Can the healthcare sector find treatment for data privacy?

The healthcare sector has experienced great technological advancement over the years. Remember pagers? We've certainly come a long way. Clinical applications used today, such as electronic health records (EHR), mobile health (mHealth), computerised physician order entry (CPOE) and self-service applications, contribute to a more efficient medical workforce. However, as with any digital transformation project, increased security risks can be expected, especially with the rise of sensitive data collected.

Healthcare institutions collect a vast amount of data, including patient records, health card numbers and radiologic images. With the exponential growth of data, many are turning to the cloud for storage solutions. This, in turn, only amplifies data protection concerns.

Whether it be in adherence to HIPAA, CCPA, DPA or GDPR, healthcare institutions are responsible for protecting and securely storing patient health information (PHI) data. PHI data must be protected in transit and at rest. This can be challenging for large healthcare institutions when sharing data with remote employees, with other departments or with other institutions. Many lack a centralised management of systems and data, losing out on full visibility and control of data.

To ensure data privacy, there are five important suggestions to follow: (1) encrypt data in transit and at rest; (2) control the encryption key; (3) share encrypted data securely; (4) back up sensitive information; (5) have a centralised management system that will help you closely monitor and remotely manage data.

1. Give PHI data the encryption pill

Encrypting data is a requirement of compliance standards, including HIPAA. Organisations are under constant attack. Regardless of whether the attack makes headlines or not, the data should be protected. A recent study found that an alarming 43% of cloud databases are not encrypted. To ensure data privacy when faced with common threats, such as DDoS and malware attacks, data must be encrypted before it is sent to the cloud, in transit and at rest.

For ultra-secure encryption, that data should preferably be encrypted with a FIPS certified randomly generated AES 256-bit encrypted encryption key. Confidential information stored on a local computer or drive, sent via email or file sharing service and shared in the cloud should be securely encrypted.

"Healthcare institutions are responsible for protecting and securely storing PHI data"

2. Don't let PHI data spread like a virus – control the encryption key

If the data is stored in the cloud, control of the encryption key is important. Granted, most cloud service providers (CSPs) will encrypt their customers' data and some even offer a key management system service, which allows customers to manage their encryption keys. However, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff – much like leaving your house key under the doormat that half the neighbourhood knows about.

In fact, the US Department of Health and Human Services launched an inquiry into Google's partnership with non-profit healthcare organisation Ascension. Reportedly, 150 Google employees can access the healthcare data on tens of millions of patients, including patient names and dates of birth, diagnoses, patient health and hospitalisation records.

The user needs full and secure control of the encryption key in order to ensure the data is kept confidential even if the cloud account is hacked. Having your own key management system will not only give you more control of encryption keys but is also more convenient for those using a multi-cloud solution.

Security measures must go beyond the cloud login credentials. If a hacker obtains the user's credentials, the breach will go unnoticed to the CSP as they won't be able to decipher between a legitimate user from an attacker. By keeping the encryption key, which should be encrypted itself within an ultra-secure Common Criteria EAL4+ microprocessor along with a PIN authenticated code, away from the cloud increases the number of security measures from just one authentication, the cloud account login, to as much as a five-factor authentication.

3. Sharing is caring, but only if the data is secure

The more people the data is shared with, the greater the challenge to ensure data privacy. In 2019, over 60% of personal data breaches reported to the Information Commissioner's Office (ICO) were a result of human error – healthcare being the most affected sector – with a fifth of those incidents caused by posting or faxing data to the incorrect recipient and 18% whose emails landed in the wrong inbox. In fact, a concerning 59% of US healthcare IT professionals cite email as the most common point of compromise.

Storing PHI data in one place and accessed by authorised users only, who have a copy of the encrypted encryption key at hand, can allow for efficient working whilst ensuring data security.

Sharing encrypted data securely allows for instant collaboration in the cloud, saving time in what would be days of posting encrypted USB flash drives to and from colleagues. This is a far greater alternative to the archaic use of fax machines the NHS only just discontinued in March 2020. The NHS admittedly agreed to increased investment in its IT department, especially following the infamous WannaCry ransomware attack.

4. Failing to back up data will make you WannaCry

The healthcare sector is no stranger to ransomware attacks. In only one week, five US healthcare organisations reported ransomware attacks last year and one Ohio-based healthcare provider paid a $75,000 ransom to unlock its systems. In 2017, the NHS infamously suffered the WannaCry ransomware attack affecting around a third of England's hospital trusts who were running unpatched systems, costing the NHS £92 million in total.

Backing up valuable data onto an encrypted hard-disk drive can save healthcare service providers the trouble of losing access to important information during a ransomware attack. Using a PIN protected hard-disk drive will secure the data even if the drive is lost or stolen.

> "The user needs full and secure control of the encryption key in order to ensure the data is kept confidential"

To avoid losing sensitive information in the event of a ransomware attack, sharing information using PIN protected USB flash drives is another safe option. This can be especially useful for remote workers as they can securely protect and back up their confidential data whilst on the go.

5. Centralised management – saving hands for data privacy

Controlling access to data is challenging when there is a high volume of data that is widely shared. For example, Canada-based genetic testing company LifeLabs reported it discovered unauthorised access to its systems, containing the data of 15 million patients, including contact details, lab results and health card numbers. The lawsuit claims the company failed to implement "adequate security measures", including failing to encrypt their data.

Another worrying example is that of a dismissed hospital administrator who hacked his NHS trust and stole 14 files relating to his sacking, 600 staff-related documents, 150 documents discussing management matters and almost 9,000 patient heart scan images.

These incidents highlight the need for a centralised management of data. Having one IT manager responsible for each department and a superior IT manager overseeing the whole organisation will help organisations monitor and manage large amounts of sensitive data in an organised fashion.

IT managers need full visibility and control of all member access to data within the organisation. Administrator capabilities – such as temporarily disabling or resetting encryption modules (storing the encrypted encryption key to access data stored in the cloud), restricting file types, encrypting file names, viewing user's log files, displaying user's location, as well as geo-fencing and time-fencing capabilities – will all contribute to an efficient oversight of data.

Healthcare institutions must assume responsibility for data privacy. Encrypting PHI data is the first step in doing so. When organisations encrypt their data themselves, they have control of the encrypted encryption key and increase security measures when storing data in the cloud. Sharing that encrypted encryption key to authorised colleagues, backing up data in PIN protected drives and having full visibility and control of users and devices will ensure data confidentiality when information is shared, if the cloud is hacked or if a drive is lost.

Taking control of sensitive information to ensure its privacy will help healthcare institutions avoid hefty data breach fines, preserve their reputation and, most important of all, earn patient and customer trust.