From: OC GCP Questions
To: [redacted]
Subject: Part 11 compliance/closed system vs. open system
Date: Monday, January 11, 2016 10:46:09 AM

Good morning –

As promised below is the response from the FDA's Office of Medical Policy (OMP) at FDA.

Kind regards,

Doreen M. Kezer, MSN
Senior Health Policy Analyst
Office of Good Clinical Practice
Office of the Commissioner, FDA

Hi Doreen, here is our cleared response:

Response:

The sponsor is ultimately responsible for assessing the validity, reliability, and integrity of any data used to support a marketing application for a medical product. When a sponsor, conducting trials under an IND, transfers responsibility to a CRO who assumes that responsibility, any obligation of the sponsor performed by the CRO must comply with the regulations. The CRO is subject to the same regulatory actions as the sponsor for failure to comply with the regulations (see 21 CFR 312.52). That said, in the situation you describe, the sponsor/CRO is responsible for the content of the electronic records. The investigator is responsible for the collection of the original source data and, by providing an official "sign-off" of each case report form, is certifying that the data submitted correctly reflects that original source data.

With widespread internet connectivity, the distinction between open and closed systems is not meaningful for the purposes of applying and implementing part 11 regulations. For example, the system you describe appears to be under the control of the CRO, and therefore could be considered a closed system. However, if the electronic records are stored on an online eTMF system, operated by the vendor (i.e., a third party), it could be considered to be an open system. In addition, we caution that, by permitting access to your system through use of the internet, the added security that results from restricting physical access is lost. Therefore, it would be prudent to implement additional security measures above and beyond those controls for closed systems, such as document encryption and use of appropriate digital signature standards to ensure record authenticity, integrity and confidentiality (see 21 CFR 11.30).

From: [redacted]
Sent: Monday, January 04, 2016 5:14 PM
To: OC GCP Questions
Subject: Part 11 compliance/closed system vs. open system

Hi. We work with a CRO that is considering a vendor's online data management/eTMF system. Authorized users of the system (pursuant to the CRO's subscription agreement with the vendor) could include not only employees of the CRO, but also investigators at study sites that have contracted with the CRO who would enter data from their sites into the system. The CRO would determine who can be "authorized users."

Under 21 CFR Part 11, a "closed system" is defined as "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system" and an "open system" is "an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the

system."

Who is "responsible for the content of the electronic records" that are entered by site personnel? That is, if an investigator uploads data into the system, is that investigator "responsible for the content of the electronic records", with the result that the system is an "open system" since the CRO, not the investigator, controls access? Or is the CRO deemed to be "responsible for the content of the electronic records" in this situation, with the result that the system is a "closed system"?

Thanks so much.

Best regards,

[redacted]