Published on *The National Law Review* https://natlawreview.com

Is HIPAA in the Clouds?

Article By:

McBrayer, McGinnis, Leslie & Kirkland, PLLC

Virtual or “cloud” data storage is an increasingly popular method for storing data electronically in a safe and yet conveniently accessible manner that may also represent a cost savings over traditional onsite data storage options. Health care providers, including hospitals, pharmacies and physicians, have been slow to avail themselves of the benefits of “cloud computing” due in part to concerns about whether the cloud offers the rigorous privacy and security safeguards required for storing electronic protected health information (ePHI) under Federal and State privacy laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and implementing regulations.

Traditional Onsite Storage.

Health information privacy laws require covered health care providers and payors as “covered entities” to protect the confidentiality, integrity and availability of ePHI.[1] Traditionally, this has involved storing patient records and other PHI onsite, on systems controlled by the covered entity.

The benefit of onsite storage is that the covered entity can implement and enforce policies and procedures to control access and ensure confidentiality of the stored PHI, literally placing it under “lock and key.” The downside of onsite storage is that the PHI is housed in one location, vulnerable to power outages, fire, hurricanes and other natural disasters, and as the volume of PHI grows, maintaining enough onsite storage capacity may become costly. Additionally, such onsite storage may present significant obstacles for the covered entity when attempting to access PHI from other practice locations.

The Cloud Storage Commeth.

Cloud computing is similar in many ways to a data warehousing solution and generally means that data in the “cloud” is stored on a network of servers that provide storage capacity for a “virtual environment” managed by the cloud storage vendor. Data stored in the cloud is accessible anywhere there is an internet connection, and the cloud vendor typically maintains firewalls, backup and disaster recovery procedures, alternate power management and other mechanisms to significantly reduce any possibility of data loss. The cloud vendor also controls who has access to the data, where the data is physically located and how the data is segregated from other data on the shared server network.

The servers used for cloud storage may be distributed over a number of physical locations (including internationally) and the virtual environment is accessed, in a “public cloud”, by multiple clients of the cloud vendor that share space on the network of servers. The cloud vendor is responsible for ensuring careful segregation of each client’s data to prevent unauthorized access by one client to another client’s data, and for security purposes. The cloud storage model is more vulnerable to attacks than onsite storage as hackers may attempt to access the data from the internet and are incentivized to do so with a significant amount of data from multiple parties being stored on the shared server network. Along with firewalls, antivirus software and a number of other defensive tools available to cloud vendors, segregating client data reduces vulnerability to successful breach.

In this piece we focus on the “public” or “shared” cloud model, with multiple clients sharing space on the cloud server network. “Private” clouds are also available that offer dedicated cloud server space for a particular client.

---

1 45 C.F.R. § 164.306(a).

National Law Review, Volume II, Number 261

Source URL:https://natlawreview.com/article/hipaa-clouds