FHS Data Breach Webinar 2-4-75 Transcript

Recording in progress.

Good evening, everyone. I am Maureen Valentino. Many of you know me as the participant coordinator here at the Framingham Heart study. We sincerely appreciate your taking the time to join our webinar this evening, and we hope that you will find it helpful

Before we begin, for those of you who may need closed captioning unless captions are already appearing. Please click show captions which is located at the bottom of your screen.

We have received questions from many of you, and we will do our best to respond to them in addition, should you have questions at any time during this event, please use the Q&A feature located at the bottom center of your screen to type your questions and then hit. Send to submit.

These questions will be only visible to our panelists, and you will have the option of submitting them anonymously.

If, after participating in this webinar, if you have additional questions, or you do not feel that you've got a specific question answered to your satisfaction. Please reach out to me at the Framingham Heart Study at 508-935-3417, or by email at fhs@bu.edu. And now, without further ado, your panelists, Dr. Don Lloyd Jones, Dr. Joanne Murabito, and Mr. Chris Sedore.

Good evening.

I'm Dr. Joanne Murabito, and I've been the Research Center director for many of the exams for all cohorts, providing me with the remarkable opportunity to meet many of you and personally hear your stories.

We're coming to you live from the Framingham Heart Study in the Perini Building in Framingham. This is the same place where you and your families have come for your exams since 2002.

Good evening. I'm Chris Sedore, and I'm Boston University's Vice President for information technology and Chief information officer.

Hello, my name is Dr. Donald Lloyd-Jones.

I may be a new face to many of you in the Framingham Heart Study, because I just started January 1st as the new principal investigator for the study.

That means I now have overall responsibility for study, conduct and oversight.

As a bit of background. I'm a cardiologist and an epidemiologist, and I did all of my training right here in Boston.

And I'm actually not new to the Framingham study. I trained here and began my research career in the late 1990s and the 2000s.

and I likely did examinations with many of you or your parents. During those 7 years

Framingham helped me launch my research career, and it's a huge honor to return now, in this phase of my career to assume its leadership.

I want to emphasize that while I'm just returning to FHS. Now, I have a deep appreciation for the legacy of Framingham.

What you all and your families have done to help us understand the life course of health and disease is nothing short of remarkable, and it's been transformative. You have saved literally millions of lives here and across the globe over generations.

I take that legacy very, very seriously, and I want to assure you that once I arrived a month ago, my number one priority is, and going forward, it will remain the security of your personal information.

We're working tirelessly to upgrade our systems, change the way we handle data, and ensure up to date training for all of our staff to ensure maximal data security.

These things were already happening. But we're now redoubling and tripling our efforts.

So now let's get to the purpose of tonight.

We're going to answer many of the questions that you all submitted.

and some of those answers are a little bit technical, since we're talking about cyber security, but we'll do our best to make things as clear as possible.

I'll start with a brief recounting of our current understanding of what happened with this data breach.

So, I'm sure many of you are just wondering how exactly this could have happened.

On the evening of Sunday, September 8th our systems and data steward detected unauthorized activity on one of our servers.

They worked very quickly to shut down all access and to limit the breach.

Nonetheless, it was clear that some data had been copied and transferred out of our system.

No data were lost to us, and there's been no demand for ransom.

Boston University Information security specialists quickly moved to understand the extent of the breach

as part of that investigation a cybersecurity forensics firm was engaged to help us understand which data had been copied, and where the attack came from.

We now have a good understanding of which data were affected.

First, most of participants, research data was accessed.

These are the things that we measure during your routine visits like your blood pressure and your cholesterol.

Those data are linked to your Framingham research idea

from separate files. The attackers may have accessed some of your personal information, including your name, address, date of birth, telephone number, email, address, sex, race ethnicity, self-reported income category and your occupational category and signature.

Importantly, no genetic data were accessed or compromised in this attack.

Now, during the investigation, we discovered that the social security numbers of 106 or less than 2% of our current participants were potentially compromised.

It turned out that those social security numbers were buried in health records we received from outside hospitals and health systems that sometimes use your social security number as an identifier.

So, if your social security number was potentially compromised, we sent you a letter describing what we're doing to help support you, and how you can help protect yourself with credit monitoring.

If the letter you receive doesn't mention your social security number, then your social security number was not compromised.

If you didn't receive a letter at all, or if you're uncertain, please do reach out to Maureen Valentino directly, at 508-935-3417, or via email at fhs@bu.edu.

Now, fortunately, the use of social security numbers by health systems is an older practice that is quickly disappearing, and that should mean a lot less risk in the future.

Also, it's very important to say that we've implemented several checks and new systems to detect and remove unexpected inclusion of social security numbers in future records that we receive from outside sources.

We'll describe a little bit more about that a little bit later in the webinar. But I just want to reiterate. Please put your questions into the QA Box now, so that we can address them as we get to the end of your pre-recorded questions.

Thanks, Don. Several people have asked us what took so long to inform us.

We understand the frustration with the length of time that passed before notification letters were sent to you. We too, felt the urgent need to communicate with participants. But 1st we wanted to be sure, we had the correct information to share with you.

The investigation was quite complex and took time for us to understand what happened and what data was involved.

We worked with breach response teams both at Boston University and at the National Institute of Health and the National Heart Lung and Blood Institute, with expertise in cybersecurity, who advised and assisted the Framingham Heart Study team. During this time

Boston University also contracted with a company that specializes in these types of data security incidents.

The Framingham Heart Study is funded by the National Heart Lung and Blood Institute of the NIH, and therefore needs to follow guidelines for breach response that includes obtaining approval from NIH and the Department of Health and Human Services, and that approval needs to be had prior to being able to send notification letters.

Once we received approval, we also wanted to be sure that we were able to set up a call center to receive and answer your questions.

All of these steps took more time than we had hoped for.

So now, tonight, we're holding this webinar to allow you our participants to hear more information and have the ability to ask questions that are important to you.

We're committed to continuing our outreach to any of you that have questions or concerns. Again, please contact Maureen Valentino, if you did not receive a letter and would like one, and, as Don said, the security of your data remains our number one priority now, and going forward.

So one of you asked, How can my health data be used against me. For example, what could insurance? What could health insurance companies do with those records?

So most of the data that was breached contains research data that is linked only to a research id number, not directly to your name or your other personal information.

But if any of your health information could be linked to you personally, the law prohibits insurers from using pre-existing health conditions to make coverage decisions about you.

And, in fact, your insurance company may have far more data on your health status from your clinical encounters in the health system than was actually compromised in this attack.

we received several questions relating to the nature of the attack, and why encryption or other measures did not protect FHS data.

The attackers gained access to the data by compromising an administrative account, allowing the attackers to bypass protections around the data, including access permissions and data encryption. While the investigation could not determine exactly how the account was compromised. Evidence suggests that attackers exploited a recently discovered vulnerability in one of FHS' network security devices. The device’s vendor identified the vulnerability only shortly before the incident.

The attack was detected by enhanced security monitoring that FHS deployed earlier in 2024. Less than an hour after the file extraction began, Boston University and FHS quarantined, the affected server interrupting the breach. Unfortunately, the attacker was able to copy some files before the server was quarantined.

We also received questions about what changes have been made to secure FHS systems, and information and, going forward, what are we doing to ensure the security of your personal information?

Immediately following the FHS attack, we reset all passwords, and conducted a full review to ensure that the attackers did not have access to any other FHS systems. We added another layer of protection between the Internet and FHS, requiring 2 distinct authentication steps with different accounts to remotely access any FHS systems

in response to the vulnerability in the network security device. We have new protocols in place to ensure that vendor updates that address immediate risk are applied as quickly as possible.

FHS has also conducted an external review of systems, and is strengthening security in several ways, including protections to regular and administrative accounts, strengthening protections for and around sensitive data, and further improving our ability to monitor FHS systems for any security concerns. As a result, FHS systems are even more secure now, and we are making significant additional investments throughout 2025. We will take all reasonable steps to keep your data secure. Going forward.

Finally and importantly, we have removed external access from the web to servers that hold personally identifiable information, including things like your birthday name and address. We are still painstakingly reviewing files, archiving those with personal information to an offline location and deleting personal information where appropriate so security numbers have been removed from all medical records going forward, personal information will only be accessible on a server with no external access.

Access to this data will be further restricted, and additional formal approvals will be required to access this data, providing a greater level of protection.

Several of you reached out to know whether you were among the participants whose social security number was obtained.

If you received a letter that discussed this, then you were among the 106 affected people.

If your letter did not discuss your social security number, then yours was not obtained in the breach.

If you did not receive a letter, or you're not sure. Please do not hesitate to reach out to us directly at 508-935-3417, or via email, at fhs@bu.edu, and ask for Maureen Valentino.

We acknowledge that there is increased concern for this group of 106 participants who had their social security numbers included in the breach, and we have offered 2 years of credit monitoring service for free.

We also encourage any of you to reach out, if you would like, information on how to make your personal information more secure. Generally.

unfortunately, these types of hacks are occurring with increased regularity, with hackers finding their way into banks, credit card companies, and all aspects of life. It's always important to make sure you're as protected as possible. We encourage you to remain vigilant. Monitor. Your financial accounts question suspicious charges with your credit card company.

so I think that brings us to the end of the questions that you had submitted before the webinar, and we'd like to transition now to address some of the questions that we hope you've been submitting online. So we're waiting for some of those to come up now. But again, please take this opportunity to use the QA. Box at the bottom of the screen to enter your questions. We'll try to address them as quickly as possible. And

While we're waiting for those to come up.

just want to thank you again for participating tonight.

So it looks like we. We do have an initial question here, which is, what is the current status of the investigation?

So at this time we have completed the investigation of the incident, and we're confident that FHS systems are secure.

We've provided information to Federal law enforcement and other law enforcement agencies so they can pursue the cyber attackers, and we've also monitored the dark web to see if these bulk data from Framingham have appeared anywhere

as of a month ago. The data have not appeared on the dark web. Now that's no guarantee that this data has not been shared. So it is important to remain vigilant and to check your Free credit reports at regular intervals. Please do that. It is a Free Credit report. You can find how to do that online, and it's important to do that, regardless of whether your social security number was compromised in this attack or at any other place.

So another question that came in, why did we have social security numbers? In the 1st place?

Well, it's important to say that social security numbers were not part of the routine internal data files that were accessed by this attack. It's very important to say that, unfortunately, as we mentioned earlier social security, numbers were present on some medical records that we had received from outside health systems here at the Framingham Hearts study.

Now the practice of including social security numbers on medical records is diminishing. Health systems are doing this less and less because they understand it puts them at risk, too.

and Framingham is taking extra precautions to ensure that social security numbers are not inadvertently included in any documents we receive from outside. So as of now, all social security numbers have been removed from medical records we've received at Framingham. Here at the heart study, and there will be instances of social security numbers on medical records here going forward, so that that part of this attack could not be repeated.

Sure. Can you repeat slowly the contact information for Maureen Valentino? So Maureen can be reached directly at 508-935-3417, or if you prefer email, you can email Maureen at fhs@bu.edu.

and maybe we'll ask one of our zoom monitors. If they can put that in the chat for everyone, or do something similar. If we can post it on there, we'll try to. We'll try to put it up there, so you can also see it and not just hear it.

And I'll also repeat that if you did not get a letter, or you're not sure if your social security number was accessed in the breach again. Contact Maureen. Maureen Valentino can help you with that information. She can resend a letter or look you up in our database to see if that was included.

Do we have the contact information going out great. perfect. So please look on your screen. The contact information should be available to you there.

So the question, do we know who the breachers are? We are not able to identify the individual or group responsible or their country of origin. We did do quite a bit of forensic investigation to understand who may have done this, but unfortunately we were unable to make that determination.

Chris, do you think it's possible that this was not actually a real person, but a bot? Just kind of randomly scraping data. How does that happen? It's unlikely that it was a bot that for this kind of incident we generally don't see bots, you know, doing this kind of compromise. It's more, much more likely to be human actors. Doing this this kind of compromise.

I think we've come to the end of submitted questions. But please take this opportunity. We're happy to wait a little bit longer if you're still typing your question.

so please do go ahead and submit those.

Maybe I'll also just remind you that we are recording tonight's presentation. We're going to post it and we'll give you the information, for where this will be posted, so that you can watch it again if you need to share it with family members or other participants who may not have been able to make it tonight.

So it sounds like we have a few questions about credit monitoring. What are the processes involved there? We actually have some wonderful sort of step by step, instructions about how to access your free credit reports and how to do simple things that can, you know, protect your credit cards and your other information.

In fact, that information was provided to us by one of the members of the Friends of the Framingham Heart Study group, which is, you know, a really wonderful group of volunteer participants who help us every day do what we do better. You can access, and we're happy to send to you that really nice sort of step by step, instruction sheet about how to protect your data.

Again, the best person to contact is Maureen Valentino. And again, you can call her at 508-935-3417, or you can email her at fhs@bu.edu

And again we have a nice sort of cheat sheet for you. Even if you weren't 1 of the people whose social security numbers may have been compromised here. It's a good idea to take a look at this sheet, and just do those simple things that may help protect you from a breach that occurs anywhere in our society, because they are happening more and more frequently.

and just waiting to see if there are any last questions coming in.

It doesn't appear so.

so maybe I'll take this opportunity to thank Mr. Chris Sedore and my partner, Dr. Joanne Murabito. Again. It is a huge honor for me to be back here. And I just want to assure you once again that you know we were. We will be working tirelessly to do everything possible to make sure that you know there are no opportunities for this to happen again.

And you know we're not going to rest until we, you know, figure out how to how to really optimize this. So please don't hesitate to reach out again. If you have further questions.

we really treasure your participation in the study what you have donated in terms of your time, your efforts, your blood, your physical measurements over generations, has changed the world, and we really understand that and value that. So thank you again for your participation. Thank you for being here with us tonight. And again we look forward to seeing you in the future here at the heart study.

And it looks like we do have a late arriving question. So, Chris, you want to take that? Sure.

So the question is, how might this data breach impact my credit rating?

If your social security number was included in the breach, please follow the instructions in your letter or reach out to Maureen Valentino. Credit monitoring is being offered at no cost to help you help to help protect you at this time.

I think I might add, that it's really important, not only to check your credit report, but also look at your credit card statements, you know, if there's charges there that don't seem to belong.

you can dispute those charges with your credit card company, just call them, and you know they have systems in place to help you dispute those. So you know, it's just a good idea to be aware of what charges are appearing there. And that's another simple step that you can do to help protect yourself and therefore protect your credit rating.

Okay, so I think those are the last of the questions.

And again, we want to thank you so much for participating tonight, but also for joining us. And please know that that we are here for you, and we look forward to hearing from you.