Amber Wilder:

Our session is called The Agents of SHIELD: Data and Privacy and Security. We will leave the last five minutes of the session for any questions. Please use the chat for any questions that you have for the presenters. We'll get to as many as we can at the end of the session. I will also be monitoring the chat. The information for applying for CLE is posted on the Permanent Commission website. An email will go out after the conference about CLE to all registrants. There will be an online form for each day. A code will be read during the session, which you will need to report on your CLE form. You must attend the whole session and must complete and submit the online form within a week of the conference. You will also need to know your attorney registration numbers. I will also post some information about CLE in the chat as well as the link to the agenda so that after this session you can go to your next one. Okay. Ellen, if you don't mind, the next slide.

Ellen Samuel:

Yes. Thank you Amber.

Amber Wilder:

No problem.

Ellen Samuel:

Welcome everybody. As Amber said, we're going to be talking a bit about the SHIELD Act and also about data privacy and some issues that you may be seeing in your firms and what we think you can do to start protecting yourselves and your firms. For our agenda, we're going to talk about what the SHIELD Act is, then we're going to do a bit of some time on attorney ethics: why you should care about privacy and security. We'll talk about some tales from the field, things that are happening in our organizations, and then we'll spend some time on what we think your next steps should be. What should you do now? Before we do that, I'd like to have us introduce ourselves. So Sandy, can you start?

Sandy Coyne:

Sure. I'm Sandy Coyne, Deputy Director of Operations here at LawNY and oversee IT. So this is pretty important to me.

Ellen Samuel:

And Lori.

Lori O'Brien:

Hi everybody, I'm Lori O'Brien. I'm the incoming Executive Director at LawNY and have been with the organization for a bit now. And when I'm thinking about technology, I'm also thinking about what does that look like on the ground for those users and for our staff that are advocating every day. Thanks.

Ellen Samuel:

Thank you. I'm Ellen Samuel. I am the Director of Consulting at Just-Tech. I am also an attorney and a Certified Information Privacy Professional. I am the former Supervising Attorney of Intake at Prairie State Legal Services. I've spent my entire legal career at Prairie State doing a wide variety of legal aid issues. And then Amber, will you introduce yourself?

Amber Wilder:

Sure. I'm Amber Wilder, one of the Project Managers at Just-Tech.

Ellen Samuel:

Thank you so much. Okay, so we're going to move on to Lori, who is going to talk a little bit about what the New York SHIELD Act is.

Lori O'Brien:

All right, so the New York SHIELD Act (Stop Hacks and Improve Electronic Data Security Act). What was the purpose? It was really to keep pace with current technology. There were rules and laws and regulations on the books already. This expanded them and really tried to get us up to speed with more guidance in terms of the safeguards organizations can put in place. So when you're thinking about being in this room, does this apply to you? It applies to any person or business that owns or licenses private information of a New York State resident. So it's not just organizations that operate in New York, it's also organizations that operate elsewhere, but process private data for New York State residents. So think about the information you're keeping, right? We're keeping information about our clients, we're keeping information about our employees. This applies to you. Now, this was signed into law in 2019 and it became fully enforceable in 2020. And I think that's important to stop and think, where were you in 2020? What was happening in the world right then, right?

There was this mad dash to get out of our offices. To set up remote technology, to maintain accessibility to our clients and to make sure our organizations were fully functional. And at the same time, additional rules came down about how you safeguard that data. Now the SHIELD Act expands and amends the 2005 Information Security Breach and Notification Act, and it does that in a few different ways. So let's talk a bit first about the types of security breaches that are covered by the law. Under the 2005 law, a security breach is defined as “an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of private information.” The SHIELD Act expanded that definition of a security breach to include any access. When we think about access, access is referring to “viewing, copying, downloading private data.” So that was a larger expansion. When you're thinking about a data breach in your organization, you’re thinking whether computerized data was accessed or acquired without authorization or without valid authorization and in such a way that compromises security, confidentiality, or integrity of that private information.

When we're looking inward at our organizations, what do we really need to know? We need to know what is the private data we're keeping. Where do we store that? How does it flow into and out of our organization? So what is private information? Under the 2005 law, private information was “any personal information concerning a natural person in combination with one or more of a few data elements.” Those included Social Security numbers, driver’s license numbers, account numbers. The SHIELD Act also expanded that definition so that the definition of private data includes “any personally identifiable information that can be combined to reveal the identity of a New York State resident.” So again, it could include a Social Security number, driver's license number, but it could also include security answers and questions, usernames and passwords, biometric data, retinal scans, fingerprints. We're not there yet, but some organizations and businesses may be. It can also include things like payment information, medical data, and on and on.

Let's talk about you had a breach, right? Some of the ways you could have a breach: maybe an employee lost their laptop, or it was stolen. Once you have a good reason to believe that you suffered from a data breach, you are obligated to provide notice. The SHIELD Act goes into detail about what that notice should consist of. Just to briefly go through some of that, your notice really contains your contact information. Contact details for state and federal identity theft protection agencies, information about what data was compromised. And although it's not in the SHIELD Act, you might also want to use that opportunity to reassure people that you're taking this seriously. What actions are you taking to control the breach, what steps that they can take. And if you've ever gotten a notification about a breach of information, those notifications kind of follow the same suit, right?

If I've heard from a company that holds my information, they're going to tell me things that I might want to do going forward to make sure I'm checking to see that that breach doesn't have any ill impacts. The SHIELD Act also talks about how you distribute that notice. It gives you various options including substitute service if you don't have the specific contact details for that individual. The SHIELD Act also talks about timing. Now it doesn't give you really specific timing in terms of hours or days. It says, “in the most expedient time possible and without unreasonable delay.” So, we want to act on this quickly and in order to act on things quickly, we really need a process internally to do so.

Another notice requirement is really also focused on who externally do you have to notify. The SHIELD Act requires you to notify certain state agencies. It talks about if a data breach affected so many individuals, you have even additional notification issues or obligations. I'm recognizing that I'm coming up on my time, so I'm going to save some of this for when I speak to you in a little bit. But before I get there, I do want to talk about one of the reasons when you think about being in this room and listening to the SHIELD Act, why should you care? We should care about other people's personal information, but if that is not enough, there are civil penalties that apply if you don't follow these laws and procedures. And there's no private right of action under the SHIELD Act, but the New York Attorney General can take your company to court if you don't provide notice. There are different ways that you can be fined for failed notifications and there's specific civil penalties that you should be aware of. I'll pass it on to one of my co-presenters.

Ellen Samuel:

Thank you, Lori. I'm going to talk a little bit about attorney ethics. Like Lori was saying, we should care about people's private information, but as an attorney or a non-lawyer legal professional, there are other reasons you need to care, which are the ethical rules in your state. We're going to go a little bit over the rules that apply, from the ethical rules that apply to technology, data privacy, and security. These are the rules that really hit the most on technology so far. Now all of our practices are constantly being changed by technology, improved by technology, the challenges of technology. And every ethical rule probably is affected by technology in some way. But I really want to focus on these rules. Here I'm dealing with the ABA model rules, but most states have adopted those whole cloth or have made kind of small changes. Generally, you're going to find these same rules in most states, including New York.

The first rule that I want to talk about is 1.1 on Competence and it's a pretty short rule that just says that an attorney must provide competent representation to a client. What was added in 2012 was a comment number eight, which clarifies that the rule means that an attorney must stay technologically competent as well. The comment says, “to maintain the requisite knowledge and skill, a lawyer should keep abreast of the changes in the law and its practice.” What was added was “including the benefits

and risks associated with relevant technology." These are things that we have to keep up on in order to maintain our competence under this rule. Since 2012, when this was added, four of these states have adopted a duty of technological competence and some like New York have implemented a technology related CLE requirement, which I'll talk about in just a minute.

We're really seeing that it is important that attorneys not only maintain competence but also maintain education in this area. It changes rapidly and we need to make sure that we are all aware of the risks and benefits of any particular technology.

The next rule I want to focus on is Rule 1.4, which is communication. And generally this rule says that we have to keep our clients informed about decisions related to their case. I want to point you to ABA Formal Opinion 483, which says that under rule 1.4(a)3 and 1.4(b), an obligation exists for a lawyer to communicate with current clients about a data breach. So if you suffer from a breach, you need to make sure under this rule that you are communicating that to the client, which seems to broaden the plain language of the rule a bit, but it makes sense.

If a client is going to be affected by our technology or by a breach, we want to make sure we're going beyond the obligations of the SHIELD Act. For those of you who are not in New York, you need to make sure that they're aware of the situation and how it might affect them. [Lack of proper] communication is a huge area for bar complaints if we're not getting back to clients as quickly as maybe they'd like us to or we're not setting those expectations. That has changed a lot with technology since we seem to be available 24/7 with the internet, with email, with our smart devices. So, there are some challenges here and we really need to set those boundaries with the technology about when we are going to communicate with clients about their cases. We definitely do need to tell [clients] if there is a data breach.

The third rule I want to talk about is confidentiality. This is a huge issue when it comes to technology. How many of us have accidentally cc'd someone on an email who shouldn't have been on it or typed in the wrong name of a client and sent off potentially confidential information to someone who shouldn't have it? Very easy to do with technology and we need to be really aware of this issue and very careful about how we're communicating with our clients and how we're using our technology to protect our client's confidential information.

Again, in 2012, there was a big change regarding supervision of subordinates, non-lawyers, and third parties. These rules generally require employers to make sure those people are also following the rules. Now that doesn't mean if a lawyer in the firm or a junior lawyer does something completely unexpected that you don't know about, that doesn't necessarily mean you're going to get in trouble for violating the rules. But if you don't do due diligence, if you aren't taking reasonable steps to make sure that you are asking the right questions, that you are supervising people appropriately -- if you could have stepped in at some point and avoided a breach or done a better job at protecting the client's information, you might be on the hook under the ethical rules, under the supervision rule. W

What should you do about vendors? You need to make sure you read the contract, those huge, awful 50, 60-page, tiny type contracts. We have to read them and make sure that we understand what they're doing with our client's information. We need to ask them hard questions about where they're storing

their information. Are they storing our client's data outside of the United States? That's a concern, right? The laws outside of the United States don't necessarily protect private information the same way that the laws in the United States do. So you need to make sure you ask those questions. If you don't know what those questions are, luckily most bars and the ABA have ethical opinions that can guide you to ask those questions. I did want to point you to some ABA formal opinions. These are all in the CLE materials, which are on the website. I am going a bit over my time here, so I am not going to discuss those, but they are available there. Here are some New York ethics opinions as well that we would like to point you to. These are really necessary reading to make sure that you are following those rules, again, the CLE material requirement. I'm going to hand it over to Sandy to talk about tales from the field.

Sandy Coyne:

Thanks. I'm here to tell you a few things about LawNY and how we either improve the processes or learned something along the way to strengthen our security. Unfortunately, sometimes change comes from an incident. However, how you define that and recover from it defines your success. Here are some things that we have experienced. A phishing email came to finance and unfortunately, we trusted that email, changed a direct deposit. Our process change now is that finance now calls the employee directly or verifies that change is valid. We also require security awareness training for all our employees. In 2015, one of our offices was hit with crypto wall ransomware due to a staff member clicking on a phishing email. We did not pay the ransom, but we did in fact have to reinstall windows on all our computers and servers. And that effort did cost this organization time and money to correct the mistake.

What we've done - we've upgraded our firewalls, our antivirus programs, and all staff are engaged in annual security awareness training. We also use a phishing simulation tool that helps train our staff to spot potential threats. I think another important thing that we do, we work closely with our IT partner; we just talk to continue to build a robust security plan and keep up with the ever-changing security threats because we all know they just keep coming. So those are a few things that we've experienced here and a few things we put in place and I'll come back to talk to you later a little bit about our roadmap and how we are going to continue to strengthen our security here. And I'm going to pass it back to Lori.

Lori O'Brien:

All right, so let's talk a little bit about how are we going to pay for this? When you go through the SHIELD Act, right, whether you're doing this internally and reviewing the safeguards they've suggested or you're using an external partner, often there has to be an evaluation of what money do we have available, what resources do we have available in terms of implementing this? We have to bear in mind that this is the law, and we need to follow it and we need to make sure that we're really ensuring individuals' data protection. But with that said, there are opportunities to make sure that you have the dollars available to not only implement, but to constantly evaluate. As your organization changes, you may have to change. Some of those are dedicated grants like for Legal Services Corporation funded organizations, you have the TIG grants. Some of those may be building in your technology budget in better ways in the budgets of your various funders.

That's going to take planning. So it really is coming together, looking at what you're doing now, look at where you need to be. If you're starting at minimal compliance, look at where you need to be going forward and then start building in those budget items as you go along. Now this can be a really tricky

spot for folks and it can be hard for other expenses as well. And I kind of love this part of pre-planning for budgets, so I'm always happy to chat about this area in particular, but a lot of it is going to take pre-planning and budget planning.

Ellen Samuel:

Okay. Sandy, did you want to add anything on that one? Nope. Okay, great. Then we're going to move on to Lori to tell us a little bit more about what should we do now and how are we going to implement the SHIELD Act?

Lori O'Brien:

Well, that's the real question here. Where do we go after we leave this session? When we go back to our organizations or turn back to our days? The SHIELD Act does give a lot of guidance in terms of what are appropriate safeguards. It is a non-exhaustive list. So you go through those safeguards. There might be additional things you're going to do for your organization depending on the complexity of the data that you keep and how it moves. There are a few things before we get into the safeguards that are really important to remember. There are reduced obligations for small organizations or small businesses. You say a small business, you're talking about organizations with less than 50 employees, gross revenue of less than 3 million per year, less than 5 million in year-end total assets. You're still required to have a data security program and you have to evaluate what's appropriate for the size of your organization.

Part of that evaluation is the size and complexity of your organization, that nature and scope of your activities and the sensitivity of the information you share. I would argue that the information we're sharing in terms of our work is of the highest sensitivity. We want to make sure that the safeguards we put in place are appropriate. Then of course there is an exemption for compliant regulated agencies or organizations. So for example, if you're complying with HIPAA, you would have an exemption, but you're going to be following those other rules and regulations about data security. Let's talk about administrative safeguards - this is the most extensive section of the SHIELD Act, and we'll just talk about a few of them and what they mean and what we should be thinking about.

The SHIELD Act does talk about designating someone responsible for the program. It doesn't really tell you who that should be. So, when you think about who that person is, you know need to have someone with expertise in data security, you need to appropriately place them in your organizational structure. You want someone who can actually act. And so there's going to need to be some independence and folks that are reporting to the highest level of management. Some rules beyond the SHIELD Act specifically identify the name or the title of that employee, but the SHIELD Act doesn't do that. The other thing I think I would caution is, as you all know, many of our organizations, we end up wearing many hats and just make sure that this hat makes sense for that staff member. Again, it goes back to what is their expertise in security.

Let's talk about risk assessment. I think I said before, you've got to understand how data moves through your organization. The questions when you're evaluating this are going to be: What are your sources of information? Where are you pulling that information from? Where are you storing it? Who has access? What's your capability? Can you limit that access? And then if we're thinking about the fact that this came into play in 2020: Can you access it outside of the office? Our organizations are changing and growing and between remote work and hybrid schedules, that's important part of this. You're also going

to want to evaluate how good your safeguards are now. What do you have in place now? Some of that is policy creation. You need a data breach policy.

You need to know what to do when, right? It's not helpful if you have a breach and then you're pulling out the SHIELD Act and then you're trying to decide what you're supposed to do at this point. That is something that needs to happen now. Staff members need to be trained on it. Some of your vendors need to be trained on aspects of it, but that needs to happen preferably before a breach occurs. You're also going to want to think about things like your personnel policies. Whether intentional or acting carelessly, employees do not follow your policies. What is that system of warnings? What is going to be the repercussion for that?

You also want to see what kind of information you can collect about who accesses your information. That might be logs or records of system activities. When we think about our case management systems or data storage, do we know who downloaded what information, when, who accessed it? When I think about training, you also want to think about your vendors and service providers. You want to see who's coming in and out of your organization, who's also accessing that data and who's capable of maintaining those safeguards and then impose a contract in provisions of your contract that actually requires them to follow that.

And then we grow, we change, we keep moving. Every organization is like that. You got to think about: Has my staff grown? I need a bigger training program. Is the type of information I'm collecting changing? Maybe you need additional safeguards there, but you need a plan for constant evaluation so that you can adjust as your organization or as your business changes. Management, which sometimes when we're dealing with the day-to-day, it is really hard to take a step back and do.

Physical safeguards. So this is where you want to look at what is your storage, where are you storing information? Talking about LawNY, the office I'm in right now, we have information and physical files. We have a string of file cabinets; we have also information in our case management system. We have information in our email. Where are all those storage locations?

Because what you're going to want to do is once you figure out where that information is held, you really need to understand the potential risks of that storage, right? When you're assessing this, you want to make sure that you know what are the possibilities if there was unauthorized access, because that's also going to help you determine what's reasonable for your organization. That initial assessment is going to be really important. And so many organizations use different things. You might use public cloud service like Amazon or Google. You might have onsite data held, you might be hybrid, but you need to not only understand the nature and scope of that, but also what are the potential risks. The other thing is when you're thinking about actual physical information that you keep, you also want to think about your physical security, right? About someone coming into the building, someone coming up to the 10th floor where I'm on right now. How do they ask access those file cabinets? How do they access the front door? Those things are also important to understand.

And then I'll just mention disposal of information. You need to think about data retention policies. How long are you keeping information? What information are you keeping? Is it required for you to keep

that? But it also has to be part of your training, right? Your staff needs to know that too. Whether it's a file on my desk that has private information about a client or my files in Legal Server, I need to have instructions on how to dispose of information.

And then technical safeguards. The first thing I'm going to say about technical safeguards is you need someone on your staff that has expertise in these technical safeguards, right? I want to make sure that the organization is complying with the SHIELD Act and other related rules, and I want to make sure that we're doing the best we can for our clients and services, but I might not personally have all the expertise available to me to make decisions without information coming into me. I want to make sure I'm surrounded by people that have this experience and that could be someone internal to your organization, but that could also be an external partner or a vendor that is coming in and has that tech expertise and after of course, you've done your due diligence, you're relying on information provided by them. But when we think about technical safeguards, do you have centralized administrative control? LawNY is a very large organization, we have many different offices. That centralization is really important in terms of frankly, how do we support each other if there was a problem? How do we come in and make sure corrections are made?

You want to make sure you have appropriate firewalls and network security measures. You want to make sure your software is always up to date. And again, you want to make sure that you're assessing how you transmit personal and private information, not just internally, but to third parties, vendors, other service providers. Also here with technical safeguards, thinking about encryption. Encryption is incredibly important and can also be very difficult, especially when the entire world is not on the same page with implementing all of these safeguards at this point. I know I went over, I'm going to turn it over to one of my colleagues.

Sandy Coyne:

Okay, no problem. Lori, you just took some of my time. It's fine.

I'm going to talk quickly about the roadmap that we have on the docket here at LawNY for the rest of this year. We are looking into multifactor [authentication] across additional platforms that's going to give us more layers of security. It shares consumer identity with username and password. It meets regulatory compliance, easy implementation, complies with single sign-on and adds an extra layer of security. We're also looking into EDR antivirus, and this is a new standard in antivirus programs as it stops malware. I'm going to quickly go through some of these MDM platforms. We will build out our current mobile device management platform. I think that is probably one of the biggest things we need to do here. We think about all the data that's on our laptops and in our offices, but it's also on our phones. When your employee resigns or you let them go, how do you get that data back? Secure IT. VPN requirements. We have many staff members working remotely and we are requiring that they all log in through VPN to secure our data. And it hides your private information and prevents data throttling. So those are the four big things we have in the docket for the rest of the year. And like Lori said, yes, it's about budgets, but it's also about the plan. I feel like we have a really good plan here at LawNY to continue our growth with cybersecurity. And I'm going to hand it to Ellen.

Ellen Samuel:

Okay, thanks to you both. I would encourage people if you have questions, we will be leaving time at the end to answer your questions if we can. So please do start putting those into the chat. I wanted to talk about wrapping up here, the top 10 things that we think your organizations need to be doing now to start protecting yourselves under the ethical rules and then also under the SHIELD Act. Lori hit on some of these when she was discussing the technical and physical safeguards, but these are things that you can put in place right now. If you don't have IT staff or you're not as up to date on these things as needed for your firm, there are people who can help you. You're not out in the ocean by yourself. There's a lot of resources. LSC is creating new tech baselines for legal aid that will be out soon and there's a comment version up on their website right now that you can review that has some steps and things that we think that you need, steps that you need to be taking.

There's also consultants and lots of other people who can help really make sure that your systems are operating properly and that you are defensible in case of attack. You've probably heard now, it's not an issue of if you're going to be attacked, it is an issue of when. We are all targets and as legal professionals, we're particularly targets, even though our clients generally don't have a lot of the money that people might be targeting for bigger firms, they do have sensitive information and we are being attacked. There are legal aid firms that have had malware and ransomware attacks that have locked their systems up and that is costly for your business, that's costly for your clients, and you need to be prepared for that. So it's probably going to happen and you need to take some steps to protect yourselves as much as possible.

The first thing that we recommend is to identify all of your information systems. That means everything that you own and that your staff may be using to reach your network. We talked about MDM policies and bring your own device policies, knowing how people are connecting to your systems. Have an actual log of every system that you have, all your servers, all your computers, all your printers, everything that connects to your networks, your internet of things devices, make sure what you know where they are in case of an attack. I would also recommend that you actually physically print this out because if your system is locked up in a ransomware attack, you may not be able to actually get to all your plans. You have all these plans that you've laid. You have all the identifying your information systems. You may need to physically print it out and have it a copy at every office just in case you need that information.

You can't access your systems and they go down. Make sure you know, as Lori said, do you have protected or sensitive information? I bet you do. Where is it? Who has access to that information? What steps are you taking to protect that information? And then be aware of shadow IT or out of band communications. Are your staff using their Gmail on your devices or using browsers to store passwords that are not within your company's policies? Or maybe you don't have those policies, right? Or your firm policies - are [staff] saving information in places they shouldn't be saving it, which means they're not being backed up by your systems? You need to have policies about that. The second thing is to implement multifactor authentication and single sign-on. According to Google, MFA blocks a hundred percent of automated bot attacks, 99% of bulk phishing attacks and 76% of targeted attacks. I know your staff is going to put up a fight. They don't like it. They don't want to be using their cell phones or they don't want to be using a physical token. They need to do it. This is essentially important, minimum right now that you need to make sure that MFA is implemented everywhere that you can do it. And if your vendors aren't providing it, if LegalServer's not giving you that, or if your case management system, not to call out LegalServer, isn't providing that option for you, you need to demand that they do that so that

you can protect your clients' information. The third thing is to separate admin and user accounts. No admin should also be using their admin account as a user account at the same time, right? Because if the user account credentials are disclosed for some reason or are phished, then somebody's going to have access to all of your admin. Please make sure that you have separate admin and user accounts for those people who do have admin accounts.

Make sure that you're updating your infrastructure. Make sure that your operating systems are being patched, that you're updating your firmware. If you have that server that's running on like Windows 1998 or something like that, right? That's a problem. They're not updating those systems. We see that all the time and it is terrifying that people are not checking to make sure that all of their systems are up to date and have been patched, trying to keep those bad actors out by making sure those things are being done. Make sure that you are changing the default credentials. Please do that on your routers, on your cameras, on your internet of things devices, on your printers, your fancy all-in-one printers. In our tech assessments, sometimes we go in and try to get into those things using the default credentials that are available on the internet, and you would be astounded. Maybe you wouldn't be astounded. Those are vulnerable to attack. You need to make sure that you have changed those default credentials. You don't want someone hacking into your Ring doorbell to see all of your client's faces when they come in for their appointments. So change those things. Make sure that you are not making it just that much easier for people to hack into your systems.

Really quickly, I know I only have three minutes here. Make sure that you're using your firewall, you're using it proper properly. That you have it set for intrusion detection and prevention. I would really suggest using geo-blocking for both your inbound and your outbound traffic within the United States. That way your systems will block anybody trying to get in outside of the US. Now, perhaps you have someone who's going off to a lovely vacation in France, that's wonderful. They wanted to do some work. You can actually set the system so that just that person can get in for a limited amount of time from outside of the United States. But otherwise, why would anybody else be trying to get in? You want to make sure that you lock that down. Make sure that people are not trying to get in from outside. Harden those systems as best you can. Encrypt everything where you have that option. Make sure things are encrypted both at rest and in transit. So your emails where possible. All of your devices need to be encrypted. If people are using their cell phones to access your case management system or your email, you need to require that they have those encrypted and also that they can be wiped remotely if they lose that device or if somebody steals it.

Make sure that you're disposing properly of your end-of-life hardware and that it is being shredded or wiped properly before you're recycling that. Then make sure you're re-imaging your computers between users and make sure that those are being completely cleared before you're setting them up. Completely off-board your users. You want to make sure that they are wiped from every system. Do they have court logins? Do they have access to other systems that maybe you don't know of? Do they have access to your password manager? Make sure you have a list of things that you are doing to make sure you completely off-board your users.

Training your users, so important, making sure that they're aware of the threats. That we are the weakest link. When somebody's getting in, it's us users. We're the ones who are getting phished. And the people at the top are absolutely no exception.

They are the ones who are being targeted and the hackers are very tricky. They're using social engineering. We need to make sure we're being trained regularly so that we're following these policies.

And then finally, disaster recovery and business continuity plans. Essentially important. Make sure you have one printed out. Yeah, that's all. Sorry, I had to go through that really quickly. We wanted to leave five minutes at the end to make sure that we have questions. So Amber, any questions in the chat?

Amber Wilder:

We do. Just in case anybody else may not have seen it, there was a question about access to slides. Those are located on the agenda for the session on New York Tech Conference website. I did put a link in there, so just hop on in. There's slides and other CLE material. There's also a question of "does it make sense not to collect sensitive information if you don't really need it, such as the Social Security number."

Ellen Samuel:

I can start and then if Lori or Sandy want to hop in. Absolutely. We do case management reviews as part of our tech assessments, and I don't want to call anybody out, but we have seen firms that use the entire Social Security number in their case management system. And when I said maybe that's not the best idea. For conflict checking purposes, I understand why you might need some of that information, but I got pushback that we need all this information to make sure that we're properly checking for conflicts. I would push back that it's really not safe to have that information, especially even open to your whole firm. But if you get hacked, all of that information out there is a problem. If you need to do conflict checks, you get your first name, last name, middle initial date of birth, and gender, maybe the last four of the Social Security number. And for 99.9% of cases, that's going to be enough, right? If you are collecting that sensitive information… perhaps you have medical records. For disability cases, for Social Security disability cases, or for other types of cases that you're doing, those need to be locked down very, very carefully. That's really important information, high value to hackers. You want to make sure that that is being protected. And as Lori said, you must have a data destruction policy and you must follow it. If you don't follow it, that leaves you open to litigation in the future. If you're not destroying your information as you set out in your own policies, then that is a problem. Make sure you check with your malpractice insurance to see how long you have to keep that information. But it is a huge danger to keep it beyond when it's reasonably necessary. Lori or Sandy, do you have anything to add there?

Lori O'Brien:

No, I'll probably preface my comment. Oh, I'm sorry, Sandy, go ahead.

Sandy Coyne:

I was just going to say from an employee standpoint for HR, we do practice that, right? But Social Security [numbers, we] can't get around. You need that to on-board. But if you're using the right HR platform and you're making sure the access is locked down internally, I do feel like that's the best case scenario, right? But that's just one population of people that you absolutely can't shorten, right? The Social Security number. But I agree with the client comments. Go ahead, Lori.

Lori O'Brien:

Oh, I was going to agree as well in saying that coming from an organization where I think we collect right now more data than we need to, so I'll preface it with that. But one of the things that happens is maybe I had a grant that required me to collect certain data, and then suddenly that becomes part of your intake and it never leaves, right? So again, it's like part of this is starting with an evaluation of why did we collect that originally? And sometimes people don't remember, and you have to face that. But to have a regular review of what data you're collecting, why you're collecting it, and is it reasonable right now?

Ellen Samuel:

You're very welcome.

Amber Wilder:

I have a few more questions if we have time.

Ellen Samuel:

Yeah, we have one minute. One minute. Yeah. Say it.

Amber Wilder:

What is the standard for professional conduct for lawyers in New York State for client document destruction?

Ellen Samuel:

Oh, that's a good question. I don't know the answer to that. I'm in Illinois. Lori, do you know the answer to that?

Lori O'Brien:

So that's a big question because it also depends on what type of information you're collecting. So I'm happy to have a conversation if folks want to reach out, and I'm happy to put my email in the chat, but it is going to depend on when we are thinking about those file destruction policies. You've got to think about what type of case file you have, what information you have, and some of that is practice area dependent too, and what type of document that is.

Ellen Samuel:

Thank you. That works. Thank you all. As you can tell, we could talk about this for hours and we would love to, really a passion of ours. Our contact information is available on the screen. We thank you so much for participating today and being here with us. We hope you enjoy the rest of the conference. I think Amber's going to put the link to the next sessions in the chat if she didn't already. Thank you all and enjoy the rest of the conference. We appreciate your attention. Our contact information again is there on the screen. So thanks everybody. Have a wonderful day.