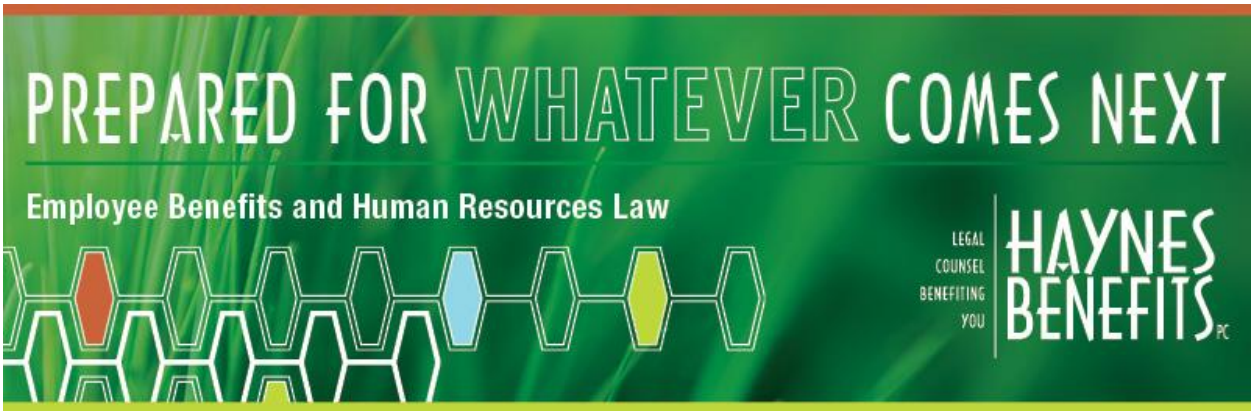


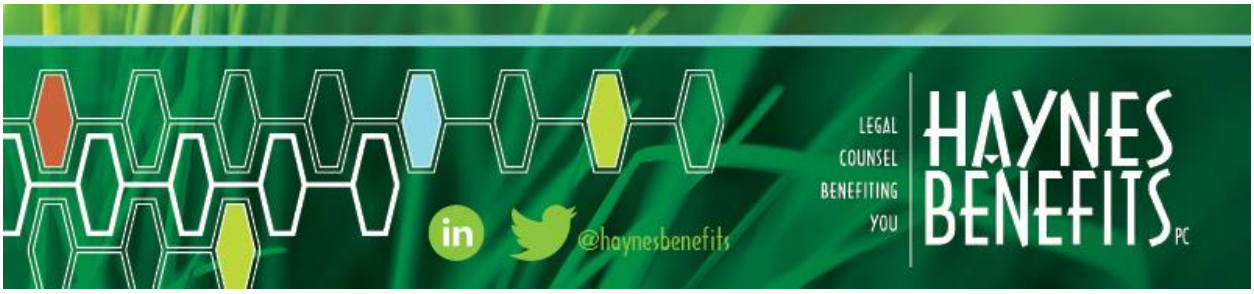
Who Knew? HIPAA Issues Lurking in Everyday Activities

Modern technology comes with many benefits that make our lives easier. However, technological benefits come with a host of risks that can affect covered entities and business associates. While it is common for organizations to ensure that devices such as notebook computers and smartphones have proper security protocols, those same companies may ignore other technological devices that pose significant HIPAA security threats that are not as obvious. These issues lurk and create traps for those not aware.

Here are a few examples of everyday technology and the HIPAA issues created, categorized from the most to least obvious (at least in my mind). Most of these issues have not yet arisen in OCR enforcement actions or agency guidance, and the issues therefore are presented from a practical or technological, rather than legal, analysis.

- **Cloud Computing.** Cloud computing solutions offer businesses a simpler way to store and share data. However, as with most technology, cloud computing is not without risk. Most cloud providers recognize this, as do most of their customers, so clouds do not present an unexpected issue.

  Nonetheless, recognizing the growing trend to use cloud computing for sharing and storing data, HHS released guidance in late 2016 regarding the necessary steps that covered entities and business associates should take when contracting with a cloud service provider. The guidance addresses the cloud service provider as a business associate, the necessity of a business associate contract, HIPAA obligations and administrative issues.



- **Wi-Fi.** We all use Wi-Fi from multiple locations on sometimes a daily basis. Public Wi-Fi networks are available in a variety of places from airports, hotels, coffee shops, restaurants and event spaces. When logging into a public domain users are at risk of having connections hacked and subsequently encountering a data breach.

  While many covered entities and business associates have considered the need for access controls (password protection, encryption, etc.) on the device itself, the need for secured connections (such as a VPN) should also be taken into account.

- **Bluetooth Capability.** Bluetooth is everywhere. We can connect our smartphones to our workstations, home computers, and notebook computers. Similar to Wi-Fi concerns, connecting devices via Bluetooth can raise the risk of hacking and security breach.

- **USB Flash Drives, Thumb Drives, External Hard Drives, etc.** Storing documents and data on USB flash drives, thumb drives, or external hard drives is an everyday occurrence. However, these devices are notoriously unprotected, and even more dangerous, frequently lost. Unless those drives are encrypted, the drives are not secure under the HIPAA rules.

  Of all the OCR enforcement actions and resolution agreements, there is no more prevalent offender than the loss or misplacement of a USB device. We can read about an employee who dropped a device out of his briefcase on the subway, one who left one in a public place, another who left a drive in his car that was stolen (both the car and the device inside), and other everyday human occurrences. The OCR sanctions have been severe, often with 7-digit penalties.

  What's missing in these discussions? In all the OCR resolutions we have seen, not one has evidence that the device or protected health information (PHI) therein was ever used or disclosed. For example, all evidence indicates the car was stolen for the car—not the USB drive inside.

- **Remote Work and Workers.** The workforce is changing, and one of the main changes is the trend to more remote work and workers. Office personnel now travel throughout the country but remain "in touch" with notebook computers and smartphones.

  From a covered entity or business associate standpoint, I recommend that all firms allow workers to access company information, especially PHI, only on company-owned notebook computers and smartphones. This way, the company can reclaim and/or purge the devices upon termination of employment, replacement of the device or, very importantly, loss of the device.

Companies should not allow employees to access this information on individually-owned notebook computers or smartphones. And companies should always have a remote worker policy that covers these issues as well as issues of establishment and maintenance of the remote workplace, often at the worker's residence.

- **Wearable Fitness Devices.** When an individual purchases a Fitbit or other similar wearable device directly, HIPAA does not apply because neither the manufacturer nor the individual is a covered entity or business associate. However, HIPAA may enter the picture when there is some sort of interaction between the device and a health plan, wellness program or other benefit plan. Now the device is provided by or offered by a covered entity, and the information is used or disclosed by a business associate.

  Further, the information in the wearable device may be transferred by Bluetooth or other system, stored in the cloud, and maintained by a business associate or other service provider. A breach of the data shared between these devices and a mobile or web-based application is possible in the event that the site is hacked.

  This begs the question—is the information PHI? What if it's just steps? Or sleep patterns? While there is no direct guidance, one can easily see that even steps are health information. If you know that John averages 12,100 steps per day, and Fred averages 4,300 steps, does that tell you something about each participant's health? Of course it does.

- **Rental Cars and USB Chargers.** When charging a smartphone or laptop through a traditional wall or cigarette lighter/charger in a vehicle, there is no risk of a HIPAA breach as data from the smartphone is not being transferred through the outlet or charger. However, many automobiles now have USB chargers instead of or in addition to the cigarette lighter/charger, and in most cases, that USB connects to the automobile's computer/entertainment system/hard drive. Depending on the settings in that system, all the email, texts, contacts or other information from the smartphone may automatically be copied to the hard drive in the car—now available to all future renters.

The lesson here? Danger lurks throughout our everyday activities. Be aware of the HIPAA issue, do a risk analysis, prepare solutions as best as possible for today's environment, and document your company's actions.

Dated: June 26, 2017
Written by: Andrew Ky Haynes