

Clinical trials Part II: Privacy, cybersecurity risks, and managing ePHI

The ongoing digitization of the drug and medical device industries continues, and, as a result, new considerations have come to the forefront for companies engaged in clinical trials. In [Part 1 of this series](#), we described a new set of clinical trial registration and result reporting requirements the FDA is imposing as of 2018. These new requirements follow on the heels of, and go hand in hand with, a number of guidance documents issued by the agency on data privacy protections and security breaches, which this Part II will address.

Ultimately, there is a significant level of risk to sponsors of clinical trials related to the security of the data they possess. Health care entities are a primary focus of cybersecurity hackers on a yearly basis, with recent studies showing that health care entities account for a vast majority of ransomware attacks. This translates into a risk to clinical trial sites, typically hospitals and doctors' offices, and, therefore, accounting for this risk in the trial design should be a primary focus.

Although the FDA has become increasingly focused on data protection and cybersecurity risk, it has yet to address these concerns directly in the context of clinical trials. Clinical trial sponsors and sites can learn from the documents that the FDA has created on the issue of data security and cybersecurity risks. These documents to date are generally directed at software manufacturers and developers where the software is used in a health care setting and will process patient data. In many instances, these guidance documents address themselves to the software, which drives and is used in medical devices. However, the overriding concern of the FDA's take on data privacy/security and cybersecurity risks, although not directly pointing to clinical trials, is very relevant to the trials, patient data security and the risk exposure to sites and sponsors.

Finally, the risks to clinical trial sponsors and trial locations includes the potential for significant fines from the Department of Health and Human Services (HHS). HIPAA violations can result in [fines in the millions of dollars](#).

In this blog post, Life Sciences Decoded will explore some of the cybersecurity concerns drug and device sponsors should keep in mind when operating clinical trials.

Controlling laws in the U.S.

There are several laws in the U.S. of which clinical trial sponsors must be aware. First, almost every state in the U.S. has passed a law dealing with what happens when a company encounters an incident where the security of an individual's personally identifiable information (PII) has been accessed by an unauthorized party. Although these laws vary greatly between states, only [one state has passed a law](#) laying out proactive requirements for data protection.

At the federal level, there are laws that apply to certain industries, but most important to sponsors of clinical trials is the Health Insurance Portability and Accountability Act, or HIPAA. When combined, HIPAA and its later amendment, HITECH, are the most comprehensive federal law addressing data privacy and cybersecurity in health care generally, including in the context of clinical trials. Generally, the HIPAA rules require that certain health-care-related entities have in place certain requirements for "protected health information" or "PHI." These rules are, generally:

1. **HIPAA Security Rule** - National standards for the protection of an individual's PHI. These requirements include extensive responsibilities for establishing policies and procedures to protect electronic PHI (or ePHI). This includes data encryption, backup and password policies.
2. **HIPAA Privacy Rule** - Controls the use and disclosure of an individual's PHI and sets standards for providing individuals with control over their PHI.
3. **Breach Notification Rule** - A set of standards for notifying impacted individuals, as well as the Department of Health and Human Services, when PHI is accessed by unauthorized individuals.

These regulatory requirements are detailed and supply the foundational considerations for how PHI is managed in terms of minimizing the amount of PHI collected and minimizing access to that PHI to only those individuals and entities that require it.

Managing PHI

Managing the “flow” of PHI between entities during clinical trials is particularly important when ePHI is involved as it can be “touched” by many different participants in the clinical trial process.

When a sponsor establishes the processes and procedures related to a clinical trial, managing ePHI must be a focused on the security of data being collected and protecting the data from breach in light of these many “touches.” Failure to manage and account for potential breaches in data security throughout the clinical trial process is likely to expose the sites and/or sponsor to liability.

The nature of clinical trials necessarily involves multiple parties, from the drug sponsor to trial locations and, potentially, contract research organizations (CROs) that manage the clinical trials for the sponsor. To simplify HIPAA compliance in the clinical trial context, a drug sponsor should determine which entities need access to ePHI and create study protocols to properly manage that access. This necessarily involves the proper identification of the role of the drug sponsor, CRO and trial sites under the HIPAA laws. There are two potential roles an entity can play:

- **Covered Entity:** A Covered Entity is the primary entity in charge of PHI. Covered Entities include health care providers (hospitals, doctors, nursing homes, pharmacies, etc), health plans (health insurance companies, HMOs, etc.), and health care clearing houses (entities that process PHI between nonstandard to standard formats).

- **Business Associate:** A business associate is an entity that performs certain functions or activities that involve PHI on behalf of a covered entity. This may include a claims administrator, a consultant that performs utilization reviews for a hospital, or an attorney who provides legal services to a health plan that necessitates access to PHI.

The responsibilities vary between the two, but generally both entities are required to have procedures and policies in place to protect ePHI according to the rules described above. However, the Covered Entity takes a primary role in compliance and managing ePHI access.

During a clinical trial, the study site will have the most extensive need to access PHI. On-site physicians and support staff must be able to properly treat patients and apply the study protocols in providing the study drug to those patients. Support staff will also be involved in managing PHI, collecting study data, collecting results and reporting those results to the CRO or sponsor. Study sites are also generally hospitals and physicians' offices that regularly handle PHI as a part of their practices. As a result, it is most likely that the study sites will be a covered entity under HIPAA.

HIPAA's requirements apply to PHI, that is, health information and information that can relate to an individual. PHI can be “de-identified” under HIPAA, meaning that the link between the health information and an identifiable person is broken. [HHS has published a set of standards](#) by which PHI can be de-identified through one of two approved methods:

1. A formal determination by a neutral third party qualified expert; or
2. The removal of certain special identifiers from the data and the lack of actual knowledge that the remaining information could be used, alone or with other available information, to identify individuals from the data in question.

Generally, CROs and sponsors do not need access to the actual individual identities (exceptions include protocol audits and special circumstances like adverse events). As a result, sponsors should employ processes to de-identify PHI to limit access to PHI to only those who must have it for the purposes of the study.

FDA and ePHI

The FDA has not addressed the protection of PHI in the same way as HIPAA, HITECH and the rules promulgated by HHS under those laws. Instead, the FDA has addressed the issue from the perspective of connected medical devices.

In the last several years, the FDA has created several rules that deal specifically with cybersecurity and the ability for device manufacturers, developers of [mobile medical apps](#) (“MMAs”), and operators of [Medical Device Data Systems](#) (“MDDSs”) to secure their systems against unauthorized access. These devices include:

- **Connected Medical Devices:** Generally, these are medical devices that have the capability to transfer data or otherwise be controlled through some other electronic device. These include networked devices, as well as devices with hardware ports.

- **Mobile Medical Apps:** MMAs are apps for a phone, tablet or other mobile computer that turn the mobile computer into a medical device, including those that have additional hardware accessories. Some of the most popular such devices are apps with accessories for testing and tracking blood glucose. MMAs also include EMR software.

- **Medical Device Data Systems:** MDDSs are software that passively handles, stores and makes available medical data, often for access and use by MMAs. An example is software that converts digital data from a sensor into a physical printout, without interpreting or manipulating the data in the process; or software that displays previously captured ECG data or X-ray imaging. MDDSs cannot be used in active patient monitoring.

The FDA has created a set of guidance documents that outline the agency's expectations for developers and users when it comes to ensuring that software and the device to which the software is associated with are secure. The most well-known and publicized issues are related to patient safety, such as a drug pump that could be compromised over an active network connection and be hacked to misdeliver drug doses. Such concerns are relevant to and can occur in a clinical trial setting. Clinical trial data not only includes patient information that is contained on a database but information related to the study drug itself. Protecting the integrity of trial data in a trial database is not only important to ensure study validity – study drug data may be impacted if patient data can be compromised and changed.

In addition, study databases contain more than just patient data. Confidential data such as drug formulations, dosing regimens, adverse event records and other sensitive information can be included in whole or in part in these study databases. Impaired or breached databases could lead to an inability to substantiate maximum tolerable dosing, efficacy and safety of the study drug. Therefore, it is critical for the developing drug sponsors to consider the security framework as outlined in the MMAs and MDDSs and understand that study databases must be designed to be secure, in addition to having a plan in place in the event of a security breach. Indeed the FDA has approached software and related systems as needing to be created and implemented with a "security by design" mentality.

FDA-regulated entities must be aware of the FDA's concerns and expectations surrounding cybersecurity, including the agency's reference to and application of the National Institute of Standards and Technology's (NIST's) [cybersecurity framework](#). This document [provides standards](#) which the FDA is increasingly applying to more and more industries it regulates. Drug and device sponsors should be aware of the framework's standards and how they apply to the sponsor's practices.

At Thompson Coburn, we have a team of attorneys practicing in Cybersecurity, FDA regulatory compliance and clinical trials. If you have any questions about the security of ePHI in your possession or how to secure ePHI collected and processed as part of a clinical trial, please feel free to contact our team.

[authorsTest](#)