Transmission Security Practices of Pharma Sponsors of Clinical Research

I. INTRODUCTION

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). In February 2003, the Department of Health and Human Services published a Final Rule adopting HIPAA standards for the security of electronic health information (the "Security Rule"). The Security Rule specifies a series of administrative, technical, and physical security procedures that covered entities must follow to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). Covered entities must comply with the regulations by April 20, 2005. Many clinical trial sites and physician-investigators are covered health care providers and, as such, will be required to comply with the Security Rule with respect to ePHI that is created, received, maintained, or transmitted in the course of clinical research sponsored by pharmaceutical companies.

Typically, in carrying out sales, marketing, and clinical research activities, pharma companies do not need to comply with the Security Rule because they are not covered entities. However, pharma companies have long recognized the need to protect the security of the PHI generated in clinical trials. One key aspect of the relationship between pharma companies and covered entities that act as trial sites is the transmission of ePHI from the covered entity to the sponsor. This paper has been prepared to provide covered entities with background on the transmission security practices of pharma sponsors relevant to a covered entity's HIPAA compliance obligations with respect to these transmissions and other technical safeguards of the Security Rule.

II. FDA REQUIREMENTS

Pharma companies must already comply with strict security standards contained in 21 CFR Part 11 for all electronic records created, modified, maintained, archived, retrieved, or transmitted pursuant to a requirement of the Food and Drug Administration (FDA) or submitted to FDA under the requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act. Electronic records generated as part of a clinical trial performed to support an NDA or ANDA fall under the scope of 21 CFR Part 11. The requirements of 21 CFR Part 11 are similar to many of the technical safeguards specified in the Security Rule, particularly with regard to the transmission of data. When adequately implemented in electronic data capture (EDC) and other computer systems, the transmission controls contained in 21 CFR Part 11 ensure that transmissions of ePHI from a covered entity (*i.e.*, trial site) to a pharma

sponsor will satisfy the HIPAA Security Rule's technical safeguards for transmission. In addition, other aspects of the technical safeguards enumerated in the HIPAA Security Rule are largely addressed through compliance with 21 CFR Part 11.

III. SECURITY PRACTICES RELEVANT TO TRANSMISSION OF ePHI

Clinical trial sites and investigators frequently transmit ePHI from clinical trials to pharma companies using EDC equipment and/or software applications provided by the sponsor, or using the site's own electronic medical record (EMR) systems. In doing so, as of April 20, 2005, they will be required by the Security Rule to "implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."[1] These measures include integrity controls and encryption where appropriate.[2]

Pharma companies are similarly required under 21 CFR Part 11 to "employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt."[3] Such procedures may include, where necessary, document encryption and use of digital signature standards. Compliance with this provision of 21 CFR Part 11 by a pharma sponsor provides that the integrity and confidentiality of ePHI will be guarded during the transmission from a HIPAA covered entity to the sponsor, in accordance with the requirements of the HIPAA Security Rule.

IV. SECURITY PRACTICES RELEVANT TO SPONSOR-PROVIDED EDC SOFTWARE AND HARDWARE

EDC software, and sometimes hardware such as personal digital assistants (PDAs) and laptops, may be provided by pharma sponsors to investigators and clinical trial participants for the purpose of recording, maintaining, and transmitting medical information relevant to the trial, including PHI. Under the Security Rule, a covered entity must comply with certain technical safeguards with respect to systems used to create, maintain, or transmit ePHI, regardless of whether these systems are provided by the covered entity or by the pharma sponsor.

When pharma sponsors purchase EDC software and hardware from vendors, they typically require the software and hardware to be compliant with the technical

---

[1] 45 CFR §164.12(e)(1)

[2] 45 CFR §164.12(e)(2)

[3] 21 CFR § 11.30

provisions of 21 CFR Part 11 (described below), which are similar in substance to many of the Security Rule's technical safeguards. Under 21 CFR Part 11, in order to safeguard electronic records generated in the course of clinical trials, pharma companies are required to:

- Implement procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, confidentiality of electronic records from the point of their creation to the point of their receipt, including, where appropriate, implementing encryption and digital signature standards;
- Limit system access to authorized individuals;
- Create complete, secure, reviewable, computer-generated time-stamped audit trails;
- Ensure that only authorized individuals can use the system, electronically sign a record, access the operation or system input or output device, alter a record, or perform the operation;
- Have the ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by FDA;
- Protect records to enable their accurate and ready retrieval through the records retention period; and
- Use device checks to determine the validity of the source of data input or operational instruction.[4]

Compliance with these requirements by a pharma sponsor serves to protect the confidentiality, integrity and availability of ePHI recorded, maintained, or transmitted using EDC software and hardware provided by the pharma sponsor.

V. OTHER SECURITY PRACTICES OF PHARMA COMPANIES

In addition to the above, pharma companies are required under 21 CFR Part 11 to implement a number of other safeguards to protect the security of electronic records generated during the course of clinical trials. Some of these are similar to certain administrative safeguards in the Security Rule, while others go beyond the safeguards and implementation standards contained in the Security Rule. These provisions of 21 CFR Part 11 include:

[4] 21 CFR §11.10 and 11.30

- Validation of computer systems to ensure accurate, reliable, and consistent intended performance, as well as the ability to detect invalid or altered records;

- Use of operational system checks to enforce the permitted sequencing of operational steps/events;

- Use of device checks to determine the validity of the source of data input or operational instruction;

- Ensuring that the persons who develop, maintain, or use electronic records and signature systems have the appropriate education, training, and experience to perform the assigned tasks;

- Establishment and adherence to written policies holding individuals accountable for actions taken under their electronic signatures;

- Use of appropriate controls over systems documentation, including controls over distribution and access to documentation of system operation and maintenance, and change control procedures;

- Use of at least two distinct identification components for electronic signatures;

- Establishment of specified controls over the use of electronic signatures;

- Verification of an individual's identity prior to establishing or sanctioning his/her electronic signature;

- Establishment of controls to ensure the uniqueness, and periodic revision of identification codes and passwords;

- Establishment of controls to de-authorize lost, stolen, missing, or compromised tokens, cards, *etc.*, bearing identification code or password information;

- Use of transaction safeguards to prevent unauthorized use of identification codes and passwords, and to detect and report any attempt of an unauthorized use to the system security unit and organizational management; and

- Conducting initial and periodic testing of tokens, cards, *etc.*, that bear or generate identification code or password information to ensure their proper functioning and that they have not been altered in an unauthorized manner.[5]

VI. CONCLUSION

Pharma sponsors understand the sensitive nature of PHI generated as part of a clinical trial and appreciate the importance of safeguarding the confidentiality, integrity, and availability of this information. Where 21 CFR Part 11 applies, pharma companies are required to implement strict security safeguards for electronic records and signatures, including transmission safeguards. These safeguards ensure that transmissions of ePHI from a covered entity to a pharma company will satisfy the transmission safeguards of the HIPAA Security Rule. Moreover, many of the other technical safeguards of the Security Rule are in large part addressed through compliance with 21 CFR Part 11. Compliance by pharma companies with the requirements of 21 CFR Part 11 with respect to ePHI generated in clinical research thus helps to protect the confidentiality, integrity, and availability of that information.

[5] 21 CFR §11.10, 11.100, 11.200, and 11.300.