

Full Disk Encryption Versus Policy-Based Encryption

Some Considerations When Using Software To Secure Hospital Data On Laptops, Smartphones And USB Thumbdrives.

Data Breach legislation has provided a new and much-needed framework for hospitals and healthcare providers who seek to protect patient information. No longer does a provider have to figure out what is “reasonable and appropriate” to protect data, or to decide what to do when someone in your organization loses sensitive data, because everything is spelled out in the legislation.

The new laws tell you how to protect data – encryption; what data to protect - personally identifiable information belonging to the company or its patients; what to tell, whom to tell and how to tell them if data is lost – the person whose data is lost; and how to avoid having to conduct such a notification in the first place – provide an audit that shows that the device on which the data resided was protected by encryption.

This list of rules for data protection looks simple at first glance—just encrypt everything including applications, data files, program files, operating systems, even empty space just in case. With this level of encryption, if any computer or portable storage device is lost, you can justly claim there is no reasonable belief that unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The “encrypt everything” approach may appear to be simple but it imposes new and more complex procedures for your IT desktop operations, help desk, and end-users to institute. And it does not protect some of the very basic things it should protect against. Certainly, it protects data when it’s in the hands of the man in the striped shirt (the thief), but it completely fails to protect data when it’s in the hands of the man in the

white shirt (your employee). To illustrate how to protect all data handled by the organization, let’s take a brief step back and look at the most widely used technology today, Full Disk Encryption (FDE).

Many of your employees have access to regulated data for various reasons and you must consider too, the risk of an insider data breach to ensure that you are compliant with laws such as HIPAA.

Enter problem #1: FDE solutions do a good job at securing data against an external threat – that of the computer being lost or stolen, but do not have the capability to protect against the internal threat – data stolen by an “authorized” representative of your organization who has opportunistic access to data that they really shouldn’t be looking at. Consider what happens when a hospital executive or doctor sends his/her computer to be upgraded with a routine need such as adding more memory or a new version of software. The computer is turned over to your IT support staff (internal or outsourced) which then performs the upgrade, and logs in to the computer to make sure everything is working properly. With FDE and administration privileges, anyone can see every last piece of data on that computer!

To really comprehend what this means, you must understand more about how FDE works. FDE protects data stored on a hard disk by encrypting almost every sector on the drive – the exceptions are a few sectors at the very beginning of the drive that are necessary to boot the computer. The only way to gain access to anything on the drive is to provide a password referred to as Pre-boot Authentication (PBA) that unlocks the encryption keys and allows sectors to be decrypted.

Full Disk Encryption Versus Policy-Based Encryption

But more importantly, once the encryption key is open, ALL sectors may be viewed by any user. This “all or nothing” approach means any insider with administrator rights who logs in to the computer protected by FDE can still get to data he is not meant to see – salaries, patient addresses and social security numbers – all data that HIPAA requires you to protect! What many organizations fail to think about is that an insider data breach is still a data breach - and would be treated the same as an external data breach under the law –all legislation still applies, including the need to notify the patient if there is any fear the insider who saw the data might misuse it.

Enter problem #2: Pre-boot Authentication – users hate remembering passwords or entering them, but PBA forces them to do both. Worse yet, PBA requires IT to manage user accounts in a non-standard way that does not leverage existing Identity Management Systems. And once accounts are managed in two places, or passwords are prompted for in two places (pre-boot and at Windows login) password synchronization has to occur and IT has to get involved when synchronization doesn’t work. Simply looking for single sign-on to solve the problem does not always work. Account name changes, password synchronization and vulnerabilities that result from lowering standard practices to deal with these challenges seriously reduce the practical security gained from FDE.

Your end-users depend on their computer to get their job done, but things happen, computers fail and disks need to be repaired.

Enter problem #3: FDE scrambles everything on the drive; so standard disk recovery tools have an almost impossible task when a disk needs repair. All the standard structures that these tools expect to find such as directories, file allocation tables, file headers, etc., are unrecognizable with FDE because they are encrypted. The net result is that special tools are needed by your

IT staff to repair these systems.

Your end-users depend on you for normal maintenance of their computer to ensure they have the latest upgrades, patches, etc.

Enter problem #4: PBA also interrupts processes such as unattended patch management. If a computer has to be re-booted in the dead of night, it’ll just sit at the PBA prompt and the whole process stops. There are ways to get around this, but that typically requires suspending the PBA step, using some type of automated password entry. This in turn raises other security concerns such as what happens if the computer is stolen in this state.

These are just a few of the operational and security challenges in deploying FDE. But fortunately there are other alternatives that also ensure all sensitive data is always encrypted to meet the challenges you are facing with data breach legislation and the changing encryption landscape. Newer policy-based, data-centric security solutions enforce the protection of data stored on all types of vulnerable endpoints can work better to ensure that data is protected against multiple threats.

When responding to data breach legislation, there are four areas that should be considered to reduce the total cost of ownership, minimize risk. and ensure you really do meet compliance regulations:

1. To ensure all vulnerable endpoints are protected from external and insider threats of a data breach, consider a policy-based encryption solution that supports different types of keys for data privacy. On a shared computer, transparent to each user, each user’s data folders are encrypted with a unique key just for that person’s data. Data common to all users of the computer are encrypted with a common key to ensure all authorized users have access to the data they need to do their job.

Full Disk Encryption Versus Policy-Based Encryption

This flexibility in encryption policies, keys, and key management supports separation of duties so an IT administrator can repair, patch or upgrade a computer, but does not have access to any encrypted user data, eliminating the threat of an insider breach and a security gap left by other types of encryption solutions.

2. To minimize the impact on the end user consider a policy-based encryption solution that works within the standard Microsoft authentication framework. This approach provides immediate interoperability with any strong authentication system that is used with Microsoft Windows (Biometric, Smartcard, RSA, or whatever else is invented) and adds no custom integration requirements. There is no pre-boot authentication and the end user is not asked to create and remember an additional password, thus allowing him to fully realize a simple and secure login advantage. And there is no need for password synchronization and the issues surrounding storing passwords or accounts in two different systems. The bottom line is, IT's job is that much simpler.
3. To minimize the impact on desktop operations and the timely recovery from disk failures, policy-based encryption solutions do not create or modify any files outside of the standard Windows operating system. If a disk failure occurs, even if the entire operating system gets deleted, data recovery is possible using standard data recovery tools. In addition, computers can be repaired in the field and data recovered, without even needing to decrypt the data in most cases. This preserves the confidentiality of data even during difficult repair scenarios.

Policy-based encryption solutions support automatic key escrow that allows over-the phone help desk recovery of data, with no network or computer connectivity required. All encryption keys are centrally generated and securely stored au-

tomatically on the server. This automation frees end users from having to manually store encryption keys on a separate device or use some out-of-band process to store keys centrally. Recovery of encrypted data is an immediate option, from the second the first data bit is encrypted, until the computer is no longer rendered useful.

4. Newer policy-based encryption solutions provide a single, centralized administration console for the secure management and maintenance of security policies across all vulnerable endpoints, including desktops, laptops, Tablet PCs, smartphones, PDAs, and external media such as CD/DVD, USB external and Flash drives, and even iPods. This breadth of endpoint coverage eliminates the need to purchase multiple products, dramatically reduces the impact on personnel who would have to manage them.

In closing, healthcare concerns for patient privacy and the need to secure data on a range of new devices requires a deeper look at what both full disk encryption (FDE) and policy-based encryption offer. In particular, looking carefully at the operational complexities and vulnerabilities of legacy technologies such as FDE, as compared to newer policy-based approaches, will help you choose a solution that provides maximum security, while preserving ease of management and transparency for end users.