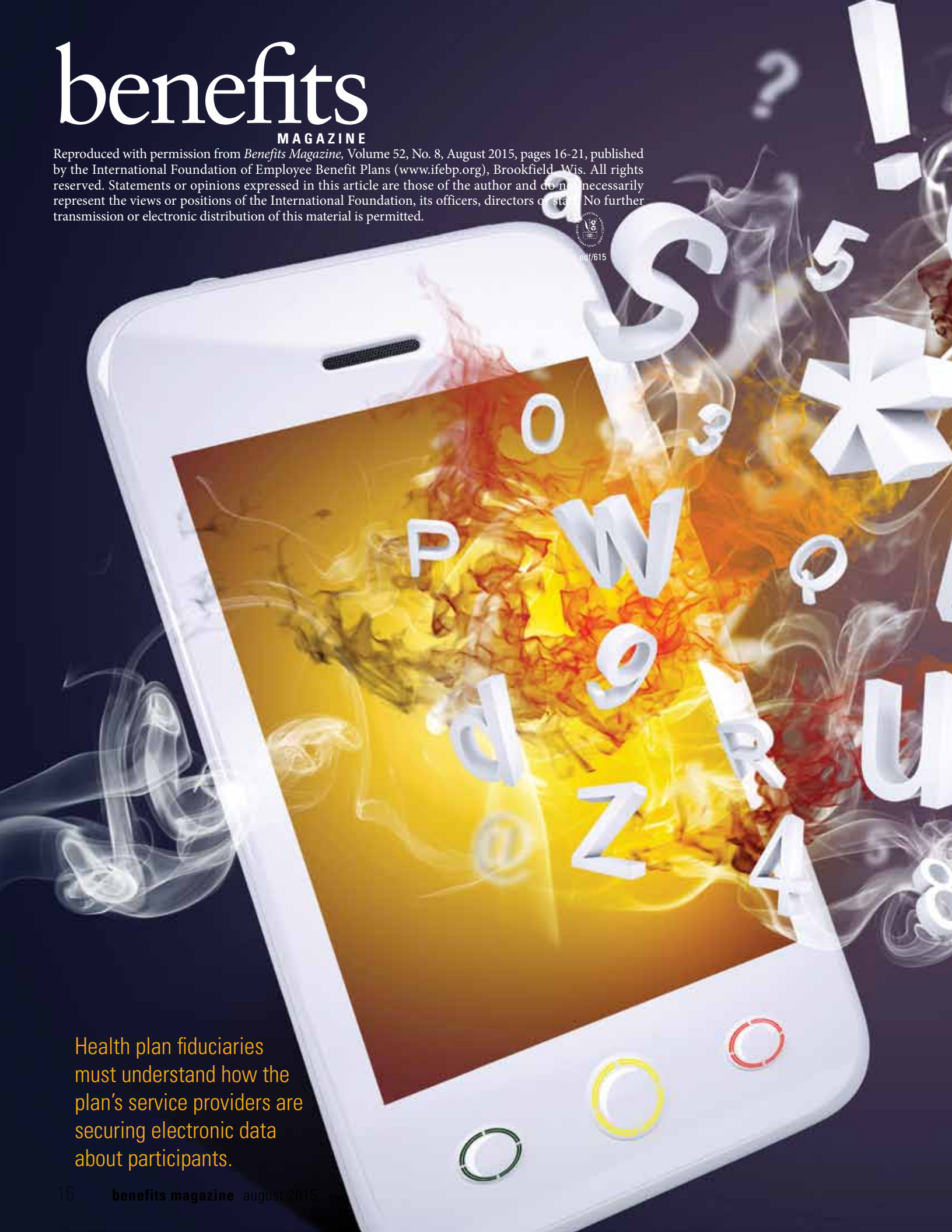
benefits
MAGAZINE



Health plan fiduciaries must understand how the plan's service providers are securing electronic data about participants.

What Fiduciaries Need to Ask Service Providers About Cybersecurity

by | **Wyatt J. Holliday, CEBS,** and **David J. Fournier**

Each passing year it is more difficult to be a health plan fiduciary. Fiduciaries must pay attention to a number of issues beyond the traditional concerns of the trust's financial returns and the resolution of claim appeals. This brave new world of potential potholes for the fiduciary includes all of the security issues related to the protection and security of the plan's data, whether stored on a server in the fund office or held by a national insurance company.

Fiduciaries of health plans subject to the Employee Retirement Income Security Act (ERISA) are held to a high standard; they must act "with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims." This is sometimes referred to as the *prudent fiduciary* standard—A fiduciary must act not only with the prudence of the average person, but with the care and skill of someone who regularly and knowledgeably conducts similar business.

Luckily, ERISA does not require that fiduciaries actually become electronic data security experts. They must, however, know enough to perform the proper due diligence on their chosen service providers. Securing a plan's electronic records is really a function of addressing three interrelated elements: managing the electronic data, securing the physical hardware storing the electronic data and managing the people who interact with that data.

There have been multiple high-profile data breaches in the benefits industry in the last 18 months. When some of the largest insurance companies in America struggle with the security and integrity of their electronic data, what is a fiduciary who sits on the board of trustees of a 3,000-life health plan supposed to do?[1]

Data Security and Management

When evaluating data security measures, the most basic concept fiduciaries need to understand and investigate is how each party manages the data for which it is responsible. Everyone knows that encrypting sensitive data is vital, but fiduciaries need to realize that not all encryption is equal. They need to ask questions and take steps to obtain a working knowledge of each service provider's data-handling and security policies.

When discussing encryption, there are two main data states with which fiduciaries need to be concerned—at rest and in flight.

Data is *at rest* when it is sitting in storage, waiting for someone to summon it up from the server on which it resides to read or manipulate it. Once a request is received by the server, the data is transmitted to the individual or program that initiated the request.

Any time data moves it is *in flight*. While the data is being manipulated by a user, it is considered in use. If an end user then retransmits that data—via e-mail, upload to cloud-based storage services or back to the server on which it is stored—the data is once more considered in flight.

Fiduciaries need to make certain that service providers have implemented steps to protect data both in flight and at rest. *Hard-disk encryption*—the encryption of an entire physical hard-disk storage drive—typically does not protect data in flight, nor do measures to protect data in flight necessarily protect data at rest. Each issue must be addressed independently.

Fiduciaries need to be satisfied that their service providers understand and take measures to protect sensitive data as it is transmitted—from the fiduciaries' network to third-party networks and vice versa. This can be accomplished by establishing and using encrypted connections and by implementing dedicated file encryption software.

Fiduciaries should also ask whether sensitive data is stored in an encrypted form, so that only authorized users/programs with the proper key may decrypt and access it. This question is especially

takeaways >>

- Fiduciaries must be sure that service providers are protecting data both in flight and at rest.
- Storing sensitive data in an encrypted form, so that only authorized users/programs with the proper key may decrypt and access it, is especially important when data is on a portable device.
- Data needs to be *deidentified*—temporarily disassociated from the person it concerns—to limit the potential impact of a data breach.
- To protect against fires, natural disasters and theft, fiduciaries should ascertain the providers have taken the proper physical security measures.
- Policies and procedures should be in place to reduce the chance that human error or criminal intent leads to a data breach.

relevant where data may be placed on a portable (i.e., easily lost or stolen) device. If a laptop containing participant data is stolen, for example, the difference between a security breach and no breach likely depends on whether the hard drive on that laptop was encrypted. If it was, the data probably is secure; if the data is stored unencrypted, the data probably is compromised.

In addition to encrypting at-rest data, processes to deidentify the data should also be utilized. *Deidentification* is a process by which certain data is temporarily disassociated with the individual to whom it belongs. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) enumerates the identifiers that must be removed from a record in order to successfully deidentify it, and fiduciaries need to ascertain whether the processes employed by providers meet those requirements. By making certain that data is encrypted and deidentified at rest, service providers can limit the potential impact of a data breach in the event that other security measures fail.

Physical Security

Data encryption helps protect against technical threats to data but is of limited use against nontechnical threats such as facility fires, natural disasters and theft. Fiduciaries need to ask service providers about the physical security measures that have been put in place to protect sensitive data. They should make inquiries into several areas.

First, fiduciaries should request information about the facility in which the data is located. Generally, fiduciaries should try to get a feel for just how tightly buttoned up (or not) a service provider's facility is—specifically:

- What security procedures have been implemented to keep unknown and unauthorized individuals away from sensitive areas?
- Is the facility fenced in?
- How many and what types of barriers stand between a potential assailant and access to the data?
- If electronic locks are used, are there procedures in place for deauthorizing lost or stolen keys?
- If physical keys are used, can the locks be rekeyed in short order?
- Is access to machines on which the data is stored limited to administrators only, or may any employee access them?

Physical security also includes the need to address document disposal practices. Fiduciaries need to ask whether protected data is ever reproduced in printed form and, if so, how it is stored or disposed of. Does the provider shred documents in-house, or is shredding outsourced to another company? If the provider hires someone to handle document shredding, are there procedures in place to prevent the shredding service from accessing the documents prior to their destruction?

It should be noted that printers can be repositories of sensitive data—If an unauthorized individual were to get hold of one, he or she might be able to retrieve previously printed protected data.

Another major physical security concern is the protection of portable computing hardware. Data breaches can start with lost or stolen laptops, tablets or smartphones. If laptops are used at workstations, are they secured such that unauthorized parties cannot remove them? If sensitive data is present on other portable devices such as phones, does the service provider use software that is able to track and remotely erase the data on those devices? Additionally, does the provider have established security guidelines for the use of those devices, such as requiring that phones and tablets be password-protected and encrypted?

Anyone who has ever had a computer die knows the importance of backing up files. Most service providers that handle data will have backup procedures established as part of their disaster recovery plan (which fiduciaries should also ask about). But where do the service providers store the backup tapes or disks? Fiduciaries should ask what security measures are taken with regard to any physical copies of their sensitive data. Copies should be stored in a secure location—preferably off site so that a facilitywide disaster does not wipe out

the backup data along with the original. Finally, fiduciaries should again determine if the backup data is stored in an encrypted state; these are physical objects that can be lost or stolen.

One final item that fiduciaries may want to investigate as they assess a provider's physical security measures is whether the service provider restricts the capacity of employees to save sensitive data to portable storage media such as blank DVDs, CDs or thumb drives. Employees at their workstations necessarily decrypt data to view and manipulate it. Service providers should take steps to ensure that the employees are not able to save that data to a thumb drive without prior permission to do so. There are different solutions for this problem, but the most common is physically disabling drives by either removing the necessary wires or physically preventing the use of the drive—for example, by filling USB ports with glue.

Personnel Management

Modern encryption is incredibly secure; if properly encrypted data falls into the wrong hands, it is effectively useless without the decryption key. And proper physical security policies regarding portable media, disposal and secured entry can go a long way in ensuring nonencrypted data is not accessible. However, all of the encryption and security protocols in the world cannot overcome the "human" factor. Computers do only what they are told; however, human beings often do the opposite of what they are told. That's why the third element of data security is personnel management. What policies and procedures are in place to reduce the chance that human error (or criminal intent) leads to a data breach?

Fiduciaries need to ask how their service providers manage access to sensitive data for their population of workers. Security training must take place on a regular basis and must address both the high-level information technology professionals and the nontechnology employees at large. Something as simple as the provider's password requirement is important. For example, most passwords are required to be "strengthened"—They must contain at least three of these four elements: an uppercase letter, a lowercase letter, a number and a special character. In theory, these requirements result in a password tremendously difficult to hack. In practice, employees use passwords such as their home address (123Street, for example). While that may both meet the security standard and be easy to remember, it is also very easily hacked—All it takes is a quick public records search, coupled with a list of employees compiled by a search of social media. Fiduciaries must remember that most hacks are not some person physically entering data into a log-in screen; instead, a computer program is employed to enter all possible combinations of likely data. Again, in the case of a stolen laptop, as above, the absence or presence of a strong password protocol can be the deciding factor in determining whether a data breach occurs.

Additionally, fiduciaries should ask about their service provider's internal audit protocols. How often does the provider review user access levels to ensure that each employee can access only the least amount of data necessary for his or her job? More importantly, how often are employee directories validated? When an employee is terminated, is there a written process to remove his or her user credentials? This is vitally important, as most networks have multiple access points—the main network log-in, but also web-based e-

<< bios

Wyatt J. Holliday, CEBS, is an associate in the tax and benefits/Taft-Hartley practice group in the Toledo, Ohio office of Shumaker, Loop & Kendrick, LLP. His practice is concentrated on employee benefits, executive compensation and multiemployer retirement and health and welfare plans. Holliday previously worked as a benefits analyst and project manager for a self-administered multiemployer funds office. He received his undergraduate degree from Denison University and his J.D. degree from the University of Toledo College of Law. Holliday can be reached at wholliday@slk-law.com.

David J. Fournier is an associate in the tax and benefits/Taft-Hartley practice group in the Toledo, Ohio office of Shumaker, Loop & Kendrick, LLP. He earned his J.D. degree from the University of Toledo College of Law and a B.A. degree in business administration and creative writing at Baldwin Wallace University. Fournier can be reached at dfournier@slk-law.com.

mail, multiple specific programs, legacy systems from acquisitions, etc. These multiple points of entry rarely are tied to only one log-in.

Finally, there is the pure "social" element of every workplace. Shelly from accounting is frustrated at having to route requests for information through claims, so she complains until she is given access to the claims system. Jason from sales squeaks loudly enough that someone from IT e-mails him a raw data dump of census information rather than the carefully redacted list of ages and ZIP codes he needs. Rather than following the (time-consuming) checklist after an employee is terminated, Gwen from IT—a ten-person department with enough work for 15 people—disables only the terminated employee's network access. Workers are expected to meet deadlines and hit productivity goals; they are reviewed and compensated based on how well they do those things. Fiduciaries must ask enough questions to ensure that their service providers place the same institutional emphasis on proper, ongoing training and management. Unless people follow them, the best electronic and physical security protocols in the world simply will not work.

Takeaway Questions for Fiduciaries to Ask Service Providers

Data Security and Management

- What are your policies about encrypting sensitive data?
- Is the data stored in an encrypted state?
- Is the data deidentified in a HIPAA-compliant process?
- Do you use file encryption software when data is transmitted?

Physical Security

- How secure is the facility that houses the data?
- What disaster recovery procedures are in place to protect and restore data?
- What policies and protections are in place for mobile computing platforms?
- If sensitive data is ever printed, how is it stored and disposed of?

Personnel Management

- What is your process for auditing your employees' access to sensitive data?
- Do you conduct security training? How often?
- How often do you scrub old employee credentials from the system?
- Do you have guidelines for making strong passwords, and how frequently do you require that they be changed?

Endnote

1. Fiduciaries should ask their consultant about cyberliability insurance. See Brian L. Smith and Matthew E. Jackson, "Need for Cyberliability Insurance Continues to Grow," *Benefits Magazine*, May 2015, p. 14.