Session III: Data Management

Bill Bates, Validic
Phil Coran, Medidata Solutions
Andy Coravos, Elektra Labs
Cheryl Grandinetti, FDA, CDER
Ashish Narayan, Mount Sinai Health System
Session III Relevant Materials

Data Management handout

CTTI recommendations and resources:

- Recommendations
- Related Resources
  - Data Flow Diagram
  - Strategies for Promoting & Protecting Data Integrity
  - Approaches to Securing Data Generated by Mobile Technologies
- Related Case Study
  - Using Remote, Smartphone-Based Data Collection to Broadly Share Health Insights

Glossary: Definition Technical & Regulatory Terms
Data Management

For mobile technology-derived outcomes data, sponsors should consider:

- Data integrity
- Data security
- Data usability and availability

Sponsors are ultimately responsible for data management, but processes are often carried out by, or in partnership with third parties, such as:

- CROs
- IT service providers
  - Mobile technology manufacturers
  - Third-party data platforms
CTTI Recommendations on Data Management

- Guide sponsors on how to extend relevant regulations and guidance to management of data captured by mobile technologies in clinical trials.

- Highlight specific data management tasks that should be internally reviewed or discussed with potential partners prior to entering into an outsourcing agreement.
Session Overview

- Q&A with technical and regulatory compliance experts
  - Data authenticity, integrity, and confidentiality
  - Optimizing data access
  - Investigator access to the data
  - Sponsor access to the data

- Presentation: A deep dive into data access – new opportunities and challenges in the digital era

- Presentation and panel discussion: Data security

- Questions from the audience
Q&A with Technical & Regulatory Compliance Experts

Cheryl Grandinetti, FDA, CDER (host)
Bill Bates, Validic
Phil Coran, Medidata Solutions
## Data Authenticity

<table>
<thead>
<tr>
<th>Data Characteristic</th>
<th>Supporting CTTI Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precisely &amp; accurately represent what the data claim to be measuring; e.g., heart rate (bpm) or activity (steps/day)</td>
<td>See recommendations on mobile technology selection, specifically verification and validation</td>
</tr>
<tr>
<td>Be correctly attributed to the intended participant</td>
<td>See recommendations on data attribution</td>
</tr>
<tr>
<td>Contain metadata indicating the source of the data and a UTC time stamp</td>
<td>See recommendations on audit trails</td>
</tr>
<tr>
<td>It should also be possible to demonstrate that the data have not been corrupted following creation</td>
<td>See recommendations on data integrity and audit trails</td>
</tr>
</tbody>
</table>
Data Flow Diagram

Study team has read only access to an appropriate level of data through an API

Mobile Technology → Apps → Manufacturer’s Servers → Centralized Server(s) → Filtering & Processing → Dataset for Analysis

TYPICALLY SUBJECTS AND SITES
TYPICALLY CROS AND/OR OTHER ELECTRONIC SERVICE VENDORS
TYPICALLY STUDY SPONSORS

Strategies for Promoting & Protecting Data Integrity

CTTI resources advises best practices for promoting trial integrity at these critical points in the trial lifecycle both:

- Pre-trial
- During trial
## Confidentiality

Ensure participant data will not be shared beyond those whom the subjects have agreed to in the consent process.

<table>
<thead>
<tr>
<th>Data Characteristic</th>
<th>Supporting CTTI Recommendations</th>
</tr>
</thead>
</table>
| **Data Minimization and Transparency** | • Collect minimum data set necessary to address study end points.  
• Be transparent in IC process on nature of collection, extent, use, & access downstream. **Engage** potential subjects regarding access & use of data to obtain comfort.  
• IC requires transparent knowledge of how captured data to be used.                                                                                   |
| **Sensitive Information/Identifiers**  | • Identify all HIPAA (or similar) identifiers that the mobile devices collect or require even if they are not the focus of the protocol; mitigate risks associated with such collection/use.  
• Consider ONC MPN (model privacy notice) to form basis for privacy model/standardization.                                                                   |
| **Balanced Data Accessibility with Minimum Privileges** | • Meet accessibility during lifecycle (review, monitoring, inspection, etc.) while securing data on a least privilege basis.  
• Utilize data flow diagrams for the lifecycle of data and ensure access to data meets needs prior to contracting with an electronic service vendor. |
| **End-to-End, Risked-Based Security**   | Assess external dependencies (vendors), systems, procedures, people, policies, and applicable regulations.                                                                                                                    |
| **Other Resources**                   | Data Flow Diagram, Data Availability for FDA Inspection, Decision Support tool: Real Time Data Sharing with Study Participants, and Using Remote Smartphone Based Data Collection to Share Health Insights                               |
Limiting Access to Electronic Records to Authorized Individuals

Apply the security principles of:

- Need to know
- Least privilege
Q&A with Technical & Regulatory Compliance Experts

Cheryl Grandinetti, FDA, CDER (host)
Bill Bates, Validic
Phil Coran, Medidata Solutions
Automated Quality Monitoring

When mobile technologies are used for data capture, existing monitoring guidance still applies…

- Centralized monitoring is well suited to check for completeness, consistency, and correctness.
  - Source Data Quality Attributes: ALCOA (+ ICH E6 R2)

- Develop monitoring plans and strive to correct technical issues earlier.

- Monitoring plans should articulate who should resolve potential issues as identified.

Q&A with Technical and Regulatory Compliance Experts

Cheryl Grandinetti, FDA, CDER (host)
Bill Bates, Validic
Phil Coran, Medidata Solutions
Data Rights & Governance Considerations in the Connected Era

Andy Coravos, Elektra Labs
We’ll start with a few grounding definitions...
I might not care that everyone knows that my blood type is O+, but I’d care a lot if someone could change my blood type to B- before my surgery and leave no trace.
Flow of Data Collected by Mobile Technologies

- Mobile Technology
- Apps
- Manufacturer’s Servers
- Centralized Server(s)
- Filtering & Processing
- Dataset for Analysis

Study team has read only access to an appropriate level of data through an API

Entering Into a New Health Data Paradigm

<table>
<thead>
<tr>
<th>Past</th>
<th>Today/Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Stock” - A person would get a new test result or piece of evidence every couple months or years.</td>
<td>“Flows” - Data can come in by the minute or second (e.g., heart rate information, continuous glucose monitoring).</td>
</tr>
</tbody>
</table>

**Human Readable** - Test results would be interpreted by a human (e.g., tissue samples, reactivity of a chemical compound).

**Non-Human Readable** - Many results now are from algorithms run on large samples of data (e.g., predictions of abnormal heart conditions). Not feasible for a human to double check analysis.

**Human Shared** - Results would be shared from one human (e.g., a doctor) to another (e.g., a patient), most often in-person, and with space for context and questions.

**Machine Shared** - A device or notification shares a digital outcome. Limited context exists to correct false positives/negatives real-time.
Sponsors should not assume that the technology manufacturer will provide them with all of the data collected by the mobile technology.

Prior to selecting a mobile technology for data capture, sponsors should consider:

- Whether they will have access to the raw data generated by the mobile technology,
- To what levels of processed data (see Table 1, Section 1 of recommendations document) they will have access,
- Whether they will have access to the algorithm(s) used to process the data, and
- In what format the data will be provided.
Factors to Consider Before Entering into an Outsourcing Agreement

- How will the data generated by the mobile technology be accessed and used by the manufacturer?
- What data will be provided by the manufacturer to the sponsor?

CTTI Recommendation:
Ensure that access to data meets your needs prior to contacting an electronic service vendor.
Would A Sponsor Want “Raw Data”? 

Let’s take “step count” for example:

A algorithm performs a series of computations (e.g., filtering and peak detection) to convert the sensor’s raw signal into an actionable metric (e.g., step-count)

Calculated using accelerometer, gyroscope, and potentially other sensors.

Combine those results with height, weight, age, gender, and other features.

What level of data would a sponsor want? 3-axis accelerometer? With gravity included? At what frame rate?

![Accelerometer Sensor Data](image-url)

Fig. 3 Gyroscope data recorded from the left shank for subject 2. The top graph illustrates a portion of running at 12 kph. The bottom graph illustrates a portion of walking at 2 kph. Stance, stride and swing times are marked with dotted lines.
Informing Patients: How Your Data Will Be Used

Sponsors should ensure that they are:

1. Aware, and
2. Comfortable with all of the ways in which data generated by participants in their trial will be accessed and used.

Sponsors should engage patients in determining acceptable access and use of their data.

Data access and use by manufacturers and additional third parties should be clearly defined in outsourcing agreements.
Informing Patients: How Your Data Will Be Used

In a 2017 CTTI Survey of 193 individuals in research database:

- More than half of potential participants reported not being worried that others, besides the research team, would be able to see their data collected by the mobile technology.
Informing Patients: How Your Data Will Be Used

- What about secondary data use?
- CTTI emphasizes the importance of collaboration, including secondary data use, to advance the development and broad acceptance of technology-derived novel endpoints.

- Recommends referencing the 2015 IOM report, “Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk”.

- Case Example: Using Remote, Smartphone-Based Data Collection to Broadly Share Health Insights
Applying an End-to-End, Risk-Based Approach to Data Security

Ashish Narayan, Mount Sinai Health System
Recent Breach Data

- There were at least 477 healthcare data breaches in 2017.

- Q1, 2018 has seen 77 data breaches.

- The main causes of healthcare data breaches in 2017 & 2018 are:
  - Unauthorized Access
  - Hacking
Recent Breach Data

Healthcare Data Breaches by Month

Breached Healthcare Records by Month

Causes of Healthcare Data Breaches (March 2018)

Mobile Adoption in Clinical Trials

Survey of pharma, CROs, and service providers conducted by Informa (Knect365) revealed:

- Currently, only 37% of companies involved in clinical trials are currently utilizing mHealth.

- mHealth technologies will play a key role in the future of clinical trials.
  - 94% of companies are looking to increase their utilization of mHealth in the future.
Data Security

CTTI recommends applying an end-to-end, risk-based approach to data security should be applied to protect participants’ privacy and the confidentiality and integrity of their data.

Mobile era creates new data security demands
- Data must be secured on both the technology itself and during transfer from the technology.
  - Transfer likely occurs over Wi-Fi, Bluetooth, cellular and networks beyond control of sponsors and ESPs
- Data must be secured during additional transfer steps (ex: app → server) and all processing steps.

CTTI recommends that data security solutions are developed with the entire infrastructure in mind.
“A Chain is Only as Strong as its Weakest Link”
A Risk-Based Approach to Data Security

- Extensive IT Security assessment
- Securing data access – authentication and authorization
- Securing data stored on mobile technologies
- Securing data generated by mobile technologies
- Securing data during transfer from the mobile technology to the server
- Securing data during storage
Expert Comments on Data Security

- Data security and privacy are not the same thing. Both can be absolute, but what's really needed is a risk-based approach; it's a balancing act.

- De-identification becomes hard, if not impossible, with this scale of data (e.g., Strava ‘breach’), making data rights and governance increasingly important if it’s not possible to have confidentiality.

- Beyond the scope of CTTI to recommend specific security solutions
  - Appendix 2 listing approaches to data security that are being successfully used at the time

- There are many approaches for securing data captured by mobile technologies.
Recommendations Recap

- Ensure the authenticity, integrity, and confidentiality of data over its entire lifecycle.

- Optimize data accessibility while preventing data access from unauthorized users.

- Ensure that access to data meets your needs prior to contracting an electronic service vendor.

- Apply an end-to-end, risk-based approach to data security.

- Monitor the quality of data captured by mobile technologies centrally through automated processes.

- Ensure that site investigators have access to data generated by their participants.
Resources Supporting these Recommendations

- Data Flow Diagram
- Strategies for Promoting and Protecting Data Integrity
- Case Example – Secondary Data Use
  - “Using Remote, Smartphone-Based Data Collection to Broadly Share Health Insights”
- Appendix of Approaches to Securing Data Generated by Mobile Technologies
THANK YOU.

https://www.ctti-clinicaltrials.org/projects/mobile-technologies

www.ctti-clinicaltrials.org