CTTI

Appendix 2: Approaches to Securing Data Generated by Digital Health Technologies

This appendix lists approaches to securing data generated by digital technologies across its lifecycle. This list reflects strategies that are being successfully employed at the time of publication, as indicated by our evidence gathering activities. It is beyond the scope of this work to suggest which approaches may be appropriate for a particular study, but per the recommendations, sponsors should apply end-to-end, risk-based approaches to data security. Approaches required by applicable regulations are printed in **bold**.

It is important to note that the list of approaches below is not exhaustive. Also, that it is unlikely that any single approach at any stage of the data lifecycle will adequately ensure its security. Finally, practices listed here are likely to evolve rapidly with both experience and technological advances.

Approaches for securing data stored on digital technologies:

- Automatically encrypt data when stored locally on the digital technology
- Restrict the users' access to data so they cannot tamper with them or view them, as it was believed that viewing data could bias future data collection
- Retrieve data from digital technologies as soon as practically possible
- Limit the amount of data stored on the digital technology
- Automatically back up data stored on digital technologies to manufacturer's secure storage platform.
- Limit the variability of digital technologies used in the study so that researchers have more ability to manage security issues.
- Program software to require users of any digital technology containing personal or other sensitive information to authenticate themselves sufficiently to permit access.
- Program software to include automatic timeouts with screen blanking and secure login for extended user inactivity
- Educate participants about the importance of data security
- Instruct participants on how to secure their data

Approaches for securing data during transfer from the digital technology to the server:

These approaches are similar to existing best practices for 'traditional' trials transmitting data from remote sites back to the central study site, and include:

- Use a secure network encryption certificate, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), and transmit data wirelessly over Hypertext Transfer Protocol Secure (HTTPS), or similar secure file transfer protocol such as SFTP (Secure File Transfer Protocol)
- Perform "checksums"[*] or "two phase commits" to help support the that the data sent matches the data received and that no data were lost or changed during transfer

[*] Checksums are algorithm-based processes developed with the sole purpose of detecting errors introuced during the transmission and/or storage of data

- Include “Certificate Pinning” software on the digital technology and on the server. This helps ensure that the technology(ies) used in the study would only be able to communicate with servers with the correct pin, and servers, likewise, would only be able to communicate with technologies that had the correct pin.
- Use a hardwired transfer (i.e., plugging a digital technology directly into a computer that can access the secure server to upload data from the technology). This approach increases both security and participant burden.

Approaches for securing data during storage[†]:

Many of these approaches are the same as existing best practices for securely storing data in ‘traditional’ trials:

- Require multiple layers of authentication to access the data
- Use a server that can only be accessed internally or through a Virtual Private Network (VPN) type setup. The VPN should require multi-factor authentication to access. The dataset may also be encrypted and tokenized while on the server and require a passcode to access.
- **Maintain a log of who accesses the data server and when** (which will be helpful in the case of security breaches)[‡]
- Encrypt data at rest (in storage) — helpful if a copy of the database inadvertently ends up in the wrong hands, as encrypted data is unreadable without the accompanying application
- Work with a security vendor or commercial company that has agreed to a HIPAA Business Associate relationship, invested in secured data storage for their business, and who can provide evidence of compliance with industry or government standards for data

Additional approaches for securing data generated by digital technologies:

- Review or audit security procedures for server hosts to ensure they have adequate standard operating procedures (SOPs) for routinely reviewing who has access to servers, for disabling access for individuals when required (e.g., someone leaves the company), and for secure backup of study data. Note that these SOPs are covered under SOC 2 and ISO 27001 certifications
- De-identify data as soon as possible or refrain from capturing personally identifiable data via the digital technology (e.g., provide unique identifiers to participants during enrollment and to use when registering their technology in place of their name)
- Implement a “security umbrella protocol” built into an app that manages three levels of security: authentication, encryption, and non-repudiation (transferring the right data from the right source)

[†] Storage in this instance refers specifically to data at rest within the data infrastructure of the trial, although similar approaches could be taken to secure data archived for long term storage to comply with applicable regulations.

[‡] While we did not collect evidence that blockchain technology is currently being used for audit trail processes, CTTI recognizes that blockchain may be valuable here