Data Collection, Use, and Protection

Guide Overview

Objectives

- Understand the confidentiality and compliance for collecting different kinds of data
- Gain knowledge on uses and best practices of collecting, storing, and transferring user data

Outcomes

- You have evaluated your technology and understand how to protect user data and comply with existing data policies
- You understand that data is important in multiple milestones along the commercialization pathway

Next Steps

- Continue to check in with users and customers data needs
- Ensure you are complying with and have proper systems in place for data collection, storage, and/or transfer

Relevant Resources

HIPAA

HIPAA

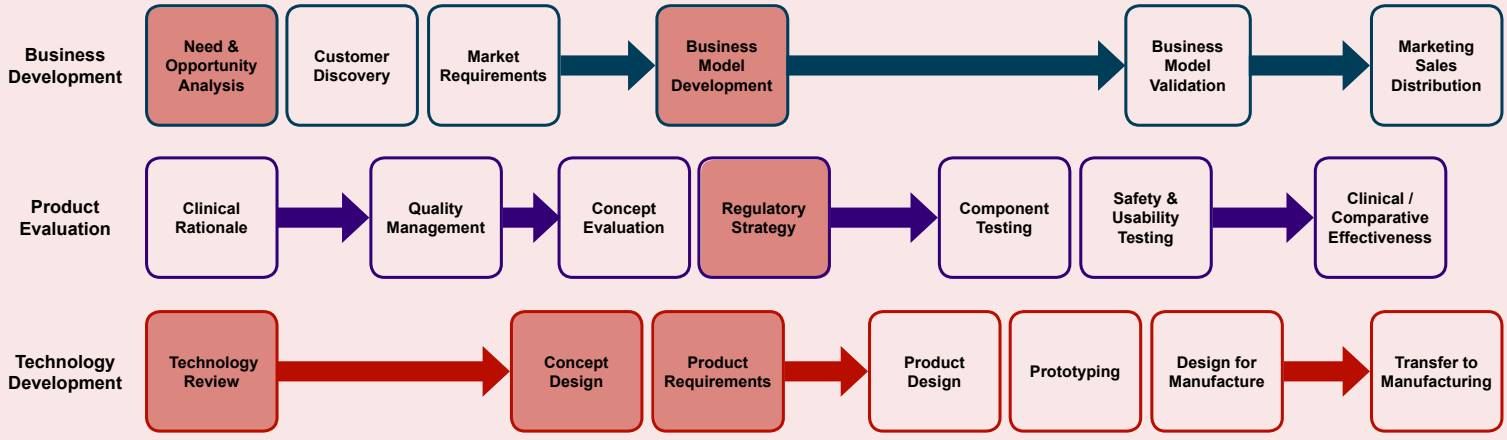
NIST National Institute of Standards and Technology U.S. Department of Commerce

Cybersecurity

Data Basics - Primary and Secondary Data

Customer Discovery Module

Commercialization Methodology



The Center for the Translation of Rehabilitation Engineering Advances and Technology

TREAT is part of the National Institutes of Health (NIH) Medical Rehabilitation Research Resource Network (MR3). Funding is provided by the National Center for Medical Rehabilitation Research (NCMRR) in the Eunice Kennedy Shriver National Institute of Child Health & Human Development (NICHD) through awards R24HD065703 and P2CHD086841.

10 Water Street, Suite 410
Lebanon, NH 03766
T: (603) 448-2367
F: (603) 448-0380
info@treatcenter.org

Data Collection, Use, and Protection

Data Module

Dealing with Data

In a world of constant technological progress, the drive for valuable data is expanding and evolving at a fast pace. Having access to data allows companies to understand their consumers on a more specified level - personalizing treatments, improving communication, and enhancing health outcomes. Using data to create a user-focused product will help improve the lives of your customers, and will also help your technology stand out amongst competitors. This module was created to help you grasp the many uses and considerations of data when it comes to your product.

Thinking About Data & How to Reduce Risk

As early in the product and business development process as possible, consider the following questions:

- Will you be *collecting data* with your device?
- Will you be *storing and/or transferring data* from your device?
- What will you *do with the data* after you collect it?

We will aim to help you answer these 3 questions in more detail inside the module.

Uses of Data

Research

Studies to show comparative effectiveness, safety, usability, and other results will require the collection and handling of various types of data dependent on study protocols. More often than not, this data use type will require conducting the study activities, data collection, and analysis under a protocol approved by an Insitutional Review Board (IRB).

Marketing

Data can help bolster marketing of your product and provide potential customers with the information they need to purchase the product. Conducting Customer Discovery (see Customer Discovery Module) to uncover the information that customers require in order to make a purchase will inform data collection and use for marketing purposes.

Monetization

Is there a question or insight for which your data can provide researchers, companies, or an outside entity an answer? This is an opportunity for monetization, that is, creating revenue out of the data you are collecting.

Business Insights

How a user engages with your product and the data collected through that engagement can help drive future product roadmaps and business decisions.

Collecting, Storing, & Transferring Data

Collecting Data

You can collect data in a variety of ways. A few examples include directly talking to end users early on in product development, through the use of your technology/device by a user, or as a follow up after using the device. Overall, how you use data, the type of data you are collecting, and how data is stored and/or transferred will require complying with various policies and standards. The following types of data described are not all-encompassing, but common to medical devices and health technology.

The Center for the Translation of Rehabilitation Engineering Advances and Technology

TREAT is part of the National Institutes of Health (NIH) Medical Rehabilitation Research Resource Network (MR3). Funding is provided by the National Center for Medical Rehabilitation Research (NCMRR) in the Eunice Kennedy Shriver National Institute of Child Health & Human Development (NICHD) through awards R24HD065703 and P2CHD086841.

10 Water Street, Suite 410
Lebanon, NH 03766
T: (603) 448-2367
F: (603) 448-0380
info@treatcenter.org

Device Performance and Maintenance Data

Data may be collected by the device itself to continuously monitor device performance. This type of data is not subject to regulations and is referred to as device performance and maintenance data. An example includes data collected via an hour-meter to track time and use before maintenance is required.

Physiological Data

Physiological data are collected through various types of technology. When collecting physiological data and information about a person's health such as a diagnosis of disease or a prescribed medication, it is important to recognize that this is sensitive data. This can include:

- Data collected from a patient with the medical device (i.e. X-Rays, blood pressure measurements, blood glucose measurements, body movement measurements, etc.)
- General Wellness collected from a user with a general wellness/consumer device (i.e. mental acuity, weight management, sexual function, etc.)

When paired with information that would identify the user, physiological data can become Protected Health Information.

Protected Health Information (PHI)

Protected Health Information, or PHI, requires compliance to Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

These policies pertain to individually identifiable health information, including demographic information, which relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

Personally Identifiable Information (PII)

Information that can be used to uniquely identify, contact, or locate a single person is referred to as Personally Identifiable Information or PII. Personal information that is "de-identified" (maintained in a way that does not allow association with a specific person) is not considered sensitive. While Social Security numbers are a type of PII, the legal requirements for protecting them are much more stringent than for other PII.

International, federal and state laws and regulations require appropriate protection of PII that is not publicly available. These regulations apply to PII stored or transmitted via any type of media: electronic, paper, microfiche, and even verbal communication.

- General Data Protection Regulation - regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

The Center for the Translation of Rehabilitation Engineering Advances and Technology

TREAT is part of the National Institutes of Health (NIH) Medical Rehabilitation Research Resource Network (MR3). Funding is provided by the National Center for Medical Rehabilitation Research (NCMRR) in the Eunice Kennedy Shriver National Institute of Child Health & Human Development (NICHD) through awards R24HD065703 and P2CHD086841.

10 Water Street, Suite 410
Lebanon, NH 03766
T: (603) 448-2367
F: (603) 448-0380
info@treatcenter.org

PII does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Data Storage

Properly storing and protecting the privacy of users' data could save you thousands of dollars in legal fees, if not your business. Prior to data collection, you will decide on storage infrastructure. This decision will factor in the prior mentioned sensitivity of PHI and PII. Other factors to consider involve cost and potential growth of both the database and your company.

Storage Considerations

- Location: Will you use a local server or web-based/cloud server?
- Scaling: The storage solution needs to be scalable based on expected growth (i.e., will the amount of data grow substantially?)
- Cost: Do you have a local server and expect data to come in slowly? If so, perhaps you can start with a local system to save money.
- Overhead Personnel: If you go with a local server, IT will be needed to support these databases and servers. This may incur additional cost.
- Access:
  - A firewall network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules
  - A Virtual Private Network (VPN) allows remote users to securely access corporate applications and other resources
  - Ports allow for connection to external devices to store data
  - Cloud storage is computer data storage where the data is stored and accessed in logical pools. More information regarding logical/storage pools can be found here.

Transferring

Some devices require data to be transferred from the device to another platform (i.e., local computer, handheld device) for viewing/storage.

- Medical Device Data Systems are devices intended to transfer store, convert, and/or display medical device data without controlling or altering the functions or parameters of any connected medical devices.
- Federal Communications Commission (FCC) requires all Radio Frequency devices to be approved prior to being marketed.
- Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. FDA requires that relevant cybersecurity risks are effectively mitigated to be in compliance with 21 CFR 820 Design Controls.

  References for cybersecurity:

  National Institute of Standards and Technology (NIST) Cybersecurity Framework

  FDA Guidance on Cybersecurity in Medical Devices

  IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices

  UL 2900 Cybersecurity for Network-Connectable Products

TREAT is part of the National Institutes of Health (NIH) Medical Rehabilitation Research Resource Network (MR3). Funding is provided by the National Center for Medical Rehabilitation Research (NCMRR) in the Eunice Kennedy Shriver National Institute of Child Health & Human Development (NICHD) through awards R24HD065703 and P2CHD086841.

10 Water Street, Suite 410
Lebanon, NH 03766
T: (603) 448-2367
F: (603) 448-0380
info@treatcenter.org

Summary and Other Considerations

Discussed below are topics to take into consideration when looking at the data you are collecting, storing, and transferring:

Privacy

Sensitive data may require de-identification (see previous sectios regarding sensitive types of data).

User Access Control

User Access Controls ensure that users of the system holding the data are only allowed to access the parts of that system they have permission to view or use. Patients should have the right to access medical device data about themselves.

Data Maintenance and Integrity

Data Maintenance are routines meant to help performance, free up disk space, check for data errors, check for hardware faults, update internal statistics, and others.

Data Integrity is the ongoing correction and verification of the data – the process of continual improvement and regular checks.

Data Interoperability

Data may have to be stored in a particular manner in order to be utilized or accessed by the user (Hospital data networks, Electronic Health Records, Health Level 7 (HL7))

Terms and Conditions

Consider the legal implications when collecting, storing, and using data collected from another party.

Generally, a “Terms and Conditions” agreement between both parties will cover the following topics:

- Data ownership
- Data lifespan
- Right to access data
- Right to use data
- Right to sell data

The Center for the Translation of Rehabilitation Engineering Advances and Technology

TREAT is part of the National Institutes of Health (NIH) Medical Rehabilitation Research Resource Network (MR3). Funding is provided by the National Center for Medical Rehabilitation Research (NCMRR) in the Eunice Kennedy Shriver National Institute of Child Health & Human Development (NICHD) through awards R24HD065703 and P2CHD086841.

10 Water Street, Suite 410
Lebanon, NH 03766
T: (603) 448-2367
F: (603) 448-0380
info@treatcenter.org