BioSpectrum the business of Bio & Health Sciences

# DLP- essential tool of pharma industry for data protection

29 April 2021 | Views

**Failure to protect sensitive data can lead to severe repercussions both from reputation standpoint and monetary damage control**

Pharmaceutical companies are both producers and collectors of vast quantities of sensitive data stemming from not only selling pharmaceutical products but also developing them. From initial research to the patent filing, clinical research phases, the issuing of licenses, and the manufacturing process, pharmaceutical companies handle massive amounts of highly sensitive, confidential data which they are obligated to protect under data protection laws.

The processing of these special categories of sensitive data is prohibited unless exemption criteria are met. Among them is an individual's explicit consent to process the data, but also processing for health-related purposes where it is necessary for the benefit of natural persons and society as a whole. A further exemption allows the processing of special categories of data when scientific research is being conducted that operates within an ethical framework and aims to grow society's collective knowledge and well-being.

While all these exemptions make it sound like pharmaceutical companies can freely process sensitive data, it is in fact limited to processing in the context of the management of health or social care services and systems, including the management of such data for the purpose of quality control. These limitations aim to curtail attempts to use big data analytics techniques to profile or market to individuals based on their health data.

Failure to protect sensitive data can lead to severe repercussions both from reputation standpoint and monetary damage control. The pharmaceutical companies need to put robust data protection safeguards in place to avoid them. At the same time, data protection is vital to maintain the trust and confidence of customers and individuals involved in clinical research.

Data loss prevention (DLP) solutions are an essential part of the tools pharmaceutical companies need to use to keep sensitive data secure. Aimed at tackling internal threats rather than external ones, DLP technology helps pharmaceutical organisations to avoid data leaks and data theft originating from employee carelessness or malicious insiders. Let's take a closer look at some of the ways in which DLP helps protect pharmaceutical data.

**Monitor data**

DLP solutions allow pharmaceutical companies to discover what types of protected sensitive data they collect or produce, where it is being stored, and how it travels in and out of the company network. Using content inspection and contextual scanning, DLP tools such as endpoint protector can search for sensitive pharmaceutical data in hundreds of file types in real-time, whether it is in transit or stored locally on employees' computers. Based on the results of searches, controls can be put into place to limit or block transfers as needed.

**Block & control the transfer**

The easiest way sensitive pharmaceutical data is leaked is over the internet. Employees accidentally send data to the wrong recipients or use unsecured third-party services such as cloud storage or file sharing websites to transfer data. DLP solutions do not only block the attachment and uploading of files containing sensitive pharmaceutical data but can also prevent employees from copy-pasting or manually inserting sensitive data into emails.

DLP tools also log any attempt to violate a policy, thus allowing pharmaceutical companies to identify the common ways in which data security is threatened and later incorporate them into training exercises to educate employees on best data security practices.

Another way pharmaceutical data can be easily lost or stolen is through removable devices such as USBs or external hard drives. Physical access to a device is needed for such incidents to occur, but employees frequently use USBs in particular to copying files they might work on remotely or when travelling for meetings or events outside the company.

To ensure that sensitive pharmaceutical data is not transferred outside of work computers, DLP solutions can be used to block the use of peripheral and USB ports, but also the connection of devices via Bluetooth. Alternatively, pharmaceutical organisations can also limit their use to trusted devices such as those issued by the company.

**Prevent unauthorised storage**

As employees perform their duties, they often store sensitive pharmaceutical data locally on their hard drives, having data stored in unknown locations can be problematic. Unknowingly storing copies of this data amounts to non-compliance due to a lack of due diligence. To prevent this, DLP solutions allow companies to search all computers on their corporate network for sensitive pharmaceutical data and, when found in unauthorised locations, remediation actions can be taken such as deleting or encrypting these files.

*Filip Cotfas, Channel Manager, Cososys, Romania*