Portable Devices, Portable Data

In the first half of this year, we've seen a rise in incidents involving lost or stolen portable devices - laptops, USB drives, and backup tapes, hard drives, or servers. These devices can hold tens of thousands, and in the case of backup tapes even millions, of personal records.

All too often, they are unencrypted, and as a result the organization loses out on the safe harbors that most state data breach notification statutes or federal laws such as HIPAA provide for data that's encrypted. Under HIPAA, notification is not required when protected health information (PHI) has been rendered "unusable, unreadable, or indecipherable to unauthorized individuals," either through encryption meeting certain standards or by secure destruction of electronic media. Although state laws vary in their approach, typically notification is not required where the data has been encrypted, so long as the encryption key has not been compromised.

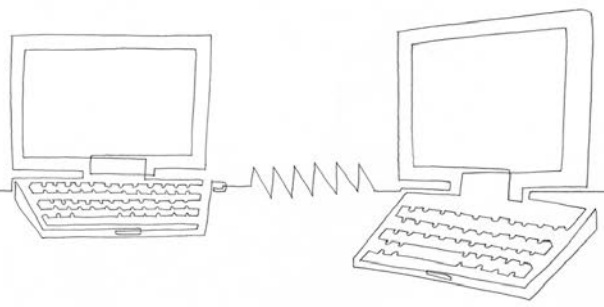
In addition to requiring notification, lost unencrypted data may result in significant fines and burdensome corrective action plans. In the healthcare sector, OCR put organizations on notice in late 2014 that it was taking this risk seriously when it settled two cases involving the loss of unencrypted laptops, requiring corrective action plans and payments totalling $1.9 million. In the financial sector, FINRA last year fined a broker-dealer $225,000 in a case involving an unencrypted laptop lost in a restroom. The findings focused on failures to update policies as technology changed over time and to make adequate investments in encryption.

Data loss from portable devices is a concern for other regulators, too. State attorneys general regard failure to encrypt as one of the most egregious deficiencies, according to Ted Kobus, head of the privacy and data protection practice at BakerHostetler. "Now, when state AGs learn of a lost or stolen unencrypted device, they also inquire about lost and stolen encrypted devices. If you have too many incidents of this type, the regulators often feel this further supports the view that the company doesn't have a good security culture because encryption may not always be implemented correctly or the encryption code may be improperly stored with the device." In addition to encrypting devices as discussed below, here are some steps you can take to help protect your organization:

- Inventory all devices on which data is stored and record which employee or department is responsible for each device. When an employee leaves the organization, ensure that devices are recovered and take appropriate steps to remove data before reissuing or disposing of the device.
- Don't forget about physical security. On your premises, portable devices should be secured like other valuable assets and should not be accessible by unauthorized persons such as visitors, vendors, or employees without a legitimate need for access.
- Understand how backups are stored, and if backups are encrypted, how encryption keys are secured.
- Make sure employees are trained on your policies for securing portable devices when traveling. Laptops and other equipment should never be left in a car, unattended, or in plain view.
- Contractually obligate any vendors with access to sensitive data to maintain physical and information security measures for the data, including any tapes or other physical means used to transfer data to or from them. Ensure that all former vendors return or destroy your records in accordance with your contract and policies.

Weighing the risks of significant fines and penalties if unencrypted data is breached, you should carefully evaluate the potential return on investment for the relatively modest costs of implementing encryption.

- Merely protecting a laptop with a password is often not enough. The security offered by passwords (including password-protected documents or spreadsheets) sometimes works like a lock on a file cabinet: if someone can break the lock, it's easy to read what's in the files.



- Full disk encryption (also known as whole disk encryption) must be enabled for data to be secure. Although full disk encryption also uses a password, the software generates a secure encryption key based on the password and then uses that key to encrypt all of the data on the disk. Full disk encryption makes the entire contents of a disk unreadable unless you have the key. It's like encrypting every file in the cabinet, so even if the lock is broken, the files can't be read.
- Do not store passwords with an encrypted device. Encryption provides a safe harbor only if the password is not compromised.
- Many servers, desktops, and laptops include encryption software by default (although it may not be enabled). If your operating system does not have built-in encryption, you can use third-party software to encrypt the full disk or to create special encrypted sections of the disk (volumes or partitions) in which to store sensitive data.
- Many of the most popular mobile device manufacturers, including Apple and Android, include an encryption feature in their operating systems. Again, it may not be enabled by default, so organizations must make sure it is in effect. Password length is critical; require users to pick a long password.
- If you buy laptops or USB drives without encryption already built-in, you can use special encryption software to create encrypted volumes within a normal file system, or encrypt the whole device. VeraCrypt, BitLocker and FileVault 2 can all be used to encrypt USB devices.

Additional resources available to BBR policyholders

Reducing your risk - email, disk, and device encryption

Sample physical and logical access security policy

HIPAA security policies and procedures templates

Password security

HHS.gov, Breach Notification Rule