UNDERSTANDING HIPAA
DATA SECURITY REQUIREMENTS

With the move to electronic health records and a more mobile workforce, the healthcare industry has seen an explosion of data-bearing technology devices. Teeming with protected health information (PHI) and proprietary data, this equipment must be handled securely at all stages of use, including the very end. To protect patients and maintain compliance with HIPAA, healthcare organizations are required to take appropriate measures when upgrading, reusing or retiring devices:

Section 164.310(d) of the Health Insurance Portability and Accountability Act (HIPAA) requires Covered Entities and their Business Associates to implement policies and maintain detailed records for the final disposition and/or re-use of all devices containing electronic PHI.

COMPLIANCE CHECKLIST

- ☐ BUSINESS ASSOCIATE AGREEMENT (BAA)
- ☐ UPDATED SECURITY POLICY IN PLACE
- ☐ CHAIN OF CUSTODY DISPOSITION RECORDS
- ☐ VERIFIABLE, PROPER DESTRUCTION
- ☐ DUE DILIGENCE ON ALL VENDORS

WHAT'S THE RISK?

If proper steps are not taken to comply with HIPAA, the results can be devastating. Not only are organizations left vulnerable to the costly aftermath of a data breach, but also to the consequences of non-compliance in general. In 2016, Advocate Health Care agreed to pay $5.55m for its failure to accurately assess potential risks to its information technology systems and ensure that it and its business associates had adequate protections in place

Business Associate Agreement (BAA): Any vendor who handles computer devices or IT equipment that may contain PHI, must have a BAA in place. Even if data is destroyed in-house prior to leaving the facility, a BAA should still be executed to prevent accidental exposure from unsecured media slipping through.

Security Policy: A well-documented policy should be implemented and reviewed annually to identify all data storage devices likely to contain PHI and the most current sanitization and destruction standards. New devices and requirements are continually introduced and policies must reflect this. For instance, the current NIST 800-88 R1 guidelines have replaced the previously used Department of Defense 5220.22-M standard.

Disposition Records: Whether located in an online portal, electronic file or paper format, disposition records must be easily accessible. In case of an audit, evidence is required to ensure data storage devices were handled securely through the entire chain-of-custoy and all data was properly destroyed.

Proper Destruction: Methods of data destruction are required to render PHI unusable, unreadable or undecipherable. Currently recognized destruction standards are outlined in the NIST 800-88 Guidelines for Media Sanitization, Revision 1.

Due Diligence: Covered Entities are required to demonstrate they and their Business Associates have reasonable controls in place to prevent the loss of PHI and to properly respond in the event of a data breach. Certifications like R2:2013, e-stewards, ISO 14001, and OHSAS 18001 help healthcare organizations identify qualified vendors who implement proper security, environmental, health and safety measures when managing data-containing devices.

With audit-ready reporting and certified data destruction services, Secure Enterprise Asset Management, Inc. (SEAM) takes care of the compliance details for you. Contact us for a risk assessment for your healthcare organization or to learn more about how SEAM can help.

SEAM

SEAMSOLUTION.COM
605-274-SEAM (7326) | SIOUX FALLS, SD