Project Completed by:

EDUCAUSE
Webinar: Data Sharing During a Pandemic: Protecting Privacy While Promoting Safety
Thursday, November 12, 2020
1:00PM – 2:00PM Eastern
Hello everyone. We will be getting started in just about a minute. Write in the chat where you are calling in from and what the weather is like there. For those who are filtering in and joining in go ahead and say hello in the chat. Tell us where you are calling in from and what the weather is like. We will be starting in just about a minute.

This meeting is being recorded.

Welcome to today's EDUCAUSE Webinar: "Data Sharing During a Pandemic: Protecting Privacy While Promoting Safety." This is Sean Burns, Corporate Researcher at EDUCAUSE, and I'll be your moderator for today's event. EDUCAUSE is pleased to welcome today's speakers: Merritt Neale, Gregory Whitten, Svetla Sytch, and Kent Wada. We will introduce them in just a moment, but first let me give a brief orientation on our session's learning environment. To open the chat, click on the chat icon at the bottom of the presentation window. You can use the chat to make comments, share resources, or to pose questions to our presenters. Be sure to select “Panelists and Attendees” from the drop down menu in order to engage with everyone. We will try to answer your questions as we go through the presentation; so we encourage you to type your questions into the chat throughout the webinar. If you have any technical issues, please direct a private message by selecting “Panelists” in the chat dropdown. The session recording and slides will be archived later today on the EDUCAUSE website. And now, let's turn to today's presentation. With the election in the rearview mirror and the extended winter break just ahead, higher education leaders have a valuable window of time to examine their approach for returning to campus. The complexity of the situation now includes vaccination policies along with ongoing tracking protocols while keeping data privacy top of mind. At the onset of the pandemic, contact tracing sparked safety and ethics discussions, requiring leaders to focus on reducing privacy risk and building greater trust with students and staff.

Good afternoon. Good morning to all of you out in the west coast. It is a pleasure to be presenting today with this group of professionals. Today's discussions working in remote learning are important topics on the top of mind. My name is Merritt Neale. I'm focused in the higher education practice. I support our academic center plans. I have overall 28 years of experience with significant experience helping clients to identify and resituate risk compliancy and compliance. Kent Wada, would you introduce yourself?
Good morning, everyone. Thank you for having me. I'm looking at my head shot. The one you have there is a little dated. The hair shows it all. I'm director of policy and governance at UCLA. I have the pleasure of being the Co chair of the EDUCAUSE higher education constituent group. And also participant of EDUCAUSE policy advisory committee.

My name is Svetla Sytch. I've been in this role for about a year now. I was responsible for implementation of large university programs. I'm looking forward to sharing with you the privacy perspective today.

And Gregory.

Hello, everyone. My name is Gregory Whitten. I'm a senior director with Huron consulting. I've been with Huron for a year and a half. Previous to that I served in the Obama Administration. I run RT3 COVID at Huron and I have a background in pandemic policy vaccines and bio-surveillance. I look forward to your questions and speaking about privacy around the pandemic.

Great. Thank you. Glad to have each of you here as a panelist. My apologies with the PowerPoint challenge. Trying to get this back here. I wanted to set the stage in terms what we are trying to establish today. We are here to discuss the data privately landscape. We have identified what those key areas of discussion are. We also want to wrap up with our next steps and resources. So our objective today is to cover each of these areas and add questions into the chat box and please let us know any questions you may have. We will try to address them as we go through this session or at the end. I wanted to start at the high level covering some aspects. As you can imagine that as we go out and engage with different clients we are starting to see a picture of what the privacy landscape looks like. We are trying to understand what that is appropriate balance of privacy and safety. For really every institution that is facing it and those challenges that are part of this global pandemic. Starting with something as something as student awareness. Even before the pandemic many institutions struggled to raise the level of awareness. Even before the pandemic many institutions struggled to raise the level of awareness. Raising that level of awareness around data privacy rights. Trying to articulate standards across the organization that will impact stakeholder groups or many organizations have set that aside for another day. I think we saw the pandemic, the COVID experience that we are going through now that is another day. We do see a lot of organizations trying to educate students on the high degree of privacy rights that they have. Students have become accustomed to provide personal information. We can clearly see that through social media use. We can certainly imagine that click through generation where they review and accept privacy terms and conditions within less than two seconds. We know that varying degrees from students. Items such as video have become more ubiquitous in terms how we are engaging with that. Privacy professionals insist educating and proliferating the message is top of mind. Insuring the privacy information collection is first and foremost. For students it does appear to be much further down their priority
list. When we look at the role of the chief privacy officer we see that the CPO is not a new title but it is one that has gain significant traction over the last couple of years. The roles have evolved over times the different reasons at different points in time. We see early adopters focus heavily on the ethical concerns of data use. It seems to be asking more of the question, should we use this data? Versus how do we use this data? More of that traditional view driven by the academic side of the institution. We have seen information systems analytics capabilities the value of that dataset has grown with it. The student and other institutional datasets have grown exponentially. Organizations are starting to realize that. We do a lot of work with chef information security offers. It is a common model for those roles to be a high degree between the role of a chief information security offer and the roles of privacy officer. There are obvious areas where these come together specifically around items Sun's as incident response, policy development and some of the more mundane items. We are going to discover some of those areas today. One of the other areas, I think we noticed during our discussions is that the privacy maturity is the topic that we have found with both decaded chief privacy officers. They have indicated a mixed reaction. We have had this discussion several times. It is really often attributed to their dual responsibilities and the challenge that they have balancing that out across the sets of roles and responsibilities. Move into our first polling question. The question is I'd like everybody to participate. Has your institution address privacy effectively as the pandemic has progressed? If everybody can take a quick minute to fill that out. I know some of the challenges that we've seen in terms of effectively addressing the pandemic has been not having dedicated resources for addressing all things privacy within the organization. As I mentioned earlier that cleared lineation of roles and responsibilities. Not just the chief privacy officer but other roles such as your general counsel and other senior leadership. Another area that we have seen an effective method of communicating privacy needs. Here we do have the results of our poll. We have 32% feel they have addressed privacy effectively. 61% believe that they have somewhat effectively managed it. And 7% no. I think that is what we have heard in our discussions with our clients and privacy officers. Is that there are degrees of maturity across the areas of the program. Trying to be responsive to stakeholder needs. Those different protocols and policies that have been put in place there have been mixed results. I would like to transition on to our panel discussion. I'd like to ask you how is your institution used symptom tracking throughout the COVID 19 pandemic?

>> At the University of Michigan we invested time and effort into developing processes as well as solutions. Obviously one of them is the symptom tracking tool. Back in May we deployed an in house application. That was geared toward researchers. It would turn to their lab following the governor's order. The operation has evolved. It is called responsible. He has a sign in version for faculty, students as well as guests. We use it to monitor some early signs on campus. I'd like to talk a little bit about some of the privacy principles that we try to follow. I wanted to make sure
we address transparency, minimization of data collection as well as data governance tools. The retention period is driven by state of Michigan health requirements. It is going to be set for one year. Access to the data is very restricted. The data can only be used for public health related purposes. We also have an existing governance framework that already supports strict measures for handling personal information. We have taken advantage of that as well. Fast forward to late August and beginning of the fall semester. We made the use of responsible application required for everyone that is in on person and on campus. And, of course, this drew a lot of attention from the University of Michigan community. What allowed us to answer questions and address privacy concerns was being very transparent and very consistent with our data processes. That has been our experience at the University of Michigan.

>> Kent I wanted to ask you a question what policies have you established that relate to health and safety during the pandemic at UCLA.

>> Thanks, Merritt. UCLA has done a lot of similar work. We are taking advantage of some of being in the eye of the storm, if you will for a moment to take relook at what we have done. If you don't mind Merritt, item going to share my screen for a moment. And let's see. Hopefully I'll get this one right. I have to caution is really a draft. I'm little nervous showing this because it is being recorded. I thought it would help to be concrete about how we are being trying to be transparent about things. Going through this document really quickly. You can see there are four sort of general reasons we are collecting data. The links that are there are in the resources for this presentation so you can follow them yourself and see pretty extensive descriptions of the protocols that we follow. If each of these categories we are showing what kind of data we are collecting. It is pretty amount of staggering data that we are collecting outside of the normal health care context. A lot of this would normally fall, you would think of it as being health data. Continuing on just briefly then trying to identify for each use case of why we use that data is identifying who needs it? For what purpose? What exactly is what they are going to get? Just showing what we need all this data. How is it being used and how it is being retained? How long information is kept currently is blank. We are still working through that. Our analysis for data retention is more complicated than Svetla has talked about. Unfortunately, for us going through the retention for the University of California. We feel will be kept for a minimum of 30 years hp hopefully a maximum of 30 years. There are some context where our retention schedule we need to keep data for 50 years. So there are a whole bunch of cases going back to this list of data. Each one is being analyzed under the obligations that we have. Our records retention schedule. A whole set of data that we don't have entries for in our retention schedule. We are working through those right now to update the system retention schedule. So thanks, Merritt. I can let you grab the screen back.

>> Sean, I was wondering if you can weigh in to HIPAA and what you have seen.

>> Sure. Yeah. There are a lot of institutions that have a medical center on campus. And usually they already have a privacy officer dedicated to HIPAA to address those concerns. A lot more
institutions don't have HIPAA specific person in a medical center. They have been struggling more deciding how to manage COVID data and navigate the right data collection, storage, and use of that. Another big problem that has been coming up a lot of researchers are interested to try and help improve our understanding of the virus. It is also really important to bring privacy into that discussion as early as you can. Maybe most importantly being transparent how you plan to use and collect and store this data has they have been sharing and discussing their plans at UCLA and Michigan.

>> Thank you, Sean. I think that is something we are seeing out in engagements as well. I've been in numerous calls over the several weeks where this data is quickly becoming a hot commodity as you can imagine. We have a number of organizes that fall under that profile that have research capability. What we are starting to see there are a top of organizations that are evolving from that. Those that have a clearly define position and disposition going into collection and dissemination and analysis. We have organizations that really don't have a plan but they are cognizant for the need of that plan. This is definitely become most evidence in the AMCs where the university and health system are capturing these data sets and see the value and combining them for rich set of data for research purposes. I'd say in most cases these conversations are just starting. We are playing a role conversation between the university and trying to rationalize what are the best steps ensuring those discussions are part of governance. Someone mentioned about leadership wanting to have access to this information. So balancing out those considerations around privacy and the value of the data are absolutely critical. I'd like to move on to the next section which is around the vaccine planning. I think that has clearly been front and center in terms of a focus of attention over the last several months. Even the last ten days. The U.S. had 1 million people test positive of Corona Virus. That represents one tenth. This is the first ten days of this month. With this increase in testing and positive rates the recent announcement that a vaccine with success rate of 90% will hit the market soon. As a result there will be implications of that as well. What I would like to do is pose the next question to Greg. Could you speak to the next chapter and how is privacy integrated in the planning process?

>> Thank you so much, Merritt. Currently right now with operation warp speed which is currently President Trump's ability to get the vaccine to market, they have currently awarded a few contracts at this point. Will be the distribution the vaccine distribution. That will be the supply chain side of it. They have said there will be an I.T. tool at this time not actually awarded that will track the vaccine. The problem that you will run into with privacy around the vaccine. Unlike measles, mumps where you go to the primary care. This will be a mass vaccination we haven't seen in the United States. A lot of big box stories such as Wal-Mart, Walgreens are going to be a part of this. When you go into one of these stores they don't track it in the same manner if you were to get vaccinated like I think at this point concerning privacy I think Universities have to think individually how they will track that. They will need to look at the state they are currently residing in. Currently right now, operation warp speed is depending on the 64 districts plus large cities to come up with a plan how they will track that vaccination. What I will say to universities in those states look what the state is doing and follow their lead and look at how you
can track their students if they have been vaccinated or haven't vaccinated. I think private will be a huge concern around the vaccination itself.

>> How do you see vaccine requirements playing into the 2021 spring semester?

>> I think this is a tricky question. By any means if you, obviously, President elect Biden struggles with this question. To mandate a vaccine is very hard. Currently right now if you look at state legislatures they have some required vaccinations. Out of those 50 states, 45 allow them exceptions. Due to religious concerns. You can provide paper work around those things. When you think about that you will see that the exception is very hard. Will schools be liable if they mandate a vaccine? If someone dies? If there is adverse effects. It is hard for schools to say if you want to return to campus you need to be vaccinated. We have never seen a pandemic of this size since 1918. I think schools will have to struggle on an individual basis. State universities will have an easier time because they can follow state regulations. If you are a private university that is a tricky question. In my own opinion, I do not see a national mandate for the vaccine just because since the 1980s it has left up to the states to make those decisions and the executive power of the President and congress can't mandate vaccines at that level.

>> On that note the efficacy of the COVID 19 vaccine do you think that will pose an issue for universities?

>> Yeah, so if you look at the Pfizer vaccine, I caution people, right. Because at this point Pfizer has released a press release. That is it. They have not provided that much data around this. One thing I want to stress is that the vaccine is not a silver bullet. This is not like an MMR. You get it once and you are done. This is a virus. The efficacy will come into play as a huge thing. If you look at the Pfizer vaccine how long will you have antibodies? It will be a repetitive thing you will have to keep getting boosters. I would say yes, this is good news. There is a lot to go from this. We are long way away of knowing a vaccine is going to be 90% efficacy for how long? I think what universities have to think about. So if you want to return to campus you want to get your student population vaccinated. How do you track that? How do you keep it private? It is 90% two weeks after you received your second shot. How long is that going to last? So I think there is a lot of things you have to think about. You have to think around the vaccine. Everybody in America were jumping up for joy we have a vaccine available, right. Currently there are 50 million doses of the Pfizer vaccine. 25 will go to the U.S., 25 million will go to the rest of the globe. You will not see the availability of a vaccine until probably late summer of next year maybe spring. There has not been modernization in scaling vaccine production. It takes a very long time. To scale a vaccine it will not be widely available. I'm very happy that the vaccine is available. I'm happy we have this progress. We have never seen anything in the world where we have been able to develop something like this. It is not a silver bullet but it will help return universities to a new normal, I would say in the next few years.

>> Thank you. I'd like to get your opinion on how universities are going to prepare and set up for
student privacy with the assumption that a vaccine is forthcoming?

>> You know it is difficult to address. We are probably going to see a similar approach which is understand exactly where the university as an institution from a leadership perspective wants to go. Consider what that means personal information perspective, public health perspective and all these aspects need to be weighed in when these decisions are made. So it is definitely a back and forth analysis. It needs to happen as we just pointed out. A lot of this is unknown at this point. I think we have a lot of work ahead of us in the coming months or two to figure this out.

>> Excellent. Thank you. I would like to move on to our next topic. Working and learning remotely. I think when we all know when COVID struck, one of my observations our clients I.T. were turn on a dime. They were able to respond quickly to the needs to the virtual explosion of remote learning and remote work. We saw clients repurposing existing hardware, increased licensing all this in an effort to operate this new model that no one had seen before within a technology era. No one was prepared for this transition but they were able to respond. The privacy implications that follow these expanded uses of technology, in some cases we say follow the data where is that taking us? What systems? What processes are being impacted? No one was prepared for this, this transition, the implications. Sean I would like to ask you what the key takeaways were from your research? What was apparent from your privacy research specifically pertaining to working and learning remotely?

>> The first big hurdle was the Zoom bombing. People popping into rooms. Solutions came quickly. That was an easily handled issue. One of the bigger issues that come up is proxy exams. Requiring students to be watched or recorded poses some privacy concerns. But institutions need to conduct exams. A know a lot of institutions faculty don't undertake proxy exams lightly. You know, if there are other solutions available, that's a good I would recommend going for another option if you don't have to do proxy exams right now. For workers and students at home, if you are being recorded in a classroom or in a meeting, you know, not everyone wants to share their room with people. Virtual backgrounds have helped a lot with that. But there are still issues within the home and especially in smaller spaces. You know not everyone has an entire soundproof room they can host meetings in or anything like that. That's a difficulty that people have to deal with. And, of course, there is listening devices in a lot of homes. Those can cause some privacy concerns as well. A lot of institutions have put together some great resources to for instructors, for faculty, for staff and students just to help them navigate a lot more of these privacy concerns and help take some of that power over their own privacy into their own hands.

>> Excellent. I'd like to kind of readdress that question to you in terms of the shift of remote services. Organizations are taking on a lot more digitation projects. How has your privacy organization been involved in those consideration planning deployment?

>> Sure. The shifted most services dramatic was not a new thing for the University of Michigan. We already had some level of remote teaching, research, and business operations. A number of
the technologies and the solutions that we are dependent today we had in place. We have Google, Canvas, VPN, cybersecurity tools and practices. So with that said, to Sean's point we did see a greater need for solutions for online collaboration. We went remote over a course of four days in the spring and two of those days were a weekend. During that time we added Zoom to our applications. Prior to that we did not have a contract with zoom. We released a HIPAA one of the things that allowed us to be so nimble having established processes. Not just for making sure they provide high quality service but also they have adequate data protection measures in place. We developed a number of online resources for our faculty staff and students for protecting privacy. We will be sharing a number of these links. So I encourage everyone to check them out. The other point, in addition to just tools and technology that our essential I.T. organization provided to campus. We saw a lot more demands to interpret privacy laws and regulation in increase online presence. I saw in the chat a couple of comments along these lines. We developed and published guidance on handling recording. There are a lot of questions about that. Who can I share it with? And under what circumstances? That was a separate effort where we helped transition youth camps and summer programs to online. That normally happens in person on our campus. Quite a bit of work around that. HIPAA there was another comment in the chat. Our administration needed guidance when health information is protected under HIPAA. We supported increased collaboration with institutions, a number of those studies were COVID related. We kept busy over the spring and summertime.

>> Thank you Svetla. I appreciate that insight. Hopefully folks are getting good takeaways from this. I wanted to move on to our second polling question. And this question is what are your biggest data privacy concerns for the spring of 2021? We have seen a mix of strategies of students return to campus. Dealing with physical separation. Limited use of facilities. Clamp down on larger gatherings. Lots of concerns for students, faculty, and staff. The risks continue to grow exponentially. This is interesting. Our number one finding at 50% is health and safety. That's an interesting finding. Vaccine planning. That is coming low 13%. This reflects a lot of organizations trying to take one step at a time. And the working and learning remotely. We heard that is going to be continuing challenge as we continue to balance on campus and off campus activities and start to deal with other groups such as international students. If we could we move on to our last section which is around the future of privacy. And with this obviously global event, major privacy implications. Where does that take us tomorrow? Where does that take us in the spring of 2021 and beyond? Our discussions with clients indicate a high degree of momentum has grown within institutions as it relates to privacy and privacy initiatives. How do we continue to leverage that memorandum and keep privacy long term? Specifically in terms where you need to take this in the future and where you think our organizations need to focus? Privacy into the process of data management into the decision support systems that are fed those data that may be of private nature. Be responsible for a data use request. Student success analytics or capturing managing EPHI. These are things we need to see they are part of future processes. We need to adopt strategies that adopt privacy planning. Security and privacy and other areas are an afterthought. This has to be on top first and foremost as part of our process. As we implement contract tracing and other systems this is going to be required more and more. Data governance, I
don't know we can say enough about that. This is a key area where a lot of groups struggle. The use of these datasets should be defined. There should be ownership and rules. They should provide safeguards and follow critical areas of compliance. Another key area is institutions really need to invest more in privacy resources. We see these chief privacy officers, we like to see starting to put more of an effort and investment into privacy personal. Trying to raise the bar in terms how we manage and communicate privacy management. That does require dedicated efforts to a high degree. I think as pointed out by one of our folks in the chat box we must insure our stakeholders their privacy rights and responsibilities. This is something we cannot emphasize enough. This is larger, privacy awareness to raise that level of understanding. We have clients' privacy and security training as part of their curriculum for on boarding students as part of these new semester start ups. So it has been interesting to have training required for students that are not in remote learning model. Sean, I'd like to ask you in terms of some of the research findings around the future of privacy and higher education. What are some of the areas you can share with us?

>> Yeah, so just thinking about privacy moving forward and how to improve it at your institution, well one of the issues that was regularly reported in my research in the last six months privacy professionals being included in conversations but slowly or later in the process than ideally. And a lot of times people reported that this it was become they saw them as a blocker or a no person or someone who would slow down these important processes that needed to have decisions made quickly and get things done. And that's you know, it is important to focus conversations with administrators on how you are an enabler and trying to help people reach their goals properly and with respect to privacy. That can help increase views on privacy across the institution and get you involved earlier and processes hopefully. Another thing I wanted to height is, you know creation of a data privacy governance board. With faculty, with students, with I.T. staff and administrators being involved. That can answer and address needs and concerns from all of those different groups across campus. It helps with transparency as well. And then another thing I wanted to mention was standardized risk assessment helps everyone. It quickens the process and privacy offices in higher education are going to continue to need conduct privacy and security risk assessments. Both within the institution when people in offices are working with PII and without outside vendors as well in third party solution providers that also require data access to fulfill their services. So I wanted to plug real quickly EDUCAUSE has worked with numerous institutional members and privacy leaders to create the higher else community assessment tool kit. We will provide a link to that. That tool kick provides a questionnaire to insure that solution providers have the proper policies in place to protect PII. And if a vendor has filled it out then they can they fill it out for one other institution. If it is standardized across multiple institutions they can pass those answers on without having to redo the same thing time and again.

>> I'd like to can you the same question. How has COVID changed your view of managing privacy going forward? You have a long career working in higher education with privacy. I'd love to get your perspective and your view on managing forward.
One is COVID time is probably an order of magnitude than Internet time. I sometimes wonder how well we were coping with Internet time to begin with. We have pivoted on a dime. We have all done that pretty well. So the first thought comes that comes to mind when everything is an emergency nothing is. I think we need a new scale, really to measure urgency where emergency is the zero baseline now. And of course, when there is an emergency we have to move forward because there is no choice. That doesn't always last. There is a storm and as I talked on the eye of the storm when we hit one of those, I think we really need to take a step back and just take a deep breath so we have time and space to think about what we are doing rather than just forever being in this mad dash to get things done and to avoid drowning. I think the other reason that we want to take that step back and take a deep breath occasionally is to be kind to ourselves. We are all trying to do the best that we can to make things better under the really difficult circumstances. I can't tell you how often in conversation that keeps coming up people are burning out. And you know, this pace is simply not sustainable for us. It just isn't. We need to think about that. The second thing, is something that Svetla has talked about, trust. So has Sean. It is a make or break pop proposition. And I think people are right to be concerned about the implications. If they can't trust we are going to do the right thing they may choose not to participate. Just at a time when so much of our Pam related activity depends on people being honest and participating on symptom monitoring and tracking. I don't think you need to be a student to have concerns everyone you associate with purposes of contract tracing. There is a really important health imperative that says that will be useful. Sort of emphasizes again. Talking about building trust through transparency. Privacy has done that. We will continue to play, a major role in that. I think we need to think about the flip side of this. Socializing what we are doing in terms of data collection as the norm is what we need to do for this pandemic and yet we don't want it to go so far that post pandemic we just fall easily into this surveillance mindset for other purposes.

On that note. I think we recognize there is a heighten level of awareness as we move to the new norm. How do we maintain that heighten of awareness.

The no more breaches part of things. We have the same difficulties that are information security colleagues have seen as inconvenient and costly and slows things down and gets in the way of things. That will continue to be true. That will be maybe have our colleagues take the lead on that. On the other side of things, there are concerns about surveillance, about machine learning AI in so many ways that biometric medications. The facial recognition. It is interesting to me with the blink of the eye the release of the iPhone X started facial recognition. It became normal to use your face to identify yourself. There are so many concerns. People have those concerns. I think the right brain hasn't met the right brain and agreed on a position on that.

I'd like to ask the same question to Svetla. How do we maintain this heighten level of awareness.
I'll keep this short. I know it is Q&A time here. I want to make a brief point. I completely agree with what Kent said. Kind in the long term vision, I'd like to just remind the notion that privacy like freedom of speech should be part of our higher ed community. It should be something that is there, understood, and accepted. The pandemic as traumatic and dramatic it has been. It has been an effective catalyst to establishing some good privacy practices. I think many of them are here to stay. I have seen glimpses of the new normal. We ask just because we can, should we? Would you think now because we have to because they are the right thing to do which was Sean was mentioning. We can maintain that level of interest and care about privacy.

Thank you Svetla. I appreciate that. We do have some time limitations here. Please add your questions in the chat. I'd like to move on to our next steps and resources in terms of just the discussion. From the next steps perspective I encourage everybody to go out and read some of the thought leadership that we pulled together and published over the last course of a year. Heavily inspired by our security professionals that we are working with at client sites. We are three publications. These are joint ventures by EDUCAUSE and Huron. We encourage you. They are great resources. We have those materials available to you. Coming soon, EDUCAUSE and Huron privacy report, the evolving landscape of higher education. This publication will be out soon enough. We look forward to continuing engagement with this great community of professionals. Definitely looking to continue to conversation. In terms of other resources we pulled a list including the University of Michigan. Kent at UCLA. Huron provided resources for all of our clients within EDUCAUSE. Within our market and obviously EDUCAUSE has the COVID 19 resource hub. I'd like to pass it over to Sean for some closing comments and thoughts.

It didn't look like we had too many Q&A any actual Qs. I wanted to go back. A lot of campuses don't have HIPAA concerns. And that is true. I don't mean to press the HIPAA alarm in this webinar. It is good to make sure that people are being transparent about what data they are collecting, why and how it is going to be stored and used. Other than that we got all of our links being posted in. So I guess I can close this off here.

On behalf of EDUCAUSE and our speakers, this is Sean Burns, and I thank all of you for joining us today for an engaging session and conversation. Before you sign off today, please click on the session evaluation link which you will find in the chat window. Your comments are very important to us. The session's recording and presentation slides will be posted to the event site. Please feel free to share these resources with your colleagues. And finally, please join us for the next EDUCAUSE webinar on December 1st to hear about “Teaching, Learning, and Student Success: 2020 in Retrospect and 2021 in Prospect”. On behalf of EDUCAUSE, this is Sean Burns, thanks for joining us for today's EDUCAUSE webinar.

Thank you.

Thank you.