this is that privacy is a link to an individual's rights, confidentiality relates to the agency's requirements, and security is how you do it. What does this mean for Ryan White funded agencies? I'm going to answer that question by looking at five areas related to data security: data access, data transmission, data storage, data sharing and release, and data disposal.

First, let's talk about data access. I'm going to address data access related to both paper records and electronic records. It is likely that your organization has both for your client information. First, I'd like to ask who has access to paper records that have client information. Access should be limited only to individuals who need to use the information. This may mean that the front

office staff has access to contact information, but may not need access to medical information for a client. Paper records with client information should not be sitting on employees' desks unattended. A common example is if an employee is reviewing a client file and then needs to leave their workspace. They should, at that time, secure that record in either a locked file cabinet or in their desk with a locking drawer.

File cabinets should be secured at all times. A common example that I'll also talk about is when a key is left in a file cabinet so that people can access the records during the day. Ideally, file cabinet keys are only provided to individuals who need access to the specific record. Records cannot be faxed unless the fax is secured, ideally in a locked room with limited access. If a separate room is not feasible, a way to secure the fax is to ensure that the person to whom you are faxing the record is standing by the fax machine on the other end when you send the record. Having a separate file room with limited access is ideal. If this is not feasible, again, just ensuring that you have a locked file cabinet would be the best way to go. Finally, ensuring mobile or outreach projects have limited access as well to records is critical. If staff see clients off-site and take records with them, you want to ensure that there are appropriate protections in place for those records as well.

Now, let's talk about electronic data. Access, again, should be limited to the level of information that each individual needs to use, often called minimum necessary information or role-based access. This is actually easier to do with electronic files often than with paper files because of the nature of how electronic data systems can be set up. Passwords and/or user IDs should not be shared. Having a distinct user ID and password for each person using a system is critical. If they are shared it eliminates the ability to have an audit trail or to understand who is accessing what type of information at what time.

Data systems should also have a screensaver, lock, or timeout period. This is no different than the system that you currently have on your computer where you can have your screensaver pop up after you haven't been using your keyboard for a period of time. You want to minimize this amount of time to the shortest time possible to not interrupt your routine daily flow of work. Finally, Data systems should have an audit trail so that access to electronic records can be monitored. An audit trail usually tells you who accesses, what they access, and when they access the information.

Internet-based data systems should have authentication for access. What this is means is that if you are accessing a data system such as a server through the internet, you have to provide some information to prove that you are the correct person accessing it and this links to the user-based authorization that they have on the other end. This could be as simple as a user ID and password. Ideally, a second-level authentication is beneficial. This prevents someone who may have access to your username and ID from being able to access the system. What you may be familiar with is that if any of you access your banking accounts online, currently a lot of the banks have you actually acknowledge that a picture that they show you is the correct picture. This ensures that you are actually authorized to access this real bank system and not an alternative website that might have been put up in its place.

Access to the data system should be terminated when employees leave the agency or for other appropriate reasons. Again, having distinct username and password is really critical for this to be implemented accurately. Also, if an individual is on leave, such as time away from the agency,

you can make their password inactive for that period of time and then reactivate it when they come back. Data systems should not allow repeated unsuccessful login attempts. Ideally, after two attempts, the system would lock out a user in the event that they forgot their username and password and this will prevent individuals who shouldn't have access to the systems from gaining access.

Finally, all employees should be trained on data access rules. The rules that we just reviewed were possible rules that you could implement and it would be critical for everyone to understand for them to be implemented appropriately.

Now, let's switch and talk about data technicians and, again, we are going to talk about paper data first and then electronic data. So, how are paper data transmitted from providers to the grantees. Now, hand-delivery is ideal, but often not realistic for us. If you need to mail data, you want to try to omit any confidential data before you mail it. If you must mail confidential data, you'd like the envelope to be signed for and also ensure that the envelope is sturdy enough to have data in it and will not tear during the mailing of the information. If confidential data are faxed, again, ensure that the fax is secured as we discussed earlier.

How are electronic data transmitted? Client data should not be emailed unless the email can be appropriately secured and this means encrypting the email route. Password protection is not adequate to ensure that the data that you are transmitting is going to be secured. Now, email is different than some of the electronic transmission that a lot of us are familiar with using, like secure data networks or what are called FTP sites. Again, those are often secure sites where data are posted and then taken by the appropriate person at the agency to which they belong.

Encrypted file passwords cannot be sent in the same mailing as an email or CD. So, when you encrypt a file, you put a password in and to decrypt it, you need a password as well. You don't want to send those same two pieces of information in the same correspondence or anyone who receives it would be able to decrypt the file.

Finally, appropriate authentication and firewalls should be in place for web or internet access for electronic data systems. This ensures that people who should not have access to your data, won't have access to your data or to the electronic systems at your organization. It also ensures that the data are getting to the individuals that they are supposed to on both ends. Some of us face challenges in firewalls when we are using server-based systems, where both aspects have to communicate, meaning your agency has to communicate and the host of the server has to communicate with each other. It is important if you are using that type of system that you involve your IT program, if you have one, or possibly a consultant to make sure that the firewalls are the way that they should be so that the systems can talk to each other.

How are paper records stored? First, after files are secured in a file cabinet and a locked file is ideal, we already talked a little about this, if that is at all possible. What about paper records for outreach mobile vans or home visits? Again, paper records should be secured at all times and records should be stored in a business environment. The reason I raise this is many times, if you are going out to visit a client, you may go home after that visit. It is really critical to consider ensuring that a business environment exists if you must bring records home to your home. What this means is having a locked file cabinet, ensuring that records aren't getting out and bringing

them back to your business environment as soon as you can, to make sure that those records are secured at all times.

Where can electronic data be stored? Well, a stand-alone system is ideal, but for many of us, we may not have a stand-alone system. If you have a networked system, you want to have limited access to the folder or drive so that only people who should have access to the electronic data do. Encrypted data is ideal, so if you are able to encrypt data that is stored on your computer, that would be ideal. Finally, as we discussed before, having the appropriate firewalls in place so that your data systems are secure from people outside of your organization is critical.

Can laptops be used for confidential data? They can if you ensure that you secure the laptop when not in use. One of the things that many of us have noted in our professional lives is that laptops have both legs and feet, so they do tend to walk away if we are not watching them. To do that, you want to make sure that you have all protections in place if you are using the laptop: securing it, taking the data off, encrypting it if there are confidential data on it, and, finally, actually using a physical lock so that the laptop is attached to the desk on which you are working.

What is the backup procedure for electronic data? Data should be backed up in a different place than original data. If you have a backup of your data system and your system crashes and you've kept the backup data on the same system, you've lost that as well. You want to ensure that you save it in a distinct place and also ensure that however you save it, it is secured in the same way as the original data. The frequency of backup should be based on the quantity of loss. Therefore, if you are entering a lot of data on a routine basis, you probably want to back up your data more frequently. If you are entering data just a few times a month, you can probably backup your data less seldomly. The reason I mentioned frequency of backups is, again, each of these backups should be backed and secured the same way ensuring that access is limited. When you no longer need these backups, they should be sanitized and destroyed. What does this mean? Sanitized means for a system such as a CD, I would actually go and say you should shred the CD and ensure that it can't be replicated or used.

If it is stored on another data system or a hard drive, you actually would want to sanitize it which means purchasing a software application that overwrites it to ensure that the data are deleted. Just deleting data still leaves a remnant of data on your system so ideally, you want to purchase a software program to ensure that doesn't happen. Can flash keys, external drives, or CD-ROMs be used for confidential data? Again, data should be encrypted, removable media should be sanitized, and, when possible for CD-ROMs, the data should be shredded.

Data sharing and release: do you have agreements in place with entities with whom you share data? Mira mentioned earlier about business associate agreements that provide a great model of what you should include. Whether or not you are a HIPAA entity, these are very good models to use. They often include the use of the data, the timeframe for the data, the agreement that the data will only be released under certain parameters, and that the data will be destroyed at the end of the relationship. Do you have specific rules regarding data release? Identifying a specific individual or individuals who can release data, determining what cell-size is required to ensure that client confidentiality is maintained. I do note to not assume that aggregate data is okay. The reason that I mention this is that if you have a small population, and perhaps you have one individual who is male, African-American, thirty years of age, and you keep having additional

data points, it may be possible for people to figure out who that person is. So, you really want to look at your data and ensure that the cell-sizes protect the confidentiality of people in the data systems.

Finally, omission of names usually does not protect client confidentiality. If you provide enough other data points and you omit the person's name, but you talk about the person who perhaps was infected by their best friend and lives on the west side of town, the more information you give, you're making it more likely that someone's confidentiality can be breached.

Finally, let's talk about data disposal. What rules are established for data disposal? It is really critical to check the state laws, institutional review boards (IRBs), and federal laws related to requirements about the disposal of data, ensuring that you don't dispose of data that you must keep on record. Ensure that paper files are shredded when you are able to dispose of them. I strongly encourage you to get a shredder that does confetti cuts and not strip cuts because strip cut shredders often make it possible for people to still read what is on the piece of paper that you shred. Also, ensure that electronic files are sanitized, as we previously discussed, or destroyed. If you buy a shredder, some shredders have a CD component so you can put a CD in there and shred it and you ensure that it is destroyed.

So, where do you go from here? First, asking the question does your agency have written privacy and confidentiality procedures and, if so, what are they and are all employees trained? Finally, how does your agency secure your client data? You may decide after this call to walk around your organization and notice file cabinets that are unlocked, notice computer screens where no one is sitting at the desk, but you can still see what is on the computer screen and perhaps, you have access to an individuals email. That will help give you a starting place about ensuring the privacy, confidentiality, and security of your client's data. Thank you.

Mira: Thank you, Debbie. Before we move on to the question and answer session, I want to take a moment to tell everyone about a few important resources. First, we hope that you have enjoyed this web conference as well as our previous ones: HIPAA and Data Sharing Partings I and II, and Data Reporting: Building Effective Partnerships with your Contractors.

Archived versions of past web conferences are available on the dataCHATT website, again that is dataCHATT.jsi.com and you can see that in the lower right-hand corner of your screen. Posted materials on our site include audio recordings, downloadable copies of the slide presentations, transcripts, and any accompanying materials. As soon as it is available, we'll also post an archived version of today's presentation.

Second, we want to let you know about another training resource we are developing here at dataCHATT. "Data Academy" will be a series of nine online training modules focused on the "Essential Steps for Data Flow." "Data Academy" will go live this coming summer and you'll see announcements on the TARGET Center website as well as dataCHATT as we get closer to launching the modules. In addition, all participants in today's web conference as well as our previous web conferences will receive an email announcement. "Data Academy" modules will provide basic and intermediate training on common challenges encountered by Ryan White grantees related to data collection and data management. Some featured topics will include: collecting data from existing sources, simplifying and organizing your data collection, getting data from your contractors, improving the quality of your data, and HIPAA compliance

strategies. To learn more about the "Essential Steps for Data Flow," visit the dataCHATT or TARGET Center websites. Direct links to the data steps information are posted on this slide and they are works in progress so you can check now and you may find that they evolve over time. Now, let's begin the question and answer session.

As a reminder, there are two ways to ask a question. You can type your question into the "chat" box on the right-hand side of your screen or you can ask your question by phone. The operator will now give instructions for dialing-in to the telephone cue and while we are waiting, we will take some questions from the "chat" box. Operator?

Operator: 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 be briefly be accessed from the conference to obtain information. If you would like to withdraw your registration, please press the one followed by the three. If you are using a speaker phone, please lift your handset before entering your request. One moment please for our first question.

ML: While we are waiting, I want to begin with some of the questions that were submitted during the registration process. The first question comes from Michael Bryson in Phoenix, Arizona and he asks about – I'll go ahead and read it. "A clinician told me that her contact with a specialist for consultation or referral does not require specific client consent since it is medically in the client's best interest. Even if this is a one-way exchange of client history, what are the limitations and when is verbal approval okay? How does physician-to-physician contact differ in this requirement?" He also asked, "I'd like to hear examples of how Ryan White Part B programs develop sharing relationships with their state Medicaid programs? How does it rule for sharing change when we are both part of a single government entity, but in separate agencies, public health, for example, versus economic security?" So, Debbie, do you want to take a stab at that?

Debbie: Sure, Michael for your first question, I would recommend actually the HIPAA presentations that are posted on the dataCHATT website. I think that the issues that you've touched on are based on HIPAA and central processes that are required. For your second one, I'd like to hear examples about Part B and Medicaid programs, there are some states that have shared data between their Part B and Medicaid programs. We are actually one of them in Massachusetts. I'd be happy to share the documentation that we use. We did develop an agreement with our Medicaid program about what data we were getting, how we were using it, and how we were going to destroy it when we were done – very similar to the business agreement that was referenced as an example previously. We did use that same model even with an organization that is part of our bigger, larger entity.

Mira: Again, just to let all of you know that if you have specific questions, you are always welcomed to email us directly and we can pass your questions along to Debbie. Our email address is: dataCHATT@jsi.com. We have another question that came in from Sharon Coleman of Boston, Massachusetts and she asked, "If a program is just starting to collect data for quality assurance and outcomes documentation for a service like a peer program, what are the concerns and factors that the program should be aware of while developing their evaluation plan?"

Debbie: Sharon, thank you for your question. I think what you want to be aware of is first starting with what your overarching evaluation questions are and as you develop them, I would also identify the data sources from which you are going to answer those questions. Finally, have someone review those data before you release them to ensure that you've maintained the confidentiality of the participants. Often with outcomes of quality programs, you are talking about system-level variables, not individual -level variables, but I would set up that review process to ensure that you are not releasing information that may disclose the identity of one of your clients.

Mira: We have one more that came in ahead and then we will check with the operator to see if we have any phone in cue and I also see that we've got a couple of questions that have come in through the chat. So, Becky Bailiff from Memphis, Tennessee asks, "I'm very interested in the store and forward functions as it relates to CAREWare and the protection and integrity of our data. First and foremost, I'll tell you that we'll be glad to pass that comment on to the folks at CAREWare to John Milberg and his team. Debbie, did you have anything that you wanted to add about that?

Debbie: I did, actually on the slide now, if you go to the second slide on resources, you'll see the CAREWare resource. The manual for CAREWare is on the website, if you go to the large manual, it is about 160 pages and start on page 34, you can read it off the form forward process, I was recently looking at it that is why I am familiar with it and understand it. Also, using the CAREWare HelpDesk that you can call the phone number and ask specific questions about it is a great resource as well. The Careware listserv, where you can actually put your questions out to other CAREWare users throughout the country; that can help both answer your questions and help you plan if you are going to use Stormforward and Careware in your data collection.

Mira: Operator, can you tell us if we have anyone in the telephone cue?

Operator: Ladies and gentlemen, to register a question, press the one followed by the four. There are no questions at this time.

Mira: Okay, well, we tend to have a little bit more of a chat-focused attendance, so we will go ahead and jump into the questions that have come that way. So, our first question comes in from Kelly Norcott and she says Microsoft Office and Excel state when you password protect a file that it uses 128 bit encryptions. Does this mean, based on your comments about passwords not being sufficient, that it is only encrypting the password and not the data in the file?

Debbie: Kelly, I am going to take a shot at answering your question based on what I'm understanding. If a file is encrypted, the *file* is encrypted, the *password* is what encrypts and decrypts the file. One hundred and twenty-eight bit encryption is adequate. I would recommend, if you have the option, to go even higher. What I mean by that is there are other options for encryption and another option is 256 bit encryption, but what that does is create the puzzle and mixes up what is in the file so that someone would not be able to have access to it. Based on my comments about passwords not being sufficient, what I meant is when you password protect a file, but you didn't encrypt the file. I would still recommend, though, that you not email those files if you can find another mechanism to transfer the information.

Mira: Again just to reiterate, the 128 bit encryption is acceptable and it is the common standard. The 256 is sort of a gold standard, right?

Debbie: Right.

Mira: Okay, so another question comes in from Robert Adams and he asks: "does using a bonded shredding service satisfy document destruction standards?"

Debbie: Robert that is a great question. Bonded services probably are using what is called the Department of Defense level shredding which is the really, really tiny particles that can't be recreated. You can certainly check with them, but if they are a bonded service, it is likely that they are going to meet the requirement for destruction. What that doesn't address is when you can destroy. I would want you to make sure that you check for the type of data that you are destroying if it complies with your local, state, and federal rules regarding whoever is funding you to collect those data, to ensure that you are following those rules as well as if you have an institutional review board for when you are permitted to destroy those records.

Mira: Thanks, Debbie. All right, our next question comes in from Ricky Hellman, I hope I am pronouncing that right. "Can you address how the required sharing of data elements in Careware as required by HRSA and project contracts is impacted by HIPAA?"

Debbie: You probably can, all of you can, hear my silence for a moment. I want to make sure I'm understanding this correctly. The way CAREWare is actually set up, which again you can contact John Milberg, use the listserv, and the HelpDesk. It actually allows you to restrict sharing. So, I may be misunderstanding your question. You don't have to share data elements in CAREWare. It is set up so that it is actually HIPAA-compliant so it enables you to have varied levels of sharing and you do have to give permission for people to share information. If you set it up and use it that way, it will actually be – it looks like I got clarification: data sharing with a grantee. Okay, so since it looks like you are very fast in your response, may I also ask one other clarification question: can you tell me what your funding is? I want to make sure I am interpreting, I am guessing that you are talking about reporting to a state level or to an agency. So, you are talking about reporting to the party, entity that is funding you.

You are probably – Oh, you are great at responding, thank you. It looks like we have a Part A funded site. It is a Part A reporting to HRSA, okay. Let me try and answer it this way. The elements that you are being asked to report for your client-level data on your RSR are considered de-identified, you don't report the full zip code, you don't report the entire date of birth. You are not required to report the client's name. You are not required to report the client's address. So, if you are asking related to sharing those information, that would not be problematic from a HIPAA standpoint. Now, I would encourage you to look at if there are any local laws or state laws that would require you to review that, but based on what you are sending to HRSA, you are not sending full date of births, you are not sending full zip. I hope that I answered your question, if not, please feel free to put another one in the cue.

I see that there is another question in the chat and if anybody has any questions and they would rather come in through the operator – Operator, do we have anyone else in the phone cue?

Operator: There are no questions at this time.

Mira: All right, then we are going to go ahead and take this question from Robert Adams. We do have plenty of time, so if other people have any questions, don't be shy. Robert Adams asked: "if volunteers have been through confidentiality training regimens, is it okay to use this select group of volunteers for filing of client-related documents?"

Debbie: Robert, and I'm saying these to all, these are great questions, I appreciate you raising them. When I was talking about training, I didn't discern between volunteers or paid staff. I think what is important is that people are trained, they understand the rules, and you have procedures in place. So, for you, if that includes volunteers and you feel that you can provide the appropriate training to them and that is a procedure that works, it seems that that would be fine.

Mira: Do we have any other questions out there? If not, let me just look and see if there is anything else that we have to tell you. I think we are just going to go over here. Oh, we did have one more question that came in on the question from Richie, maybe: "Wouldn't the business associate agreement between the providers and grantees be sufficient for confidentiality?"

Debbie: This may be how I interpreted the previous question. I interpreted it on reporting data from the grantee level to HRSA. If you are talking about agreements that you have in place with your provider, I think you'll find that varies among providers. In Massachusetts we do have business agreements with our contracted sites. That is the way that we choose to approach it. We are a non-HIPAA entity and we still choose to use that approach. Other providers may not use that same approach. I think what is important is that people understand where the data are stored, how the data are used, and how the data are released.

Mira: Okay, well I don't see any other questions coming in, so what we'd like to do is open up the polling option and in just a minute, you should see it popping up. If you look on the right-hand side of your screen now, you'll see that the polls bar has been added and you'll see a few questions there. Please take a moment to answer those questions before leaving the session. It is now time to bring our call to a close, but first I want to thank our wonderful presenter, Debbie Isenberg, for joining us today and I would also like to thank all of you for listening in and participating in today's call. Remember, don't forget to check out dataCHATT, TARGET, and the HAB emails for information about Data Academy, other upcoming events, and our other archived materials from past web conferences. Thanks again for joining us. Good bye.

Operator: Ladies and gentlemen, that does include the conference call for today. We thank you for your participation and please disconnect your line.

[End of Recording]