## Q&A Summary for Data Security Refresher, 2/25/2015

| # | Questions | Answers |
|---|---|---|
| 1. | Does this data have to be encrypted when being submitted to HRSA? | Yes, when you upload the data (for the RSR or ADR), it goes through an encrypted site.<br>Grantees and providers do not need to encrypt their XML files further. |
| 2. | Does it have to be encrypted on the server? | If it is a secure server, it does not need to be encrypted. If the data are not on a secure server, then yes, absolutely, the data should be encrypted when "at rest."<br>If you need to remove your data from behind your secure server in order to upload to HRSA, as some grantees have reported, then you should remove the data from the temporary location as soon as possible after upload. |
| 3. | Do you have any guidance about whether or not to send data via email WITHIN an organization? | You should discuss this with your IT security staff. In general the answer is no, data should not be emailed. |
| 4. | In this age where participants are increasingly accustomed to, (even expecting) e-mail communications with PHI, what is proper protocol for communicating via e-mail? Encrypting file attachments and e-mailing the encrypted attachment with a password given over the phone? | Again, using email is an open channel, rife with opportunity for mistakes (e.g. forgetting to encrypt, or encrypting with insufficient protections). Email can be intercepted and read.<br>The safest way to do this is to use a secure patient portal that requires login. |
| 5. | Some of us use encrypted email services to communicate between providers. The email is coming out as an encrypted packet. The recipient needs a username and password to open the attachment. Is this sufficient? | Your IT security department should frequently review the federal standards to ensure they understand what is required for compliance. In general the answer is no, data should not be emailed. |
| 6. | It is my understanding that secure e-mail services that provide end-to-end encryption are HIPAA compliant. Are you saying that it is not ok to transmit PHI in this way? | See above. In general the answer is no, data should not be emailed. |
| 7. | Can a DUA be included as a separate document to be signed between parties or can it be included in a grant | It can be included in a contract. If someone is asking you to sign something that looks like a legal agreement that includes language about data use and sharing, |

| # | Questions | Answers |
|---|---|---|
| | agreement or MOUs? | that is, for all intents and purposes, a data agreement. |
| 8. | Can provider id or org id be considered as an identifier?<br>Likewise, an EIN or the provider registration code used for the RSR web system? | Proceed carefully! If it can be cross-referenced with other identifiers to identify an individual (especially in smaller populations or sub-groups), then this starts to become a security concern . |
| 9. | How do we reconcile the requirement to provide patients with their records in a method preferred by them with the no email rule? | Patient portals (e.g. secure FTP sites) are recommended. These require patients to login to view their data. |
| 10. | Can URNs be emailed in a list format through a password protected worksheet? | This is not advisable, because the clients' full date of birth is part of the URN before it is encrypted.<br>Password protection is not sufficient. |
| 11. | Are password protected data files (e.g., excel, SPSS) sufficient to comply with security requirements? | No, they are not. |
| 12. | Does the CAREware server have to be encrypted? | No, the server does not have to be encrypted. It is usually the data transmission that is encrypted or the storage of certain fields in the data that is encrypted. Those are doable in CAREWare but may have an impact on transmission performance over a network. |
| 13. | Has HRSA done a HIPAA review of CAREWare used by covered and non-covered entities for coordination of care? | HRSA has not done such a formal review, but the software meets all the basic HIPAA technical requirements for software such as password length, duration, etc. Remember, CAREWare is a distributed application and therefore agencies themselves must do their due diligence to secure the data on their computers, and run over networks etc. HRSA is not responsible for that. |
| 14. | In Texas, we use the ARIES client # in email, but NOT the URN per HRSA definition (The URN is PHI). Can you confirm this?<br>Isn't the ARIES number an identifier, conceptually much like a medical record number? | Medical record numbers are considered one of the 18 identifiers that are considered vulnerable information. In general the answer is no, data should not be emailed. |

| # | Questions | Answers |
|---|---|---|
| | | |
| 15. | Can we print the presentation slides? | A recording of this webcast, along with a copy of the slides with notes, as well as the Q&A summary will be posted to the TARGET Center website within 1-2 weeks.<br>https://careacttarget.org/content/webinar-and-call-archives |
| 16. | Where can I find the Federal standards for data protection? | You can find them on the HHS Office of Civil Rights Health Information Privacy page:<br>http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html |
| 17. | Are there any requirements to have a certified EHR in order to hold this type of patient data? | HAB does not require grantees or providers to use a certified EHR. The main requirements are that protected health information (PHI) be kept secure. |
| 18. | When you say "cross-referenced" does that mean within the same document, or any other document that could potentially be acquired by some other method? | It means the latter. It is much easier now than it used to be to get the missing pieces to identify someone than it was just a decade ago. |