Gravely Group

TEFCA PRIVACY AND SECURITY CONSIDERATIONS

National Committee on Vital and Health Statistics

Full Committee Meeting

April 12, 2024

Steve Gravely Esq., Founder & CEO, Gravely Group

www.gravelygroup.com

About Gravely Group

Gravely Group was founded in 2018 by Steve Gravely. After more than 30 years in Big Law, Steve decided he wanted to do things a bit differently. Gravely Group operates virtually (and was doing so pre-COVID) and leverages technology to provide smarter, more efficient, and more affordable legal services to clients in the digital health sphere.

- 40 years in the healthcare industry
- 30 years providing legal counsel to healthcare organizations
- 10 years focusing on digital health issues including EMRs, interoperability, health information exchange, and cybersecurity

Steve Gravely

Steve's unique perspective on healthcare originates from his experience as a firefighter and EMS provider during college. Today, Steve serves as a volunteer member of the National Ski Patrol, responding to accidents on the mountains. First responders must be calm, skilled, and able to use whatever resources are available to overcome immediate challenges- and it's this "first responder" mentality that Steve brings to his work representing healthcare organizations on complex legal and strategy issues.

TEFCA Approach to Data Privacy

Protecting the privacy of health data is built into the DNA of TEFCA

- Specific Eligibility Criteria that organizations must meet to become a QHIN
- QHIN Designation Process is rigorous and requires demonstrated ability to protect the privacy and security of TEFCA Information (TI)
- TEFCA supports specific Exchange Purposes for the transaction of TI and each EP has specific requirements

Data Privacy

HIPAA Covered Entities

The Common Agreement recognizes that some QHINs, Participants and Subparticipants (Q/P/S) are already subject to HIPAA as either covered entities or business associates of covered entities and this continues under TEFCA

Non-HIPAA Entities

For Q/P/S not already subject to HIPAA (Non-HIPAA Entities or "NHE"), the Common Agreement requires compliance with specific sections of the HIPAA Privacy Rule as a matter of contract for all Individually Identifiable Information as if it is PHI.

NHE does *not* include the following:

- Public Health Authority
- Government Benefit determination entity
- Government Healthcare Entity
- Other entity exempted by an SOP

TEFCA Data Privacy

All Q/P/S must have a written privacy policy describing its privacy practices for Individually Identifiable Information that is used or disclosed via TEFCA,

- If a Q/P/S is subject to HIPAA, then its HIPAA NPP will be deemed to meet this requirement
- If a Q/P/S is an NHE, it may already have a privacy policy due to other applicable law, but if not then it must develop one

This approach establishes a consistent set of obligations across the diverse set of Q/P/S and promotes trust among all TEFCA participants that the privacy of TEFCA Information is protected

IAS Providers are subject to very specific requirements that are laid out in an SOP regardless o whether the IAS is provider is a QHIN, a Participant, or a Subparticipant

TEFCA Approach to Data Security

The Common Agreement requires QHINs to comply with the HIPAA Security Rule as if they were subject to HIPAA

- Including NHEs
- Requirement flows down to Participants and Subparticipants via the Terms of Participation

QHINs must be certified under a nationally recognized certification body approved by the RCE

- HITRUST is currently the only approved certification body
- Rigorous certification process

QHINs must have an annual technical audit conducted by a third-party to assess compliance with the HIPAA Security Rule, NIST Cybersecurity Framework, comprehensive penetration testing

TEFCA Data Security

The Common Agreement requires the RCE appoint a Chief Information Security Officer (CISO) who is responsible for monitoring and maintaining the overall security posture of the TEFCA Framework

The Common Agreement requires each QHIN have a CISO who is responsible for evaluating the security posture of the QHIN and addressing threats

The TEFC Security SOP establishes a Cybersecurity Council which is responsible for assessing the cybersecurity risks to the TEFCA Framework and addressing those risks

- RCE CISO serves as the chairperson
- The TEFCA Transitional Council selects 5 QHIN CISO's to serve on the Council

TEFCA Data Security

Liability Coverage for Cyber Threats

- The Common Agreement limits the liability of each QHIN to $2M per incident/$5M, aggregate
- QHINs are required to obtain cybersecurity insurance in the amount of the TEFCA liability limits
- Alternatively, a QHIN can show financial reserves in the same amount
- A combination of insurance and reserves is also permitted

Security Incident Notification

- QHINs must report a TEFCA Security Incident to the RCE and all QHINs that are likely impacted by the incident
- Notification must be made within 5 days of discovery *(may be revised in CA v. 2.0 and a future SOP)*
- The notification must provide enough information to provide the RCE the nature and scope of the incident
- The Terms of Participation requires P/S to notify its upstream Q/P/S and its own Subparticipants of a Security Incident

TEFCA Data Security

Data Encryption

- A Q/P/S that is subject to HIPAA must comply with the HIPAA Security Rule requirements for data encryption
- All NHEs must encrypt all Individually Identifiable Information that it maintains both in transit or at rest regardless of whether the information is TEFCA Information

Restricted Use

- The Common Agreement and the Terms of Participation restrict the use or disclosure of TEFCA Information outside the US
- Any use or disclosure must comply with the HIPAA Security Rule or other applicable law
- Applies regardless of whether the Q/P/S is a HIPAA covered entity or business associate

Gravely Group

THANK YOU

QUESTIONS?

CONTACT:

Steve Gravely, Esq.
Founder & CEO, Gravely Group
steve@gravelygroup .com

www.gravelygroup.com