How to Dispose of Electronic Devices and Media with PHI

The Department of Health & Human Services ("HHS") Office for Civil Rights has issued a cybersecurity newsletter outlining the steps that Covered Entities and Business Associates under the Health Insurance Portability and Accountability Act ("HIPAA") should take when disposing electronic devices and media that contain Protected Health Information ("PHI"). Examples include desktop and laptop computers, tablets, copiers, servers, smart phones, hard drives, USB drives as well as any storage device.

The guidance has been issued to help Covered Entities and Business Associates mitigate the risk of a potential breach and the associated costs and damage that would follow. HHS recommends taking electronic devices and media that contain PHI out of service before final disposition, a process referred to as "decommissioning", that would include ensuring:

- All devices are securely erased, and then either destroyed or recycled,
- An accurate inventory of decommissioned devices or those that are scheduled to be decommissioned has been taken, and
- Procedures to protect the privacy of PHI have been implemented when migrating to another system or before destroying the data.

Under HIPAA's Security Rule, Covered Entities and Business Associates must have policies and procedures regarding the protection of electronic PHI ("ePHI") including the disposal and re-use of devices containing ePHI. The guidance suggests the following:

- Determine and document the appropriate methods to dispose of hardware, software, and the data itself.
- Ensure that ePHI is properly destroyed and cannot be recreated.
- Ensure that ePHI previously stored on hardware or electronic media is securely removed such that it cannot be accessed and reused.
- Identify removable media and their use (tapes, CDs/DVDs, USB thumb drives).
- Ensure that ePHI is removed from reusable media before being used to record new information.

In this age of heightened awareness of electronic espionage and identity theft, it is imperative that businesses take all precautions to secure, not only HIPAA-governed PHI, but all personal and sensitive data that the organization may possess. The guidance contains links to additional materials regarding the proper and secure disposal of PHI.

More information about the HIPAA privacy and security rules may be found here.

HIPAA definitions:

Covered Entity: (i) a health plan which includes: health insurance companies, HMOs, company group health plans (medical, dental, vision, prescription drug, health FSAs, HRAs, etc.), and government health programs (Medicare and Medicaid), (ii) a health care clearinghouse (third-party billing services), or (iii) a health care provider who electronically transmits any health information in connection with transactions for which HHS has adopted standards.

Business Associate: A person or organization, other than a member of a Covered Entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity (i.e. claims processing, data analysis, utilization review, and billing) that involve the use or disclosure of individually identifiable health information.

Protected Health Information: "Individually identifiable health information" held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral and may include demographic data, that relates to the: (i) individual's past, present or future physical or mental health or condition, (ii) provision of health care to the individual, or (iii) past, present, or future payment for the provision of health care to the individual, and that identifies the individual or there is a reasonable basis to believe it can be used to identify the individual.

Breach: An impermissible use or disclosure that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.

For additional information about our services, please contact Kyle Frigon at 404-733-3256 or via email at: kfrigon@cherrybekaertbenefits.com.