How does PRC comply with HIPAA?

HIPAA stands for Health Insurance Portability and Accountability Act and, in part, establishes rules for maintaining the patient's privacy and security of their health information. HIPAA rules apply to "covered entities," which include health plans and health care clearing houses (such as billing services and community health information systems). These rules also apply to healthcare providers that transmit healthcare data in a way that is regulated by HIPAA (for example, healthcare providers transmitting patient records to PRC).

In accordance with HIPAA, hospitals are permitted to send patient records to PRC (or other research vendors) as long as it is for the purpose of improving the quality of care delivered to their patients. How hospitals send patient records to PRC has evolved as a result of HIPAA. Prior to HIPAA, hospitals could send their patient records to us in unsecure methods, such as regular email with no encryption or password on the files. In the current age of HIPAA, sending patient records via email is no longer allowed; instead, more secure methods are required. PRC offers clients two primary methods of transmitting patient records in a HIPAA-compliant fashion: 1) via our Secure File Transfer Protocol (SFTP)* server, or 2) via Securemail**.

PRC is mindful of how we conduct the research to ensure it is HIPAA compliant. The following are some of the precautions and protocols PRC follows:

- Access to EPHI (Electronic Protected Health Information) is restricted to only those PRC employees who have a need for it to complete their job function. For example, an interviewer only views the minimum information about the patient he or she is calling for on the screen. Once an interviewer has the correct person on the phone, the interviewer no longer sees that patient's information – just the questions to ask and the discharge date.

- When a PRC interviewer calls a household, she cannot mention information that reveals she knows someone in the household who was a patient. PRC has developed specific screening questions to comply with HIPAA:

    - When an interviewer calls, she introduces herself by name and simply says, "(Hospital Name) has asked us to conduct a survey about doctors, hospitals, and the services they provide."

    - Then she asks, "May I please speak with (Patient Name)?"

    - If the patient is under age 18, the interviewer speaks with the parent/guardian. First, however, the interviewer must establish that the parent/guardian she is talking to is aware of the visit; PRC has specific screeners developed for this purpose.

- All files sent from PRC to clients that contain Protected Health Information (PHI) (e.g. patient comments, action alerts, raw data files, etc.) are sent via SFTP or Securemail.

**PRC allows files to be transferred using any SFTP client (e.g., Internet Explorer, WS-FTP, etc.). These files must be encrypted with a password.*

***Securemail is a path through which PRC can transmit files to clients, and clients to us, that is encrypted both ways via Secure Sockets Layer (SSL) encryption.*