

**Ohio Department of Job and Family Services  
Office of Workforce Development**

**Transcript of Webinar**

**Personal Data Security**

**Date: October 25, 2012**

## Personal Data Security

[Numbers in brackets indicate the approximate playtime, or time stamp, in the audio version]

GRAIG PELLMAN: Good morning, this is ODJFS Central Office. If you can hear me, and if you can see our PowerPoint, what we'd like you to do is, we'd just like for you to use the chat feature and type in that you can hear us. I see that we're making the connections properly. Please know that the webinar will begin in about three minutes. Thank you.

[3:25]

Good morning everybody. This is Graig Pellman from ODJFS Central Office. We want to welcome you to the final webinar as part of our Legal and Compliance Series. We want to thank all of you for registering. And today's topic is Personal Data Security. I do have a couple of housekeeping items I want to cover with you before we start our presentations. I do want to let you know that we have four presentations today and in between each presentation it will take us about a minute to move speakers around, to get the PowerPoint set up, so we'll ask for your patience at the end of each presentation.

Also, for those of you who are seeking the Certificate of Completion in the Legal and Compliance Series, it's very, very important that you remain logged in during the entire session. That is how we are able to validate your attendance. Also, for those of you who may be watching this in a group setting, the individual who organized this particular webinar will need to submit to us an attendance list indicating who has attended from your location, and the person who registered can get a copy of that attendance list by e-mailing me.

At this time, what we would like to do is begin our presentations. Our first speaker is Ramesh Thambuswamy and he's from our legal office here at ODJFS. Ramesh has asked that all questions pertaining to his segment of the presentation be held until he is done with his presentation. You will be able to ask your questions by using the chat feature and type those in. You can type them in at any time, but we will be holding those questions until he's done going through his PowerPoint. At this time, I would like to ask Ramesh. I'm sorry, I used incorrect language. What you need to use is, you need to use the question feature by typing in your questions. So, at this time, we'll have Ramesh begin his presentation. Ramesh. [5:25]

RAMESH THAMBUSWAMY: Thank you Graig. Good morning everyone, thank you for participating in today's webinar. I appreciate your interest in the topic: Privacy and Confidentiality, which Graig Pellman here at ODJFS asked me to talk about. I was informed that today's participants play differing roles in the One-Stop system and have varying degrees of experience.

The information I'm providing today is not new; it is primarily meant to serve as a foundation for understanding the necessity for safeguarding personal data as it relates to workforce programs. My apologies in advance if you're already familiar with these privacy and confidentiality provisions.

Today's presentation isn't meant to serve as legal advice. As you all know, information about applicants and participants in workforce services is not a public record. The reason for that lies in federal and state law, beginning with the US Code 29USC2935, says that information

## Personal Data Security

maintained by WIA-funded entities is not public if its disclosure would constitute a clearly unwarranted invasion of personal privacy, or it's trade secret for commercial or financial information that is gained from a person, privilege or confidential. [6:37]

The same language also appears in Section 185 of the Workforce Investment Act. The Workforce Investment Act also contains numerous references to confidentiality in Section 403, which pertains to vocational rehabilitation services. So when we're providing workforce services, we need to be cognizant of privacy issues for all of our clients, but, even more so, for individuals seeking or receiving vocational rehab.

In order to understand the term "personal privacy", we have to look to state law, beginning with the definition of personal information. Personal information is defined in Ohio Revised Code Section 1347.01, as any information that describes anything about a person whether it indicates actions done by or to a person, or that indicates that a person has a certain personal characteristic that contains and can be retrieved from a system by name, identifying numbers, symbols, or other identifier. [7:29]

The Ohio Administrative Code expands on that definition and says that personal information includes names, addresses, social security numbers, phone numbers, and information about an individual's social and economic status. Not all personal information has the same level of sensitivity. Some personal information is more sensitive than others and requires an even greater level of care. As I've already mentioned, the Workforce Investment Act specifically mentions the importance of maintaining the privacy of anyone seeking or receiving vocational rehab services.

Federal law also treats student educational records as confidential. Under the Family Educational Rights and Privacy Act, or FERPA, if we acquire educational records of a workforce participant as part of our performance reporting or auditing obligations, we need to exercise care in how we use and dispose of those records. The same goes for social security numbers. And with social security numbers, not only is there federal law to make it confidential, we also have state law that requires public and private entities treat SSNs with a heightened degree of care. This is probably due to the risk of identity thefts. State law also emphasizes the importance of protecting driver license numbers and bank account information. [8:50]

So, any unauthorized access to, or user disclosure of, SSNs, driver's license numbers, or bank account information can create a material risk of identity theft subject to the information and require notification to that individual along with other corrective measures.

Other categories of personal information that require a heightened degree of care would be protected health information, personal financial information, and information identifying individuals as applicants or recipients of public assistance or unemployment benefits. For those performing vocational rehab, or receive or use medical health data, you need to be aware of HIPPA requirements, including notifying individuals whose medical information was wrongfully accessed or disclosed. If you access or disclose your (inaudible 09:40) reputational financial or other harm. [9:47]

## Personal Data Security

I want to talk a little more about unemployment compensation and public assistance confidentiality, since many of the individuals served by One-Stops are recipients of unemployment benefit or public assistance. ORC 4141.21 says that information collected by the ODJFS Office of Unemployment Compensation with Employers and Employees can only be used for UC Program Administration. It can't be used in any other proceeding.

ORC 4141.22 allows the Office of Unemployment Compensation to share certain information with workforce development agencies, county family service agencies. But it can only be used by staff at workforce development agencies and family service agencies in the performance of their duties. If it's not carefully used, it could lead to termination from employment and disqualification of future employment. In addition, there are also criminal penalties that can result from unauthorized use and disclosures of unemployment benefit information. [10:52]

With respect to public assistance applicant and recipient information, ORC 5101.27 says that it can only be used for the administration of public assistance programs, such as cash, food and medical assistance that are disclosed pursuant to the individual's conformed written consent. Unauthorized uses or disclosures can lead to termination from employment and criminal prosecution. The confidentiality laws and regulations apply to anyone performing work at One-Stops who accesses or uses any personal information about participants, applicants, or recipients.

Access by the subject of the information. Individuals are allowed to see, for the most part, their own records and information, but not information and records about other applicants, participants, or recipients. Information made available to individuals online must be password protected and, in many cases, encrypted. In general, access, use and disclosure is limited to program administration, which means those purposes authorized by ODJFS and is directly related to an individual's official job duties and work assignments and furtherance of Workforce Investment Act or Wagner Peyser. Any rules, policies, guidances, memoranda, agreements related to WIA or Wagner Peyser.

The level of access depends on need, and an individual's level of access should be limited to the minimum necessary to fulfill his/her job duties. Access, use, and disclosure by One-Stop staff is not permitted if it is for personal or political gain, or the personal or political gain of others. It's also not permitted if it is for commercial uses unrelated to program administration, or if it would be a violation of state law or administrative rule, or local WIB policy, or outside of the scope of one's official job duties. [12:43]

I already mentioned an unauthorized access to, or user disclosure of, certain information requires that the subject of the information be notified the details of the incident and protective measures that can be taken. I also mentioned that unauthorized use or disclosure of public assistance or unemployment benefit information can result in termination from employment and criminal prosecution. In addition, depending upon the circumstances, it could be civil liability to the individual and local Workforce Investment Board.

Because of the privacy laws and the potential consequences for unauthorized uses and disclosures, it is important to implement security measures to safeguard information. This is also required under State Administrative Rule, which says that individuals who are granted access to

## Personal Data Security

personal information must take reasonable precautions to protect it from unauthorized modification, destruction, use, or disclosure. What's considered reasonable depends upon the nature and vulnerability of the information, the physical location of the information, and any applicable laws, rules, and policies. [13:46]

Because of the department's obligation and desire to safeguard personal information, a completed JFS Form 7078 is required prior to granting access to the department's e-mail system or any state maintained databases. The JFS 7078 lists the responsibilities placed on each and every system user. Those responsibilities are further detailed in Internal Policies and Procedures 3922.

State employees have additional requirements, particularly when it comes to accessing and logging access to personal and confidential information, which are described in OSU Rule 5192216 and IPP3925. ODJFS employees should have already received training and information about their responsibilities with regard to access and log in. Thank you for your time. [14:44]

GRAIG: Do we have any questions for Ramesh? Okay, thank you very much Ramesh.

[15:08]

Just give us a moment while we get our PowerPoint up. Okay, thank you very much for your patience.

[15:31]

This is Graig Pellman again, and I'm going to be spending a few minutes talking to you about Training and Employment Guidance Letter 39-11 from the US Department of Labor. I did send to you in your handouts a copy of form 7078. So you should have that in your handouts from Ramesh's presentation. I've also sent you a copy of this Training and Employment Guidance Letter 39-11. I will be using the PowerPoint to guide my presentation, but you might want to have both of them handy in case you have any questions.

TEGL 39-11 provides guidance to the workforce system on the handling and protection of what is called Personally Identifiable Information, or PII. You're going to find out during this presentation, there's going to be some overlap of information from Ramesh's presentation, but that's because this particular guidance letter is based, in part, off of some of the federal laws that Ramesh made reference to.

What is PII, or Personally Identifiable Information? In the PowerPoint slide, I'm literally going to read this, because it is the exact definition that's in the Guidance Letter. The Office of Management and Budget defines PII as information that could be used to distinguish or trace an individual's identity, either alone or combined with other personal or identifying information that is linkable to a specific individual. [17:10]

There's also a definition of what is sensitive information. Sensitive information is any unclassified information whose loss, misuse or unauthorized access to, or modification of, could

## Personal Data Security

adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled to under the Privacy Acts.

On your screen, you should see some examples of what is protected PII. Of course, Ramesh talked a little bit about social security numbers. That's really one of the big ones in terms of what we really want to be sensitive to, in terms of protection. But, also, in addition to social security numbers, home telephone numbers, ages and birth dates, a person's marital status, the name of a person's spouse, educational history, financial information (which would be credit card numbers or bank account numbers), computer passwords, and, of course, driver's license numbers. Anything that could be used to access a person's private information pretty much falls under the category of protected PII. [18:26]

Here are some examples of non-sensitive PII: first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, a person's gender or race. I do want to make a distinction, to sort of illustrate the difference between non-sensitive and protected PII.

If you go to the previous slide, you notice that one of the factors that's listed under protected PII is educational history, whereas under non-sensitive PII there's a reference to general education credentials. The difference between those two are like this. If you were to say that Graig Pellman is a college graduate, that is a discussion of my general education credential. However, if you were to disclose to the public that Graig Pellman attended Earlham College in 1983, that would be protected PII. So the protected PII has more specific information that you would be able to connect with my personal information. [19:44]

One of the things that the TGEL emphasizes is that you have to be very, very sensitive to the fact that even non-sensitive information, if combined together, or combined with other information, can make it protected or sensitive PII. This would happen in situations where some of this non-sensitive information, when brought together in combination with each other, or other information, would be able to allow an individual to access your private information.

Now, they didn't provide any specific example of that, but for example, if you were to take a person's general name, and perhaps some of their contact information, and then, in combination, that were to bring together a picture of who I am, and you, as a result, would be able to invade my privacy, then that non-sensitive information together would collectively become sensitive PII, or protected PII.

When in doubt, we would hope that you folks would always assume the highest standard and assume that the information is sensitive. That way, you will be protecting the customer, and also you will be protecting yourself against any liability. [20:59]

Has a question come in? Okay, thank you.

At this time, I would like to have you take a look at some of the selected highlights of this particular TEGE. I do want to emphasize that this is just sort of a surface level view of this TEGE, and we would encourage all of you to very, very carefully read the entire document. That

## Personal Data Security

is why we've supplied it to you. I do not want you to think that everything that we're covering in this presentation is comprehensive. Again, I'm just going to touch some of the most prominent features.

We have a question. [21:36]

WOMAN: Much of what we do in core service is connected people to job openings. Resumes have the home phone numbers, and educational information, where they've attended, their graduation dates are also on the resumes. These are posted on the OMJ, and they're also forwarded on the resumes that are sent out to the employers. What's the balance? Do we need a release for any core services, or does OMJ automatically do that if people sign up for the service?

GRAIG: Okay. Well, if a person signs up for OMJ and they voluntarily put their resume on there, they are actually doing that. So if they are voluntarily releasing their information by posting the resume on OMJ, then that is fine. In terms of what you can do, I want to be very, very candid with you. I do not know how that is to be handled, and I think that is a question I think we're probably going to want to follow up on. That's a good question. [22:35]

WOMAN: They want the question repeated. The question was: much of what we do in core service is connected people to job openings, resumes have the home phone number, and educational information, where they've attended, their graduation dates are also on the resumes. These are posted on the OMJ, and they're also forwarded on the resumes that are sent out to the employers. What's the balance? Do we need a release for any core services, or does OMJ automatically do that if people sign up for the service? That was the question from Stephanie that –

GRAIG: That was the question. Of course, the person registers for OMJ, they are, in fact, posting that information on that website. I will get you an answer on the other part of that question. That was a very good question.

Are there any other questions out there? All right. [23:27]

Let's go through some of the features of TEGL 39-11. Regarding encryption, all PII and other sensitive data transmitted by e-mail or stored on CDs, DVDs, thumb drives, etc. must be encrypted. Grantees must not e-mail unencrypted sensitive PII to any entity including ETA or contractors. I want you to notice that, what it's suggesting here, is that the information has to be encrypted. At no particular point is it suggesting that there is any intent to mishandle the data. But even if you are legitimately working with this information, you have to make sure it's encrypted.

In terms of processing PII. All PII data must be processed in a manner that will protect the confidentiality of records and documents, and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. If you have a person who is working with private data, you need to be very sensitive about where they're working and how they're protecting that data when they're accessing it. [24:36]

## Personal Data Security

WOMAN: Question.

GRAIG: Yes?

WOMAN: Michelle Fields is asking, can One-Stop partners receive PII?

GRAIG: In the conduct of their business, yes they can. If they're using it for legitimate business for the stated purpose intended.

WOMAN: Donna asks, if OMJ has an option given to the individual when they put their resume out there, as to whether they want their personal information shown and/or given to prospective employers. I do believe so, that the person is making the choice upfront. [25:15]

GRAIG: Yes. Again if they post things on OMJ and they're doing the posting, this particular TEGL applies to us as employees of the workforce system. Individual customers can do whatever they want with their own personal information. Of course, we would hope that they would be very, very careful in terms of what they choose to share and not share, but that is their decision. This information I'm sharing with you is the state and local systems' obligations of protecting that information.

WOMAN: The next questions is regarding partners receiving PIIs. Does that include the wage records part of the data sharing agreement with ODJFS?

GRAIG: Absolutely.

WOMAN: How does one encrypt? Does this have to go through our IT Department?

GRAIG: I'm going to be very, very candid with you. There are some standards in terms of what kind of encryption software needs to be used in terms of sharing information, and information put on things like DVDs or CDs and thumb drives. I am not an expert, on that but I would consult with your IT person regarding those standards.

WOMAN: Mary (inaudible 26:30) thinks the comment on OMJ, if they choose private, it cannot be viewable to employers. [26:32]

GRAIG: Okay, very good.

WOMAN: Next question is, can you repeat the question prior to the (inaudible 26:49). Okay, that's not really a question.

GRAIG: Okay, maybe they're having trouble hearing you talking – the questions. Maybe you want to talk a little louder. Are we ready to move on? Those are some really good questions and comments.

## Personal Data Security

Safe storage of PII. PII's shall be stored in an area that is physically safe from access by unauthorized person at all times. I don't know how you folks handle your local PC, but here at work, whenever I walk away from my computer, I lock my computer down. I don't want to get into our next presenter's Good, Best Tips about how to store data, but I do that as a matter of personal habit.

I know that the only person getting into my PC is myself. If I'm accessing PII on my computer, I make sure that I'm out of it completely before I walk away from my PC. So it needs to be physically safe. Of course, that can be done a number of ways. I don't want to get into the next presentation. [27:54]

WOMAN: Another question. If we maintain a database of resumes, social security numbers, addresses, names, phone number, etc., does it have to be encrypted?

GRAIG: Does it have to be encrypted?

MAN: If you put it on a disk?

GRAIG: If you put it on a thumb drive, or a CD, or are transmitting it through e-mail, it has to be encrypted. It does not necessarily have to be encrypted if it's safely stored on a server.

Any other questions?

Accessing, processing and storing of ETA Grant PII data on personally owned equipment at off-site locations is strictly prohibited unless approved by ETA. We assume that everybody's working out of their offices. [28:48]

Advising staff about PII. Grantee employees, and other personnel who have access to sensitive data, must be advised of the confidential nature of the information, with safeguards required to protect the information, and that there are civil and criminal sanctions for non-compliance. Now, we are providing for you today a very surface level overview of this topic. It is up to the local offices to make sure that their employees understand what is expected of them in terms of protecting PII.

Regarding PII access. Access to any PII created by the ETA Grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the Grant Agreement. That means that, just because a person works in the office, that doesn't mean you give them access to the information, if their duties don't require it. [29:52]

Grantees must not extract information from data supplied by ETA for any purpose not stated in the Grant Agreement. Now, I would just like to make a comment here. You have access to all this information, to conduct your business in your local One-Stops. You cannot access this information for any other purpose, other than what's it's designed for, or the reason it is given to you. That is also to say that, even if you have another benevolent purpose, you still cannot use this information for any purpose other than the reason it is being supplied to you.

## Personal Data Security

At this point I'll take any other questions regarding this TEGL. Again, I want to emphasize I think it's very, very important that you take a look at this TEGL and read it thoroughly. Again, Ramesh's presentation talked about the laws that govern the protection of private data. This particular TEGL sort of fleshes out some of that information for you. This is, to me, a very, very understandable document and if you have any questions regarding it after this particular webinar, you can certainly e-mail us for clarification. [31:11]

Are there any other questions?

WOMAN: One question. Does the state have one master encryption program which we all can use?

GRAIG: I'll tell you what. Our next presenter can address that issue. There's another question?

WOMAN: Another encryption question. Encryption is required for an internal emails as well as externals, is it?

GRAIG: Yes.

WOMAN: And that will be covered on –

GRAIG: It will be covered in the next presentation. These are good questions folks. Is that all? Okay. What we're going to do at this point is, I'm going to mute the microphone again while we get our next presenter set up here.

Our next presenter is James Matheke. He is from the Office of Information Services here at ODJFS, and he's going to be speaking to us regarding some Best Practices in terms of protecting personal data. So give us about sixty seconds to get this presentation set up. [32:13]

[33:25]

JAMES MATHEKE: Hi, this is James Matheke. I'm the Information Security Architect at ODJFS. I'm an engineer by trade, so if you have any technical questions regarding encryption or anything else that was brought up, I can try to answer it to the best of my ability, and, hopefully, to your understand as well. If you don't understand anything I'm explaining, I tried to keep it to using – let's say, common terms that the average person would understand. But sometimes I do go a little deep. Stop me if you don't understand. I don't want to get to the end of my slides and say, "I don't understand anything you've talked about." [34:06]

I think everybody understands that security is really everybody's job, and we have an obligation to protect, really, our employer's data, their operations, information systems, and, really, the people themselves. If we have this in mind, I think we have to focus on what are our individual responsibilities related to security. Really, that's the heart of my conversation with you. I want to cover the Best Practices, and I expect you to ask questions. You've asked some of these questions, I've heard them. I'm going to try to cover it in relation to my slides, and if I don't cover it in enough detail, please ask questions.

## Personal Data Security

What are your responsibilities? I think the first and foremost is really the password. I believe you heard that we are asking you to not write down your passwords. That really gets difficult because you have a number of systems that you access and every system may have these rules, or policies, that they expect your password to adhere to. They would be like upper and lower case, special characters and numbers. Some systems require all four, and they may say you have to have two special characters.

That becomes really hard for people to remember their passwords. A lot of people create conventions with their password. If you do start creating conventions, we ask that you keep the conventions different between your businesses and personal – meaning, we don't want your personal password to be used as a business password. [35:48]

Secondly I'm going to go through and bullet, point by point, and if you have any questions regarding each one, feel free to ask.

WOMAN: We have one that asks, how do I encrypt my e-mail from ODJFS?

JAMES: We'll cover that. That's on the next slide. We'll get to e-mail encryption.

WOMAN: The next one is: IT Department asks for you to give them your password in an e-mail. Do we respond to the e-mail with the password, or how do we share that information?

JAMES: That's a really good question. You NEVER share your passwords. Our IT people have procedures and methodologies in place where they can bypass your password or get access to your system without your password. Never share your password with an IT person.

WOMAN: Can we write down some variations of our password?

JAMES: In general, do not write down your passwords. I know there are password protection tools that allow you to store your password in them. We ask that you not write them down, period. [37:00]

The next thing we have are approved devices. We have to make sure that we are using approved devices to connect to the network, for business purposes. What I mean by that is, we have applications that we call Internet Applications and Intranet Applications. The Internet Applications means that you basically can access the application from anywhere. In those cases, you may use, in certain circumstances, personal devices to get access to those applications. If something's on the Web, and you can access it from the Internet, you typically can use your own personal device.

Regarding that, if we have an Intranet Application. In those cases, for ODJFS, we provide state computers, or the county computers with the VPN access, where you have to have a token to connect to our internal network, to get to our internal applications. In those cases, we really insist you use only the approved computers to connect to our internal network.

## Personal Data Security

The reason why is, we're worried about the data that you access, and how it gets stored on the computer – because we have an obligation to also cleanse that data from the computer, let's say, when you end your employment with the JFS or the county. Our data responsibility extends beyond the terms of the employment. We want to make sure that we cover the device.

I know sensitive data can be accessed from our e-mail system. In those cases, you have to be careful of what you load on your personal devices. Myself, I access my e-mail from the Internet, but, in those cases, I primarily keep it to the calendar and looking at the topics of the messages. If I know I'm going to access sensitive data, then I get to an approved computer and get inside the internal network, and then look at the content of the messages.

The key point to understand there is – and I'll cover this again and remind you – that e-mail, the subject line is not considered sensitive. You should never put sensitive information in the subject line, because, when you send it out externally, or internally, the subject line is always visible. Never put sensitive information into the subject line.

WOMAN: A question about the password. She wanted to be specific and say, I mean it's not the exact password, but if it's close to. So I'm assuming like, January1, January2. Are you able to do that?

JAMES: No. You shouldn't write it down. Basically, the rule is: Do not write down or share your password. [39:58]

I think Graig covered this already, protect using your screen saver when you leave your PC. Other precautions: personal devices. A lot of people get smartphones and other devices and don't password protect their devices. You really should protect all of your devices with passwords, and they shouldn't all be the same. If you leave your office, you should probably lock your door as well. So the screen saver is just like closing your door.

WOMAN: We have a question coming in. It's probably going to be for you Graig, or who was the last speaker? This is in regards to the last speaker talking about protected information. I manage a WIA Youth Program and place youths at work sites in the community. You say that ages and birthdays are considered protected information. Yet, according to the Bureau of Wage and Hour Administration website, the following statement is listed: every employer shall post in a conspicuous place frequented by minors, a printed abstract to the minor labor laws that are furnished by the Wage and Hour Division, and a complete list for all minor employees, which shall contain, at a minimum, the minor's name, age, date of birth, and occupation. What are we supposed to do? [41:37]

GRAIG: I'll be honest with you, I don't understand your question completely. I can tell you that within the Workforce Investment Act Program posting minor's personal information in a public space is not to be permitted. I'm not certain that your question is suggesting that the federal office indicated wants you to post personal information. That doesn't sound right to me, to be honest.

MAN: They can keep a list confidential.

## Personal Data Security

GRAIG: They can certainly keep a confidential list in their files, but in terms of posting a minor's personal information on a wall, that would not be permitted. If you have any questions about this, more specifically, please give me a call. My telephone number is 614-644-0677 or e-mail me, and we'll work through your specific question. But I'm very, very certain that we are not to post private information in any public space. [42:37]

WOMAN: The next question is (inaudible 42:38) including the last four digits of the social security number with the client's name, is that acceptable or not?

GRAIG: That is still private information. That is considered protected and sensitive PII. So you cannot publicly release that information as well.

WOMAN: Someone makes the comment, basically the two federal offices need to talk to each other and figure out which one's wrong.

GRAIG: If you could please contact me, I would like to follow up with you personally so we can get some clarification.

WOMAN: Okay, the next question we have is, how do you determine who in a business has a different level of clearance for information? For example, HR has access to personal data for HR purposes. But a floor supervisor should not have the same level, correct?

GRAIG: You're talking about a private business?

WOMAN: I don't know.

GRAIG: Understand, what we are talking about in this presentation are the One-Stop systems' obligations in terms of protecting private identifiable information. What an employer would do with that data is outside the scope of this presentation.

JAMES: One comment on social security numbers. If you have the last four digits of the social security number, if you have any information regarding the individual you can easily derive the rest of the social security number, and that's really why it's considered sensitive information.

GRAIG: Thank you. [44:33]

JAMES: The next bullet item is running scheduled virus scans. Make sure you have virus scans as well on your personal devices and smartphones. If you access any system, the viruses and Trojans that are available that are out on the Internet today, not only capture your passwords for your systems, but they will mail them in.

GRAIG: Just for clarification, could you explain to the audience what a Trojan is?

JAMES: A Trojan is, in layman's term, there's really not that much of a distinction between the two. But a Trojan is really, in essence, a malware that gets placed on a computer that give access

## Personal Data Security

to somebody else to your computer, let's say at a later time, at any time they want. But consider they call it like the Trojan horse. That's what a Trojan is. One of the problems that we have within our agency today, is that people go to websites and they get infected, and even with our virus scans that we run within our agency, on servers and desktops and it will check any downloads that you do and try to look for viruses.

We still do get infected with viruses that basically do a key logger and capture your ID and password and will mail that to the author of the virus. What happens there is, then we get notified or we detect that, and then we may have to wipe your computer clean. That's why, even with up-to-date virus scans, you may not be able to, let's say, keep yourself from getting infected. [46:10]

The other thing that I want to point out is portable computers and media. You need to protect them from loss or theft. This includes encrypted thumb drives – any encrypted hard drives, as well as portable computers or tablets. The key thing to understand there, with portable computers like laptops, a lot of times you have these locks that you can place and attach them, in case you're briefly away from your office and want to keep that computer from getting stolen.

The media. The idea is to keep it on your possession. My son goes to school, he has a hard drive. They have a lanyard and a badge; then they attach their thumb drive to their lanyard, so that it's always present to the student. The students also have requirements that they have to wear the badge at all times within the school. That helps prevent the loss of his thumb drive. [47:14]

I think we covered this a little bit, and I can go into more detail. If you are provided with protected service storage space, store information on it rather than your own hard drive. Within our agency and the counties we support, the hard drive on our desktops are not encrypted. We ask that you not store the information on your local drive, and you store it on your "P" drive, or the Public drive, or a private drive that you have access to from our agency.

In those cases where you store it on a secured area, that means, typically, depending upon your ID and password, you get rights to certain directories, and only other people with privilege to get access to those directories can get access. In those cases, depending upon the sensitivity of that, you may want to encrypt those files before you place it on those secure drives as well. The main reason we do the protected server storage is that we do not backup locally your hard drive.

So if your hard drive on your computer, for any reason, got infected with a virus, we would wipe out that entire drive and you would lose all of your data. If it was placed on the server, the servers are backed up and if we got that infected we would restore to the earlier date, where we knew that the infection didn't occur, and then we'd be able to restore the file. [48:49]

If you deal with sensitive information, we covered some of this in Graig's presentation, but I will review it. You need to do encrypted file transfers. The state basically approves two types of encryption and this is working with the Feds and they have a standard called FIPS 140-2. Basically it says that Triple-DES and AES encryption are permitted.

## Personal Data Security

If you have any questions, or if your IT people have any questions regarding what is an approved file transfer mechanism, they can contact us. People typically lump together all the secure file transfers at secure FTP. Really, with secure FTP, there are really two different protocols that are supported. We just have to keep that in mind.

Use encrypted e-mail messages. I heard someone mention GroupWise. GroupWise e-mail is encrypted. When I send it from one individual to another, those messages are encrypted and we do have mechanisms to send mail outside of our agency, and we've just transferred that to OIT, where we do encrypted messages where you put, I believe the word is "secure" – I'll have to look that up; I haven't done it recently – in the subject line to indicate that this message needs to be encrypted. [50:15]

Again, as a reminder, the subject line is not encrypted. So when you send an e-mail message out, even though you're sending it through an encrypted means, whether it's GroupWise or through OIT with our outbound secure email service, you should also probably, depending on the sensitivity of the data, attach the sensitive information in a file that is also encrypted. The reason for that is, the majority of the cases where we have an incident with sensitive information being released to the public, is it's usually sent to the wrong individual.

You can have a to-list or a copy-list, or you're doing a reply and you think you're replying to the correct individual, and you basically send sensitive information to the wrong individual, because they were on a copy-list. In those cases where you do attach an encrypted file, we also ask that you contact the people that you're sending the message to, and relay the password for the encrypted file. That's important because you want to use a different mechanism than attaching it, or including it in the e-mail, or just simply sending another e-mail with the password. [51:37]

GRAIG: I have a question. Let me use a hypothetical example. Let's say I wanted to send to one of the local One-Stops a file that had partial social security numbers and it was in an Excel database. If I password protect that Excel database, is that encrypting it or not?

JAMES: Excel, I don't believe, encrypts it. We ask that you use WinZip. For JFS employees, they have Winzip.

GRAIG: Okay, thank you. [52:08]

JAMES: We got a little off track there. Encrypted media and hard drives. The key to understanding encrypted media and hard drives is, we actually use a higher level of encryption than, let's say, WinZip. WinZip is a password-based encryption scheme. The scheme is used to encrypt a secure hard drive, like what we use with SafeBoot, or, we're actually deploying another encrypted thumb drive now. They use what we call an encryption key to encrypt the data.

One of the things that we have to be careful about when we encrypt the data, is that we also have to be able to unencrypt it. Anything you use to encrypt the data, we're also mandated that we have to be able to unencrypt that data. So we can't just say that we've encrypted the data and

## Personal Data Security

we've protected it; we have to have a way to recover that data in the case of any kind of investigation that we have to conduct. [53:15]

The schemes that we use to protect media and hard drives, we have recoverable keys for those. If, for any reason, you forget, for example, your SafeBoot password to a JFS laptop, we're able to recover that key and get access to the data even though it's encrypted.

One of the things is, we talked a lot about sensitive information and the key thing that you have to worry about when you're using personal devices is, really, the eavesdropping. If you access sensitive information in a public area, make sure you're aware of your surroundings, and make sure you're aware that other people can hear what you're talking about, or possibly see your screen. At the end of the day, we ask that you shut down your computer and also store all of your sensitive information, and lock your office door if you have an office door.

Finally, any security incident must be reported to your appropriate security officer. Within JFS, all incidents have to be reported to the Office of Chief Inspector. Finally, are there any other questions? [54:33]

WOMAN: First question is, in the example of the PII, I don't see the personal address, only the business address. Where does personal address fall?

GRAIG: A personal address would be considered secure, or protected PII. So that would be in the highest level of security.

WOMAN: In regards to Trojans, should any unfamiliar sender in an e-mail be considered spam mail?

JAMES: Read that one more time?

WOMAN: In regards to Trojans, should any unfamiliar sender in an e-mail be considered spam mail?

JAMES: Spam mail is really considered Junk Mail. When someone is trying to hack your system, they are trying to get to you with some level of social engineering, like you may know who they are. Bottom line is, you should refrain from opening anybody's e-mail that you don't know who they are, and definitely don't open any attachments if they have included attachments – because that's how Trojans really get installed on to your system.

WOMAN: The next question is, has the state finalized the encryption process for emails going out to individuals externally to GroupWise? My understanding is that there was a system, but then it was pulled due to some technical issues that came up. Is this back in place now? [56:20]

JAMES: I'll have to follow up with you on that.

## Personal Data Security

WOMAN: Okay, next one. This person was asking about whether she should save information onto her “P” drive, but what she’s asking now is: so everything that’s on my desktop, should that be backed up and saved on my “P” drive as well?

JAMES: Absolutely. You’re “P” drive is where data that you have on your computer should be stored. Your “C” drive or your local drive, even though it’s encrypted, it’s not backed up. Like I said, if your laptop or your computer were to be infected, we would just wipe out your drive and you would lose all your data.

MAN: And the desktop is your “C” drive.

JAMES: Right, your desktop is your “C” drive.

WOMAN: Is it okay to e-mail a social security number like this, with all x’s, and the last four digits? I think we covered that already. [57:24]

JAMES: It’s still considered sensitive information. Depending upon the context of that, you’d have to check with each of the program areas to see whether that was permitted for the appropriate business reasons.

GRAIG: It has to be encrypted. It has to be encrypted in the e-mail, even if it’s the last four digits. Now again, I’m going to make sure that I’m correct in hearing this, GroupWise is encrypted.

JAMES: Correct. As long as you’re sending it internal to another GroupWise recipient.

GRAIG: Okay, the answer is yes. You have to treat the four digits just like you would treat the entire social security number if all the digits were there.

WOMAN: How do you encrypt a flash drive?

JAMES: Flash drives usually have software that’s included that has encryption software. So if you get for example, Western Digital’s Passport, it comes with software to do the encryption already. So they password protect the drive, and you have to basically enter a password before you have access to the drive.

We are working to release within JFS a flash drive, or thumb drive that uses an encryption key that is recoverable – where the system actually maintains the key for you. The issue is, normally, if it’s password protected, the software is already on the drive that does the encryption for you. [59:03]

WOMAN: Okay, the last question that we have: how do we obtain information on how to use WinZip?

## Personal Data Security

JAMES: I don't have the answer to that except using the Help within the tool itself. And if you do have questions, if you're within JFS, you can go always to the OIT Help Desk to get help on how to use the tool. I don't believe that there is a specific document that you can refer to.

WOMAN: My understanding is that when we're sending information through GroupWise, we are to use JFS Secure in the subject line.

JAMES: The secure option was the outbound e-mail security, but the tool that I think they were indicating had a problem and may no longer be available. I believe JFS Secure is how you secure the information when it's outbound. When it's internal, GroupWise is already sending the data encrypted. [1:00:16]

WOMAN: Does password protecting Word and Excel documents mean that we don't need to encrypt them?

JAMES: I'm not aware that it does encryption to the level we need it to. So I would password protect it within WinZip.

WOMAN: This person said, I was given a jump drive with sensitive information. Do I need to encrypt the jump? The jump drive was not mine.

JAMES: Say it one more time?

WOMAN: I was given a jump drive with sensitive information. Do I need to encrypt the jump? (I assume the information's on there.) The jump drive was not hers.

JAMES: Right. I would really refrain from using other people's jump drives, because they could contain viruses or Trojans. And if you do attach it to your computer, I would run a scan. We really would refrain from using personal jump drives. [1:01:17]

WOMAN: Then this person has a comment. Just an FYI – GroupWise, there's also an encryption feature which suppresses subject matter. (Inaudible 1:01:38).

JAMES: All right, thank you.

GRAIG: I have one comment that goes along with James' presentation. Recently the Ohio Department of Job and Family Services, as well as the county Department of Jobs and Family Services, employees were required to go through a mandatory training called Securing the Human. It was a very, very broad-based, very easy to use, online training program that deals with the broad topic of protecting private data. Some of it would apply to your work, some of it wouldn't. It would be broader than that.

If you are not a CDJFS or ODJFS employee and you are interested in going through that training what you can do is contact your local county Department of Job and Family Services and ask them to sign you up for this training. The CDJFS, in turn, has to contact the state, and you would receive a unique log in protocol, where you would be able to access this training.

## Personal Data Security

If you are interested in doing this training, I would strongly recommend that you contact your local CDJFS right away, because we're really past the deadline of when this training was to be completed, and it's soon going to be shut down. It's really, really good training. It takes about 45 minutes to go through all the modules, gives you a lot of common sense information. Again, if you're interested in doing this and you're in the One-Stop and you've not gone through it yet, call them today and ask them to sign you up, because that's the only way you can access this training. [1:03:35]

JAMES: I want to comment on that training, the state of Ohio acquired that training through an organization called the SANS Institute. The best practices that I've outlined in this presentation also came from the SANS Institute.

GRAIG: Very good. Any other questions for James?

WOMAN: I have a couple more questions here. How do we safely fax authorizations with sensitive information to service providers?

JAMES: Unfortunately, fax is a really old technology. It does have capabilities to do encryption, but it really depends upon the system that you're using to do that data. In general, I know that, even within the IRS, they have allowances that basically say that fax is still permitted. Basically, if you can avoid using fax, I would avoid using fax. That's not the way we would typically work our systems. [1:04:50]

WOMAN: The next question is: If a client is in the resource room and they're not able to open their document with their thumb drive, are we allowed to open it from our desk computers to assist them? And that would be like out in the One-Stop.

JAMES: I guess I'm a little confused. Why they wouldn't be able to – we would strongly refrain from opening or attaching anybody's thumb drive to our computers.

WOMAN: The next question is: What was the name of the training, again, that you were referring to?

GRAIG: It's called Securing the Human. Sort of an odd name, but the training is very, very good. Trust me, I found a lot of information, a lot of good common sense tips on how to protect my personal information, as well as information in my state capacity.

WOMAN: Is that for only state employees though? (Inaudible 1:05:46).

JAMES: State and county.

GRAIG: State and county.

WOMAN: State and county.

## Personal Data Security

GRAIG: But if you're in a local One-Stop, and you contact your local CDJFS and identify yourself as working at the local One-Stop, they can sign you up for the training. That is the only way you can access the training, and do it quickly, please. [1:06:08]

WOMAN: That's it.

GRAIG: Well, thank you very much. We're going to go ahead and mute the microphone and set up our next presentation. Please give us one minute.

[1:07:37]

JULIE WIRT: Good morning, my name is Julie Wirt and I am the WIA Program Monitoring Supervisor and with me today is Diana Skinner who is the WIA Monitoring and Auditing Manager. Today, we are here to talk about how our program monitoring will be capturing data sharing when we're out doing our program monitoring. What, in detail, we're going to be looking for is how is the local areas conducting their ability to safeguard and maintain confidentiality.

Specifically, our monitoring will be gearing towards the data sharing that is being done with wage record information. However, how you handle the wage record information, it should be the way you're handling all confidential information that you are receiving. So, in a sense, we'll be reviewing the area's ability to maintain confidentiality.

All areas that are currently receiving wage record data has signed a Data Sharing Confidentiality Agreement. This agreement is basically an outline of everything you learned this morning. It's the ability to safeguard and maintain confidential information, of all the information that you receive, how to restrict that access to wage record information, as well as any confidential information that the area has received. So, only those who are authorized to receive that information. Also, the wage record, the data sharing agreement has also given us the authority to have a list of individuals who will be authorized to access the information.

Finally, this agreement has outlined that all staff members who have access to the information, will receive some sort of training, or been advised of the information that they're receiving. That is in the sense their confidential nature of the information, how to safeguard to protect that information. And of course the civil and criminal sanctions for non-compliance.

With this agreement in place between the department and local areas, WIA program monitors will be reviewing with the areas the local processes that have been put into place to ensure that the terms of this agreement are being upheld. It is extremely important to ensure that all confidential information, including the wage record information, is being kept in a confidential manner, and that this information is being used only in manners that have been approved through the agreement. Therefore, we have modified our Comprehensive Monitoring Guide to include the discussion regarding safeguarding confidential information and a wage record data.

[1:11:06]

The first question that we have added is, Does the area provide monitoring and oversight regarding wage record information – including tracking what staff has access to wage record

## Personal Data Security

information? This question really is geared towards understanding how the area is overseeing the use of confidential information, and wage record information. The agreement that is signed by the local area and the ODJFS specifically states that wage record information is restricted only to those who have been authorized.

What the program monitors will be looking at is how the area ensures that this information is only being shared with those individuals. How is it done? So, the questions really are getting at the heart at how the local area is ensuring that those who have been granted access, who have access, are only the ones that are viewing this information. [1:12:31]

The second that has been added to the Comprehensive Monitoring Guide is, Does the area provide security and confidentiality training associated with wage records data sharing with the staff? Of course, this is also with confidential information in general. The purpose of this question is to learn whether or not the area advises staff regarding the confidentiality of wage record information, and if they did, how did they do that? Did they do it through a training, one-on-one, information sharing?

Really getting at to how was –making sure that the staff who have access to the information understands – the confidential nature of the information, how to transmit this confidential information, what to do with the confidential information, and then, finally, what is the ramifications, if that process is not upheld.

DIANA SKINNER: I think that most of you have been through several monitoring seasons with us and know that the key to what we're looking for is documentation of what you have done. So whenever you do your training for your staff, it is always good to have a copy of information you discuss, who all was there, and that will provide information that we can check off to make sure that it has been provided to everybody who needs that type of training. [1:14:14]

JULIE: The third question is in regards to the steps that the area has taken to ensure that the wage record information is kept confidential. It's – what types of policies and/or procedures that are implemented by the area to ensure that confidentiality of wage record information is monitored, tracked and maintained.

This really goes towards all confidential information, even though we're specifically saying wage record information. Does the area have any policies, is there any formal policies that are in place to maintain confidential information, or is there any procedures that are being implemented? Again, as Diana just said, the best way to ensure that the procedures are upheld is if you have them in writing. Does the staff know these procedures? Do the staff know the policies? That is some of the things that we are looking for.

Also, the agreement talks about destroying the information once the records are no longer – that way we – no longer needed. So what we are looking at is, how are they being destroyed? Are they printed out and shredded? Are they being deleted? How is it being destroyed? [1:15:37]

JULIE: I think one of the biggest things that have been talked about is how this area stores the confidential information. Many of the other trainers earlier today went through the different

## Personal Data Security

steps to be done. What the monitors will do is, while they are there on-site monitoring visit, is to observe how the local area stores the information. Are they in locked bins, if they are printed out? Are they on computers that have the proper password protected when you're away from your desk? And that type of information.

Also, the monitors will be reviewing the list of individuals who have been granted access, so that we know that they are the ones receiving the information. We also ensure that that list is being kept updated as staff changes, so that ODJFS knows who has that access to the wage record information.

DIANA: A general rule of thumb, you know, we've just been given access to the wage record so that's really something that should prove beneficial to us in doing our jobs. So we do want to make sure that we do treat that information very carefully, so that we don't violate anything. So the wage record is going to continue to allow us to have access to that information.

A good rule of thumb is just to make sure that we treat everybody else's information with the same caution and respect as we would treat our own. If we do not normally throw information in the trash, or recycling bin – especially if it's personal and confidential information – if we would shred it, then we need to treat everybody else's the same way. Just need to have a heightened awareness that this is somebody else's information – so, would I do that with my own? Treat it in that manner. [1:17:54]

Also, as far as having access? Very few people have been given access to go onto the system and to check into the wage record information. But if you're going to make copies, you have to be very careful, too, about who will look at those. And I guess I'm going to throw this out there – I think it's pretty common knowledge, but, just resist temptation. Information that is available in the wage record is – some people might be tempted to look and find something that is not related to one of their clients. That can get you into a lot of trouble. You just need to use it strictly for the purpose that it was intended for, and that is to look at client information to use to validate the purposes that we need. [1:18:51]

Are there any questions?

WOMAN: One question. Who was given access to wage record information?

DIANA: Actually we are pulling information down and putting it in a file that – Is that right, Graig? or –

GRAIG: That I do not know. I know that some areas that signed agreements to get that information, but how that happens, I cannot tell you.

DIANA: Okay, I didn't know if everybody was given that access – I mean, every local area, somebody in that area.

GRAIG: Not every area.

## Personal Data Security

DIANA: Who is handling that?

GRAIG: I don't know.

DIANA: Don't know. Okay.

GRAIG: One of our questions we'll have to answer.

WOMAN: The next question is basically the same thing. Is wage record access forthcoming to selected One-Stop staff? Currently no one within our WIA staff has access to wage record.  
[1:20:00]

GRAIG: Wage record information is being provided after an agreement is signed, and I want to be very honest with you, I do not know how many areas are using that information right now. We can ask that question and get back to you.

Are there any other questions? I would like to just finish with a comment. We've taken about an hour and twenty minutes now to do these presentations. This is not only a very important topic, but it's also a very, very large topic. There is no way that you can spend only 80 minutes and cover everything that you really ought to know regarding the protection of personal data.

So, we would like you to assume the attitude that this just sort of the beginning of the discussion and the beginning of you learning ways of protecting information, and that you would continue, on your own, to continue to read all of the information that we send out to you. All the information supplied to, from the various sources, so that we can do our due diligence and protect the information that the customers expect us to protect, and that the laws expect us to protect.

So this is not the end of the presentation. It's really, sort of, the beginning of a process, because, as we continue to work with this data, there are always ways to get this information that change on a regular basis. Please consider yourself lifelong learners in this regard. [1:21:40]

Are there any other questions before we conclude this webinar?

WOMAN: One more. The data sharing agreement seems to be specific between JFS and WIA staff, is that correct?

GRAIG: I do not know the answer to that.

DIANA: Between JFS and local area.

GRAIG: According to the information supplied, the agreement is between the Ohio Department of Job and Family Services and the local WIA area (local Workforce Investment Board).

WOMAN: Local partners are asking if they can also gain access to wage record information. Is this permissible?

## Personal Data Security

DIANA: Again that's something we'll have to –

GRAIG: What we're going to do is, we're going to pull down this transcript from this particular webinar, and we'll catch these questions and try to get some sort of response. But I don't have an answer for you right now.

MAN: The sharing of wage record data is determined by the Office of Unemployment Compensation, we don't have any representative (inaudible 1:22:45).

GRAIG: Any other questions? All right, hearing none, first of all, I want to thank everybody who participated in this particular webinar. Also, a special thanks to all of you who participated in the entire series. We appreciate that, when we send out to you the evaluation tool – I'm sorry, do we have another question?

(Inaudible 1:23:20).

GRAIG: Okay, I'm going to be sending out the evaluation tool probably, within the hour. What I'm going to ask you to do is, first of all, answer the questions specifically regarding this particular webinar in those first several questions, and then, at the end of the survey, a place for you to put in additional comments or suggestions. If you have anything you would like to say about the entire series, whether it was useful to you, or not. Or suggestions for the future, we would appreciate your input. The only way we can really serve you is to know what is useful and what is not in terms of the training that we provide. So, thank you all very much for participating in this series, and we'll be in touch with you very, very soon. Good bye.