BEACHHEAD

Solutions Brief

"Is Your Solution HIPAA Compliant?"

Answers to this and the many other questions asked of us in light of the "Final" HITECH rule (9/23/2013)

Cam Roberson

September, 2013

Is encryption required for HIPAA compliancy?
Is your Beachhead's encryption HIPAA compliant?

These are among the questions I am asked ever more frequently as the federal government has (finally) published the "Final Rule" rule as it applies to the security of electronic patient health information (ePHI) mandated in the HITECH Act of 2009.

The answer to these questions is much more involved than a simple "yes" or "no." This isn't a cop-out. Really. Allow me to explain. But before I do, please let me qualify my explanation with the "I'm not a lawyer nor am I offering legal advice" preface. There are simply too many details specific to your environment, treatment and security circumstances that must be considered and there's no way I could know.

Strictly speaking, the U.S. Department of Health and Human Services which has oversight and enforcement jurisdiction over HIPAA HITECH compliance requires that ePHI is "Unusable, Unreadable, or Indecipherable to Unauthorized Individuals." The document cites two ways in which the requirement can be met. One method is encryption and the other method is destruction. Makes sense, right? - If the data is properly destroyed, it's certainly not readable or decipherable. Since Beachhead's products protect "data at rest," this discussion will focus on data as it resides on Windows and Mac PCs, Phones, Tablets and USB Storage (and not email or other "data in motion" requirements although email data at rest is protected). The website provides additional, specific information about these two methods through reference to other, additional documents. One of these documents, NIST publication 800-111, provides specificity to (data at rest) encryption and highlights the different methodologies that are available to you. Beachhead's encryption approach is described in this document. In short, encryption used properly can ensure that ePHI is unusable, unreadable, and indecipherable to unauthorized users. More on the specifics & detail of data destruction shortly.

HIPAA compliancy actually begins with a well-considered plan. It should be comprehensive, enforceable and it must be followed. Fundamentally it must include answer(s) as to how you are going to ensure that ePHI is unusable, unreadable, or indecipherable to unauthorized Individuals. Does your plan include encryption? It should. Is that the end of the plan? It should probably not be. There are many experts and attorneys in the field that can speak to the complete legal requirements for your specific situation. For a complete assessment and plan for your business I'm pleased to recommend Clearwater Compliance or Entegration. Under full disclosure Beachhead maintains relationships with both firms and there are certainly others who are well-suited to help you with this task.

A well-considered plan will describe where ePHI can be found under normal, expected business practices. It should also describe how data should be protected. And here's what might sound like and odd admission coming from an encryption solution provider: ePHI that is viewed on a PC might not need to be encrypted. Let me explain. If the ePHI was not physically located (stored) on that device and it could be guaranteed that it never find its way on that device and if the plan outlined the reasons for such, it's conceivable (perhaps reasonable) that the firm wouldn't have to encrypt their mobile device(s). Such would be the case if the data were accessible only through the cloud – viewable but not locally cached or stored. Now here's where it all gets tricky. One must always take circumstances beyond technological tools and measures when determining the overall efficacy of the security plan. Using employee policy– "We told employees not to download and store ePHI on a laptop" – is unlikely to garner sympathy or a reduction of the fines & penalties from the OCR if a breach of patient health information takes place.

All the encryption methodologies identified in NIST publication 800-111 are effective and entirely effective under ONE condition. Uh oh – you're probably smelling another caveat. And there is one. All encryption – including Beachhead's – is effective ONLY if authentication is secure. Once a device is authenticated, encrypted data is decrypted or placed in a decyrptable state and is therefore absolutely vulnerable to misuse. I suspect you're beginning to see the inadequacy of an encryption-only solution. Consider the following all-too-familiar circumstances. Passwords are often written down and sometimes stolen along with the hardware. Computers can be swiped with the power on. And what about when users are no longer authorized but still have the hardware and the credentials? Under any of these scenarios there is no encryption in the world, ours included, that will protect ePHI on a PC, USB device or Android tablet.

Remember a couple paragraphs ago I stopped short of getting into the topic of data destruction? It's time to discuss it again. It was the second methodology outlined as an approach to render ePHI unusable, unreadable etc. Employee behaviors and practices should be considered when assessing your data vulnerability. What if your employee copies and pastes ePHI into a document on an unencrypted tablet despite being told they should not do so? What happens if your contractor stores classified documents on a computer and then defects to Hong Kong (perhaps later to the Soviet Union) with the credentials to the device(s). If encryption is all you've got to protect that data, you're out of luck. Beachhead's products begin, but don't end with encryption. Rather, encryption is just a start. Our products give an organization the ability to deny access to data remotely, or to destroy compromised data entirely. Beachhead tools give our customers the unique ability to do either or BOTH. Other publications (for example NIST publication 800-88) recommend that if the data destruction approach is pursued, that it be done with "Agency approved and validated overwriting technologies/methods/tools." Beachhead employs a Department of Defense (DOD) 7x overwrite methodology.

Part of your *comprehensive* HIPAA/HITECH compliance plan

Beachhead's SimplySecure^{TM} Management System should be a consideration in your HIPAA/HITECH compliancy plans. There is more to compliance however than simply implementing a tool and calling it a day. Real thought needs to be given to where ePHI might reside - on what devices and with which employees. Your plan should account for contingencies and the behavior (careless or nefarious) of employees. The best security is one which does not rely on action or diligence of your employee. The more security involment necessary of employee the less productive they will be or the more active they will in working around or disabling the security.

Here are the check list items that need to be considered for your HIPAA/HITECH compliance plan.

- □ Develop a thorough plan that considers all instances of ePHI exposure (on what devices and with which employees)
- □ Select tool(s) that will enforce encryption of ePHI when stored on device (e.g. PCs, phones, USB storage)

□ Select tool(s) that will protect ePHI (e.g. access control or destruction) when password or authentication is breached (and encryption ineffective)

□ Select tool(s) where the employee is not depended upon for execution of security policy

□ Make sure the tools or services are easily managed

BEACHHEAD

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126

408.496.6936 x6866

Question, comments? Write Cam Roberson

croberson@beachheadsolutions.com