Table 3: Promoting and Protecting Data Integrity

This table outlines CTTI recommended strategies for promoting and protecting data integrity during critical steps in its lifecycle. CTTI recommends the following best practices for implementation either during the pre-trial planning phase or during the conduct of the trial. This list is not meant to be exhaustive and may be adapted to individual trial requirements. For additional considerations pertaining to data integrity, please reference Section III-1 of the recommendations.

Critical Point in Data Lifecycle	Pre-Trial: CTTI Recommended Practices	During Trial: CTTI Recommended Practices
Data collection	▶ Appropriate mobile technology selection (see recommendations on mobile technology selection ○ Mobile technology selected with the needs, preferences and abilities of the study participants in mind ○ Mobile technology verification ▶ Development of effective technology user training program (see recommendations on mobile technology training)	▶ Effective, centralized monitoring (see recommendations on data monitoring) ▶ Effective training and support for all mobile technology users (see recommendations on mobile technology training and support)
Generation of processed data	▶ Appropriate mobile technology selection (see recommendations on mobile technology selection) with a specific focus on verification and validation	▶ Effective, centralized monitoring (see recommendations on data monitoring)
Data during transmission	▶ Appropriate mobile technology selection (see recommendations on mobile technology selection) ▶ Pilot test data transmission and retrieval systems	▶ Secure, computer-generated, time-stamped, electronic audit trails of users' actions and changes to data[1] ▶ Data security measures such as data encryption, checksums[2] and tokenization.
Data at rest[3]	▶ Include services such as backups and disaster recovery arrangements in service level agreements with outsourced electronic service vendors ▶ Develop a risk-based data security system based on an information security assessment (see recommendations on data security) ▶ Formalize and document processes for requesting, changing and removing access rights using the principles of ***'need to know'*** and ***'least privilege'***	▶ Secure, computer-generated, time-stamped, electronic audit trails of users' actions and changes to data[1] ▶ Implementation of a robust, risk-based data security system (see recommendations on data security). May include such measures as data encryption, checksums[2], and tokenization. ▶ Regularly review and audit 1) access rights and 2) users with access to data
Data during filtering and processing for analysis	▶ Existing best practices for preparing analysis datasets from raw data sets continue to apply	▶ Existing best practices for preparing analysis datasets from raw data sets continue to apply

[1] Note: the use of these audit trails should not obscure any original information that may be modified
[2] Checksums are algorithm-based processes developed with the sole purpose of detecting errors introduced during the transmission and/or storage of data
[3] It is noteworthy that the strategies recommended for promoting and protecting the integrity of data at rest are likely already being applied to electronic clinical trials data