HIPAA Security Compliance | 13 Critical BitLocker® Settings to Help You on Your Path to Compliance

Abstract

With more than 600,000 laptops (and countless USB flash drives) stolen or lost each year, protecting your data with full disk encryption is both necessary and urgent. Healthcare organizations in particular can leverage full disk encryption to maintain HIPAA compliance, ace government spot audits, and avoid costly fines if data theft does happen. Learn the why and how of implementing free full disk encryption in Windows-based healthcare environments with this informative whitepaper.

Jason Iacono | Certified HIPAA Security Expert

Certified Ethical Hacker

HIPAA and You

It's been official for years. Healthcare organizations of all sizes must maintain compliance with the Federal Government's HIPAA-HITECH ruling, and the final Omnibus Rule. With each update to HIPAA, financial, civil, and criminal penalties have grown more teeth. And as the Office of Civil Rights starts beefing up audits against healthcare providers nationwide, now may be a good time to think about where your organization stands.

Today, noncompliant healthcare providers of all sizes risk potential fines of up to $2.5 million. That could mean you. The largest metropolitan hospital networks on down to the smallest of rural health clinics are directly responsible for securing their IT infrastructure and the protected health information it stores. The Department of Justice has confirmed that criminal penalties for a HIPAA violation are directly applicable to covered entities—including small independent physician practices, dental offices, and other healthcare organizations once considered "too small to appear on the radar". What, exactly, does this mean? And how does it affect you? Whether you're an owner of a medical practice, a practicing doctor, or even a regular employee, the HIPAA rule can find you criminally liable in the event of a data breach, under a vague term called "corporate criminal liability." The truth is, you hold a personal stake in the security and confidentiality of patient data.

> Properly implemented full disk encryption is one of the biggest "bangs for your buck" out there.

There are many provisions and requirements of HIPAA-HITECH. The entire law contains 22 standards which all covered entities (CEs) and business associates (BAs) must in some form implement, validate, and document. This paper will focus on just one piece, or implementation specification. In the following pages, we'll shed a light on the Encryption and Decryption Implementation 164.312(a)(2)(iv), under HIPAA's Technical Safeguard Requirements.

Why are we focusing on such a small part of HIPAA's overall requirements, and not talking about all of them? Among the 22 HIPAA Security Standards your business must navigate, encryption of protected health information is one of the easiest and cheapest investments you can make. Full disk encryption gives you maximum protection of data at rest, and even protection against breach penalties with Safe Harbor, which we'll talk about ahead. And while HIPAA does not specifically require full disk encryption, consider it insurance you cannot afford to ignore.

The Case for Encryption

According to the FBI, from 2005 to 2008, reports of stolen laptops jumped from 73,000 to more than 100,000 – in US airports alone. The Computer Security Institute's 2008 Computer Crime & Security Survey found IT breaches cost companies an average of almost $300,000 a year. The Institute also estimated that robberies cost average major corporations 640 laptops and 1,985 USB memory sticks.

Also consider:

- In a 2010 study, 46% of lost laptops contained confidential data, only 30% of those systems were encrypted, and only 10% had other anti-theft technologies. i
- The average value of a lost laptop is $49,246. The data breach costs represent 80% of the total cost of a loss. Encryption on average can reduce the cost of a lost laptop by more than $20,000. i
- 94% of healthcare organizations suffered at least one data breach during the past two years; and 45% of organizations experienced more than five data breaches during this same period. Based on the experience of 80 participating healthcare organizations, data breaches could be costing the U.S. healthcare industry an average of $7 billion annually. ii
- For every HIPAA data breach penalty involving a lost laptop or hard drive, Office of Civil Rights Director (OCR) Leon Rodriguez says that the penalty would have been avoided if the data had been encrypted. iii

Now ask yourself:

What if you could avoid risks like these with a single piece of technology offered natively, for free, with all Windows-based operating systems starting from Server 2008/Vista and beyond?

Today, noncompliant healthcare providers of all sizes risk potential fines of up to $2.5 million.

If you're running a Windows IT environment of at least Server 2008, (preferably 2012 R2) you can implement HIPAA's Encryption and Decryption specification with little to no cost. BitLocker, included in all recent Microsoft operating systems, allows you to encrypt and decrypt your data at rest – including OS hard drives, fixed data drives, and removable storage devices. If your healthcare environment is in an Active Directory domain environment (recommended for HIPAA compliance as a whole) you can deploy BitLocker settings to all the PCs and laptops in your business automatically.

How can full disk encryption help your organization? Principally, two ways:

1. Encryption can help you pass surprise government spot audits
2. With encryption, you can use Safe Harbor in the event of data breaches or thefts

Encrypting protected health information wherever it sits – on desktops, laptops, USB thumb drives, or file servers – and documenting it, will earn you high marks in the event OCR picks your organization for a surprise spot audit. Period. End of story. In this case, you absolutely want to be the teacher's pet.

Another way full disk encryption helps protect healthcare providers? By protecting them from a data breach itself. It may seem obvious, but data breaches do happen. It isn't always a result of a malicious attack from the outside. People lose hard drives and thumb drives all the time. Plenty of the most high profile data breaches have involved carelessness and nothing more. Someone simply lost a laptop or thumb drive. But that can cause huge problems if the data is human readable.

The HIPAA-HITECH ruling says it best: "Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information–that is, the information is not considered 'unsecured' in such cases. " If you're using strong encryption like AES on data at rest (which BitLocker provides), a loss or theft presents no risk to the data. The AES cypher is considered computationally unbreakable, therefore you would not need to notify authorities, file an official breach report, or contact the local media.

Encrypting data at rest is one of the cheapest ways to protect yourself against a government spot audit, or civil/criminal penalties in the event a breach does happen.

Let's examine two scenarios:

Company A discovers one of its laptops was either lost or stolen from baggage claim after a conference. Not an unusual event. The laptop had 13,000 patient records on it. Thankfully, Company A used BitLocker to encrypt the laptop's hard drives. After consulting with legal counsel, Company A decides to document the lost laptop internally. However, it does not need to notify regulatory authorities, or local media about a breach. This is because the information was encrypted, and not considered "unsecured." This is known as Safe Harbor. Company A is only out the cost of the laptop, and some additional time spent buying a new one. No lengthy reports, no government oversight pressure, no loss of reputation.

Company B also loses a laptop from baggage claim. Similar to Company A, this laptop had about 10,000 patient records stored on it. Unfortunately, Company B never bothered to encrypt the laptop's hard drives. They must report the 10,000 breached records to the Office of Civil Rights. To make matters worse, Company B also has to notify local media. After a lengthy investigation and media circus, the government fines Company B $6.3 million. The media reports on the data breach reach national news. Less than a month after the laptop disappeared from baggage claim, Company B is on the verge of bankruptcy. The constant barrage of media reports has painted an ugly picture of Company B. New patients have stopped coming, and existing patients have moved to other providers. After 8 months, the practice is forced to shut down.

Remember, as a healthcare provider, covered entity, or business associate, you are never "done" with HIPAA. Consider HIPAA to be a living, breathing organic process. You must remain focused on it throughout the year.

If you're using strong encryption like AES on data at rest (which BitLocker provides), a loss or theft presents no risk to the data.

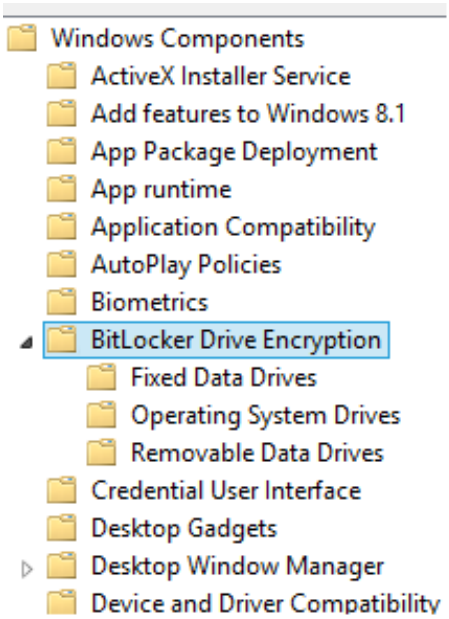
Accessing BitLocker Settings

Getting to the BitLocker configuration settings page is straightforward.

1. First, open a Windows command prompt or Powershell window.
2. Type *gpedit.msc* and hit Enter. The Local Group Policy Editor window opens, and from here, you can configure local BitLocker settings.
3. Under the Local Computer Policy tab, expand Administrative Templates.
4. Expand Windows Components.
5. Finally, click BitLocker Drive Encryption.

You are now ready to begin encrypting all protected health information at rest.

Industry best-practices recommend that you deploy BitLocker settings via Group Policy so you can roll out BitLocker to all computers within your organization at once. Group Policy in a Microsoft Active Directory domain environment is better for security, and for the IT team's workload. But, Active Directory and Group Policy is an entire topic unto itself. So for our purposes, using the Local Group Policy Editor will be fine for demonstrating the amount of control you have with this technology.



There is a lot to take in when configuring BitLocker in your environment. At first glance, it may even overwhelm you. With a dizzying array of configuration options – some that apply to your environment, and some that won't – setting everything up right can seem daunting. BitLocker offers some settings that are particularly important for rock solid disk encryption. The remainder of this paper examines 13 critical BitLocker settings to help on your path to HIPAA compliance.

Microsoft has divided BitLocker settings into three categories based on the type of hard drive you're going to encrypt – OS drives, fixed data drives, and removable media drives (like USB keys).

Just remember, don't implement everything on this checklist without first understanding the settings you plan on deploying and how they will interact in your own organization.

BitLocker Drive Encryption Main Settings

✓ | *Choose drive encryption method and cipher strength* |

HIPAA's Encryption and Decryption Specification does not detail a type or strength of encryption to apply. Overall, the law is vendor-agnostic and at times, technically vague. BitLocker, which uses the AES cypher to encrypt data, is a solid rung on the climb to HIPAA compliance.

The AES cypher is unbreakable today, and there exist no practical ways to crack it. Windows offers both AES 128-bit and 256-bit encryption key lengths. Both provide more than enough protection to meet requirements. But many encryption algorithms, once considered unbreakable, become weaker over time. If there is ever a crack in AES that reduces the time or resources required to break it, a bigger key gives you a better chance of staying secure. The longer the key, the higher the effective security.

✓ | *Prevent memory overwrite on restart* |

Certain BitLocker "secrets", information used to decrypt and encrypt the drive, are temporarily stored in volatile memory. It may be possible for a determined attacker to recover these secrets if they have physical access to the system. Enabling this setting ensures that the secrets are securely wiped from memory when shutting down or restarting the machine.

Although the chances of recovering BitLocker secrets out of memory are low, enabling this setting should cause only a slightly longer reboot and shutdown time. Therefore, it's recommended that you enable this setting for extra protection of your protected health information.

Fixed Data Drive Settings

✓ | *Deny write access to fixed data drives not protected by BitLocker* |

This setting provides an additional layer of hardening. It requires that all fixed data drives installed be BitLocker protected. As a best practice for HIPAA and data security at large, you should encrypt all hard drives. Denying write access to non-BitLocker-protected devices is one of the strongest defenses you can build on your path to HIPAA compliance.

This setting prevents users from installing external hard drives and then inadvertently or even purposely copying protected health information. This setting is an effective way to prevent data exfiltration.

✓ | *Configure use of passwords for fixed data drives* |

Require a password to access fixed data drives that may contain protected health information. For HIPAA compliance, require password complexity, and set the minimum password length to at least 8 characters, or preferably at least 10 characters. Requiring a longer and more complex password can help mitigate password guessing attacks.

✓ | *Choose how BitLocker-protected fixed drives can be recovered* |

If you lose access to BitLocker protected media, you can configure several methods of recovery. For best practices in non-domain environments, require the use of a 256-bit recovery key, and disallow the 48-character recovery password method. Users tend to keep these passwords written down on slips of paper, and that's something you must avoid for HIPAA compliance.

If you opt for recovery keys, keep these recovery keys under lock and key, preferably offsite. Storing the recovery keys in Active Directory, if applicable to you, offers the strongest form of data protection for recovery keys.

Operating System Drive Settings

✓ | *Require additional authentication at startup* |

If your computer hardware does not have a compatible TPM chip, you'll need to configure an alternate method to unlock the drive, like a USB key or a PIN. Consider requiring the use of multiple authentication methods. You could require a TPM, USB startup key, and a PIN, for instance. This may be overkill for a receptionist's desktop, but perhaps vital for a file server or backup server. Know your environment, and plan accordingly.

✓ | *Allow enhanced PINs for startup* |

Enhanced startup PINs permit the use of characters including uppercase and lowercase letters, symbols, numbers, and spaces. Consider enabling this setting if you are requiring or allowing a startup PIN as an authentication method. Requiring the use of complex PINs can help mitigate PIN guessing attacks.

✓ | **Configure minimum PIN length for startup** |

The startup PIN must have a minimum length of 4 digits and can have a maximum length of 20 digits. Consider enabling this setting if you are requiring or allowing a startup PIN as an authentication method. It's recommended to set the minimum PIN length to at least 8 characters. This setting can also help mitigate PIN guessing attacks.

✓ | *Choose how BitLocker-protected operating system drives can be recovered* |

This setting is identical to the recovery methods used for fixed data drives. Again, for best practices and security, store the recovery keys and/or passwords in Active Directory. If you are not in a domain environment, require the use of a USB recovery key and disallow the use of a 48-character recovery password. Keep the recovery keys in a secure location, preferably offsite.

Removable Data Drives Settings

✓ | *Control use of BitLocker on removable drives* |

If you've decided to allow employees to use removable media in your organization, and you have good security policies and training in place, consider allowing this setting. Users may then encrypt removable drives themselves. This setting, in conjunction with a strong policy and a centralized process for obtaining, using, and accounting for all removable media, can cut down on help desk calls by allowing the users to encrypt the drives for BitLocker themselves.

✓ | *Deny write access to removable drives not protected by BitLocker* |

This setting is identical to the one under the Fixed Data Drive Settings. You must develop a method to account and control for removable media. You may be hit by millions of dollars in HIPAA fines if protected health information lands on a USB thumb drive.

This setting prevents users from installing USB hard drives and then inadvertently or even purposely copying protected health information. This setting paired with the previous setting is a cost effective way to implement a denial-all policy towards removable media. For instance, disabling the Control use of BitLocker on removable drives setting will prevent users from encrypting USB keys with BitLocker. Also enabling this setting effectively prevents any removable media from being writeable.

✓ | *Configure use of passwords for removable data drives* |

Require a password to access fixed data drives that may contain protected health information. For HIPAA compliance, require password complexity, and set the minimum password length to at least 8 characters, or preferably at least 10 characters. Requiring a longer and more complex password can help mitigate password guessing attacks.

✓ | *Choose how BitLocker-protected removable drives can be recovered* |

For best practices and security, store the recovery keys and/or passwords in Active Directory. If you are not in a domain environment, require the use of a USB recovery key and disallow the use of a 48-character recovery password. Keep the recovery keys in a secure location, preferably offsite.

In Review

HIPAA requires a lot of security controls. Full disk encryption in particular is a no-brainer and can save you millions in potential fines. BitLocker is one of the cheapest ways to protect yourself against a government spot audit or penalties in the event a breach does happen. If you are running a Windows environment of at least Server 2008 (preferably 2012 R2) you can easily implement HIPAA's Encryption and Decryption specification at little to no cost.

Do not make the mistake in thinking an 'addressable' implementation means it's optional. It does not! All covered entities, including small providers, must determine whether "Encryption and Decryption" is reasonable and appropriate for their environment in accordance with Section 164.312(a)(1) of the Security Rule. And if you determine that encrypting protected health information is not appropriate, you'd better have a defensible, documented reason why that is.

While the HIPAA Rule does not specifically require full disk encryption, you should do it anyway. BitLocker, a free full disk encryption suite offered in many Windows operating systems since Server 2008/Vista, offers a cost effective way to encrypt all at-rest health information and protect you from the perils of information theft or loss.

Jason Iacono

Certified | CHSE | CEH | Security+ |

I am an experienced IT Professional passionate about helping businesses protect their digital assets from misuse or attack. I've supported organizations of all sizes, from Fortune 500 clients to small businesses, and can articulate technology needs to both implementers and decision makers. I've supported and built customer-first relationships with medical offices, law firms, churches, nonprofits, multinationals, banks, brokerages, and telecoms.

Citations

i The Billion Dollar Lost Laptop Study, Ponemon Institute and Intel Corp., 2010

ii Third Annual Benchmark Study on Patient Privacy & Data Security, *Ponemon Institute and ID Experts, December 2012*

iii *http://www.hhs.gov/news/press/2013pres/01/20130102a.html*