Cooper, Richard

From: Matthew E. Anton <Matthew.E.Anton@hitchcock.org>
Sent: Tuesday, June 4, 2024 8:00 AM
To: Cooper, Richard
Subject: RE: TEMSIS data request.
Attachments: Copy of TEMSIS Encounter data_6_3.xlsx; EMTS Identifiable_6_3_24.docx; TEMSIS Transporting agencies.xlsx; EMTS Data Management and Security Plan_MA 6_3.docx; TEMSIS project_N_5_31.docx

Follow Up Flag: Follow up
Flag Status: Flagged

Chip,

Sorry for the delay in correspondence but I think I have good news. I reviewed your email and general security concerns with John Macchella, our associate chief health information officer, and it seems we all have the same concerns. Our system has multiple safeguards in place to guard against the exact type of absentmindedness you mentioned. Our plan will be to keep the data on a shared drive that only the team and IT could access behind the firewall. The password protected DH issued laptops that we use, if misplaced, can be immediately wiped remotely, so it would not be considered a breech even if that were to occur. Him and I filled out the form together and we are hoping the verbiage will suffice, even if we were unable to answer a question or two directly.

Additionally, I was able to make some changes to the proposal that you had pointed out in prior correspondence. I added in response time and dispatch time. We did submit the project IRB exempt process, which was approved. The one area I am still having an issue is being able to find the exact NEMSIS element name. Is it possible for DOS to either do that part or potentially show me how to find the first couple via virtual meeting. That may be a little much but I figured I would ask. I added 1 additional member to the team, another resident who could help with the writing.

I have attached updated forms and requested documents. Please let me know if there are additional steps I can take to move the project forward. My hope is to have this reviewed at the privacy committee at this months meeting.

Matt

From: Cooper, Richard <Richard.L.Cooper@DOS.NH.GOV>
Sent: Wednesday, February 21, 2024 11:19 AM
To: Matthew E. Anton <Matthew.E.Anton@hitchcock.org>
Subject: RE: TEMSIS data request. **EXTERNAL**

Matt,

The security form was built primarily around the HIPAA risk assessment tool, since I know I have people making requests that haven't even thought about that or ever done one. Supplemented with stuff taken from forms from UVM and some other state EMS offices. I agree the form may use language that is a bit more complicated than necessary. I'm open to looking at simplifying the language, but not necessarily the security concerns. My greatest fear is that a busy (or maybe even distracted/absent minded) academic researcher will be walking around with our data on an unencrypted laptop with poor password management and no physical security – often leaving it unattended or unsecured while heading to

lunch or forgetting it somewhere and the device gets stolen or hacked and now we have a major problem. I have many undergrad and graduate students contact me asking about data and I know they haven't put any thought into how they need to secure the data, much less their own device for everyday use.

All that being said, I am not a security expert, so I need to rely on national standards and examples from organizations that have teams that do that stuff. If your guy has some examples that insure maximum security of data, especially when combined with any other data sources, I'm open to looking at it. I have to admit, I have pretty limited bandwidth right now (think 2-3 hours) to work on this at all as I'm about to be down a full-time staff person, so if he can provide examples and back them up with technical supporting basis to prove that we can assure that anyone filling the form out will be able to employ the measures and that they would pass a HIPAA risk assessment based on their security plan, I'm totally open to looking at it.

Regards,

Chip

Chip Cooper, MPH, NRP
603-223-4200
richard.l.cooper@dos.nh.gov

For Help with TEMSIS, Elite, Hospital Hub or Online Learning Academy, please submit a helpdesk ticket to: Helpdesk [nhfa-ems.com]

From: Matthew E. Anton <Matthew.E.Anton@hitchcock.org>
Sent: Tuesday, February 20, 2024 10:24 AM
To: Cooper, Richard <Richard.L.Cooper@DOS.NH.GOV>
Subject: TEMSIS data request.

Chip Cooper,

I hope all is well. I am a general surgery and preventive medicine resident physician at Dartmouth Health. A while back we corresponded about an external data request from the TEMSIS database to do a Trauma/EMS project that could assist the TMRC.

Unfortunately despite sending the security form through multiple pathways I always ended up not getting to anyone with access to the details of some of the questions on the form.
This leaves me to attempt to fill it out to the best of my ability, knowing that some of the details will not be provided and hope for the best. I could make it clear that our plan is to use a shared drive with limited access, behind the Dartmouth Health firewall, which you mentioned sounded good.

On the other hand, I was wondering if the DOS was open to simplifying the forms for external requestors of TEMSIS data. I have been in dialogue with John Mecchella, the associate chief information officer at DH, who is the go-to informatics contact for the preventive medicine program. One of his roles is to help clinicians access data both through our analytics institute but also external databases. He thinks that the data security form I have presented to him is more complex than other security forms for state managed health databases. He is willing to virtually meet to discuss further. Although perhaps a harder route, coming up with a more feasible pathway for academic researchers to access TEMSIS data does seem like a valuable thing for the future. At the end of the day, I would think our institution has the safeguards in place to protect PHI, it seems the hiccup is in the paperwork proving that.

Let me know what you think. I am also happy to converse in any other medium. Thank you again for your time.

Matt Anton
815 354 5519

IMPORTANT NOTICE REGARDING THIS ELECTRONIC MESSAGE:

This message is intended for the use of the person to whom it is addressed and may contain information that is privileged, confidential, and protected from disclosure under applicable law. If you are not the intended recipient, your use of this message for any purpose is strictly prohibited. If you have received this communication in error, please delete the message and notify the sender so that we may correct our records.