HEALTHCARE

HIPAA AND USED DEVICES: DON'T MAKE THE $31K MISTAKE

The Center for Children's Digestive Health (CCDH) recently paid a $31,000 HIPAA settlement for failing to obtain a written business associate agreement (BAA) with one of their medical records storage vendors, FileFax. There was no actual data breach here, just a missing written agreement. Another recent case cost North Memorial Health Care of Minnesota $1.55 Million for failing to implement a BAA with a major contractor.

These examples are clear: Having a proper agreement in place with all vendors managing data or data-containing equipment is critical to prevent Health Insurance Portability and Accountability Act (HIPAA) penalties.

If you are working with or planning on working with a vendor to manage your retired computer equipment, treat them as a business associate. Even if you have an in-house data destruction policy, there may be instances where you want your vendor to perform data wiping or hard drive shredding services onsite for you. An agreement in place will also cover you if by chance a hard drive is missed in your internal process and it ends up at the vendor's facility (which we've seen firsthand happen at SEAM).

According Ponemon Institute, more than half of all healthcare vendors have experienced a data breach that exposed protected health information (PHI), with the average impact per organization costing $2.7 Million. If simply executing an agreement will help avoid a breach, there's no reason to not have one in place with all business associates, including electronics recycling or resale partners.

FOLLOW THESE STEPS TO MAKE SURE YOU ARE COVERED:

1. **Identify Current Business Associates.** According to HIPAA, a business associate is any organization or person working in association with or providing services to a covered entity who handles or discloses PHI or Personal Health Records (PHR). Examples could include consulting firms, equipment resellers, electronics recyclers, IT Asset Disposition companies, or any other organizations that have or could have access to PHI or PHR.

2. **Ensure Valid BAAs are In Place.** An agreement should clearly define the vendor's privacy and security obligations. The BAA should contain an indemnification provision that indemnifies you as the provider if the business associate causes a data breach through negligence, for example. The agreement must be documented for at least six years after the relationship is terminated as well.

3. **Compliant Data Destruction.** If a business associate is managing the destruction of your data, make sure they have compliant security policies in place for the final removal of electronic PHI and the final disposition of the equipment it's stored on. HIPAA's Privacy Rule does not spell out a particular disposal method, but does refer to NIST SP 800-88 Guidelines, which outlines disposal methods including clearing data and physically shredding data storage devices. Using an experienced partner will make this process easier with auditable documentation, industry knowledge and advice, more predictable costs, and peace of mind that you are in compliance with all current regulations.

4. **Track Data-Containing Assets**. To accurately account for all potential PHI under your control, make sure you know what you've got. You should be tracking every piece of equipment that contains sensitive data, from the largest server down to the smallest thumb drive. Don't forget devices like printers, copiers, fax machines and scanners that you don't typically associate with data storage. And remember, just because the equipment doesn't work doesn't mean its data can't be retrieved – make sure you or your disposition vendor can account for all devices, functioning and non-functioning, all the way through disposal.

5. **Maintain Written Policies and Procedures.** HIPAA requires covered entities to develop and maintain written policies and procedures for the privacy and security rule requirements. A provider that maintains these required written policies may be able to avoid penalties imposed for "willful neglect." Make sure everyone who touches the process understands the requirements. All employees, whether at your location or working off-site, must receive training on your disposal policies and procedures.

6. **Be Prepared to Prove your Process.** All of the effort you put into compliance will be wasted if you can't show documentation for the disposition of each piece of PHI containing equipment, usually by serial number. Make sure you receive a Certificate of Destruction for all equipment used to store or view patient information including smart phones, tablets, mobile devices or computers in case you are ever challenged in an audit. You may also want to witness the actual destruction process to ensure data is being properly destroyed.

"Having a proper agreement in place with all vendors managing data or data-containing equipment is critical to prevent Health Insurance Portability and Accountability Act (HIPAA) penalties"

"You must have an airtight IT Asset Disposition plan in place with a compliant BAA executed for any vendor managing your organization's electronic devices"

To avoid the risk of a costly data breach or a negative audit, you must have an airtight IT Asset Disposition plan in place with a compliant BAA executed for any vendor managing your organization's electronic devices.

SEAM recognizes the unique needs of IT managers in the healthcare community and we're here to help you implement compliant, secure and responsible procedures while gaining the most value back from your equipment. We provide on-location data destruction using our secure mobile shredding truck, as well as facility-based shredding and data sanitization services. We also provide a transparent chain-of-custody audit trail from the point of collection all the way through final disposition.

By making your data security our highest priority, we make HIPAA compliance seamless.

CONTACT US

605-274-7326 (SEAM)
705 E. 48TH ST. NORTH
SIOUX FALLS, SD 57104
WWW.SEAMSERVICES.COM

SEAM
SECURE ENTERPRISE ASSET MANAGEMENT