



Dear Hitachi Data Systems Customer,

It is our understanding that as a health plan, health care clearinghouse or a health care provider you may be a Covered Entity (“CE”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). As a CE, you may have certain obligations relating to the confidentiality of protected health information (“PHI”) that you are required to impose on your Business Associates (“BA”).

According to HIPAA, a BA is any person that (1) provides services to a CE, (2) is not part of a CE’s workforce, and (3) provides services that involve the use or disclosure of individually identifiable health information on behalf of a CE. Hitachi Data Systems Corporation (“HDS”), as a provider of back-end data storage products and services, is not a BA under HIPAA. HDS does not create, collect, compile or maintain PHI in any form. Nor does it receive PHI from a CE in a form that is readable by HDS. The mere fact that customer data is stored on equipment purchased from HDS does not define HDS as a BA under HIPAA because HDS’ services do not involve the receipt, much less the “use or disclosure of individually identifiable health information.” HIPAA specifically provides “health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information”. 45 CFR 164.514(a).

As explained below, the technical infrastructure of HDS is such that any information contained within the system is the equivalent of de-identified information, because HDS does not possess the encryption key or have any other means to derive identifiable information from whatever is maintained on the storage array. As a result, the transmission of data through the server does not constitute the disclosure of PHI to HDS. Therefore, a BA Agreement with HDS is not required.

As you know, recent HIPAA rules clarify that the loss of PHI does not trigger breach notification if such data has been encrypted according to standards set forth by the Department of Health and Human Services, because adequate encryption renders such data unusable for purposes of identifying individuals. *See* 45 C.F.R.

§ 164.402 (definition of unsecured PHI).^{1[1]}. In most instances, the data on the disk drives of HDS' products can be encrypted if the Encrypting Back End Controller ("EBED") is installed. HDS recommends the use of encryption to protect PHI and other HIPPA related information for the following reasons.

The EBED provides hardware-based strong encryption (AES-256) for data at rest and can be applied to some or all of the internal drives within the disk subsystem. For customers that require encryption of data at rest on external or virtualized storage or data in flight (e.g. data that is being replicated from one storage array to another), HDS can provide partner solutions that will encrypt that information. When encryption is enabled on the EBED or via a partner solution, data is stored as cipher text on individual hard disk drives. In the case where data is stored as cipher text and a disk drive was to either fail and be returned to HDS or fall out of positive control of the data owner, data is protected from unauthorized access. Additionally, HDS does not maintain or escrow the encryption keys for any of its customers, and therefore cannot decrypt customers' data.

You may also be aware of the preamble discussion of the final Privacy Rule, where the agency specifically noted that "A covered entity may transmit the portions of the transactions containing protected health information through a financial institution if the protected health information is encrypted so it can be read only by the intended recipient. In such cases no protected health information is disclosed and the financial institution is acting solely as a conduit for the individually identifiable data." 65 Fed. Reg. 82462, 82496 (December 28, 2000). Likewise, HDS is merely a conduit and not a recipient of individually identifiable data.

In circumstances where a customer does not utilize the encryption controller, data would not be accessible in human readable form to HDS. The data on a single drive is in cleartext format only, meaning that it contains sequences of ones and zeros. Additionally a single drive houses bits of information because the data is sprayed across several drives. Therefore, block data, such as a social security number or name, would not be available on a single drive.

In addition, a single drive that is removed from its set of drives is unusable because the information on the drive is destroyed when and if the drive is introduced to a new system. To explain it more fully, a single drive's residence in a system establishes it as a member of a contiguous set of drives, or "array group," and it is identified as a unique member of that series of drives. Because it is identified as such, once it is removed from its array, it cannot be used in another system until it is formatted to fit the array structure of the new system.

^{1[1]} Encryption standards are found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>

HDS takes data protection seriously and appreciates your concern that a drive being removed for maintenance may compromise the data contained on the drive. Consequently, we want to confirm, that a drive removed from its original system would not be usable in a second system until it is formatted to fit the established structure of the second system. The process of formatting the drive once it is introduced into the second system would destroy the data contained on the drive from the first system as the second system would have the data replaced with information to fit the second system's data structure.

HDS trusts that above explanation on how data on the drives appears to engineers will provide you with satisfactory assurance that your systems will be properly safeguarded. Thank you for your time and attention to this matter. Please contact the HDS Legal Department at 408-970-1000 with any questions or comments you may have.

Sincerely,

Hitachi Data Systems Corporation

ALL RIGHTS RESERVED. Copyright © 2010 Hitachi Data Systems Corporation
Hitachi is a registered trademark of Hitachi, Ltd. in the United States and other countries.