From: Beers Block, Patricia on behalf of OC GCP Questions
Sent: Wednesday, January 26, 2005 10:27 AM
To: [redacted]
Subject: RE: hard drive encryption

Dear [redacted],

I'm glad we got to discuss your inquiry in detail during our recent telephone conversation. As we discussed during this call, FDA does not stipulate how computerized systems need to be secured; only that the level and measures for ensuring system security be appropriate and reasonable based on the risks associated with the use of a system. For example, if data are to be transmitted from your server to, for example, the FDA for use in a market application, it would be reasonable and appropriate to encrypt data as a way to help to ensure that your data are protected throughout the transmission. Likewise, encryption of data on a hard drive might be useful if computer equipment is portable in nature (e.g., laptops store confidential information that needs to be protected).

Under 21 CFR 56.111(a)(7),in order to approve research involving human subjects, IRBs must determine that "where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data". Based on this regulation, IRBs (and FDA as well) consider the methods used to protect the privacy and confidentiality of data associated with the research. As you can see, this regulation does not explicitly identify methods one might use to protect data; this lack of explicit system requirements was very intentional for ensuring that the regulation was adaptable to any record-keeping practices/environments. As we have moved from a paper-based to an electronic-based record environment, we have seen the methods for ensuring limited access to data dramatically change. For example, in a paper environment, one might rely on SOPs (and their appropriate implementation) that describe ways to limit access to data contained on these records (and the records themselves) as appropriate measures for controlling access to confidential information. The electronic environment requires very different controls, such as the use of encrypted data for information that will be electronically transmitted from one system to another, or the use of limited access controls to the system itself through the use of individual user accounts that are password protected.

As we suggest in our Part 11 Scope and Application Guidance (see http://www.fda.gov/ohrms/dockets/98fr/5667fnl.pdf), I would recommend that your company document its reasons for selecting the methods/tools used to secure your computerized systems and protect records to enable their accurate and ready retrieval throughout the records retention period. Your company's decisions for using the selected methods should be based on a justified, risk-based assessment.

I hope this information is helpful to you.

Sincerely,

Patricia M. Beers Block
Special Assistant to the Director
Good Clinical Practice Programs
OSHC/Office of the Commissioner
301-827-3340

This communication does not constitute a written advisory opinion under 21 CFR 10.85, but rather is an informal communication under 21 CFR 10.85(k) which represents the best judgment of the employee providing it. This information does not necessarily represent the formal position of FDA, and does not bind or otherwise obligate or commit the agency to the views expressed.

-----Original Message-----
From: [redacted]
Sent: Monday, January 17, 2005 1:35 PM
To: patricia.beersblock@fda.hhs.gov
Cc: [redacted]
Subject: hard drive encryption

Dear Dr Beers-Block
I understand that a guidance for industry -"Computerized Systems Used in Clinical Trials" was published in September, 2004 and that you are the draft document contact for this document.
I would appreciate your assistance in helping us to determinie the level of system security required by the FDA, specifically whether encryption of the database on our server will be required.

We are fully encrypted from the site [redacted] all the way to the server. The only issue therefore is what would happen:
a) if a burgular breaks into the server room and removes the hard drive and tries to read it.
or
b) if a hacker breaks through our multiple security firewalls and accesses our hard drive (and reads it or changes it).

The chances for either of these events is probably one in a billion, given our security walls, but it is not impossible.

There is nothing in the FDA guidance which provides a clear picture of what to do, since they use words like "appropriate security" and "appropriate levels of encryption", but they never state that the encryption has to be on the hard drive.

Our feeling is that the FDA is concerned primarily about the safe private transmission of data and does not require more than routine security. Can you or someone else in the Division determine/confirm that our assessment is correct, and that encryption of our hard drive is not required.

Thank you for your assistance.

[redacted]