Healthcare facilities at mines have vulnerable data - is it being adequately protected?

In the mining industry maintaining accurate, secure medical records for up to 40 years is compounded by an environment that that are often fairly hostile and prone to natural disaster. Mining healthcare facilities are also profitable targets for cyber criminals because of the wealth of highly personal data, making them vulnerable to ransomware and other malicious attacks.

By Hemant Harie 11 Nov 2019

Hemant Harie

Legislation and data protection regulation

The Healthcare Professions Council of South Africa's (HPCSA) guidelines state that medical records must be stored for a least 20 years. In addition, the Protection of Personal Information (PoPI) Act stipulates minimum requirements for maintaining privacy when it comes to processing personal information. Both of these laws are relevant in the mining secto and must be adhered to as part of data management.

However, mining operations are typically global and multinational, which means that they also need to comply with global la including the European Union's General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) enacted by the USA, amongst others. This makes compliance complex and requires stringent management of all data, particularly personal information such as healthcare records.

An attractive target for cyber crime

Because legislation demands that huge volumes of information be stored by mines these facilities become highly attractive targets for cyber criminals. Ransomware in particular is a challenge, the critical nature of data such as medication needs and medical clearance often leaves these facilities with little choice other than to pay the ransom to recover information ar access to their infrastructure. Proactive management of data is vital, including adequate disaster recovery (DR) to ensure that these facilities can recover quickly without having to pay the ransom.

Protecting the data to ensure continuity and compliance

Medical software utilises specific technologies such as a picture archiving and communication system (PACS) to store an access data from multiple different source machines. Even though these solutions are designed specifically for the medica industry, they only address the needs of storage and access. However, they are not designed to manage and protect data

and this is where vulnerabilities have emerged.

If data is only stored locally on site, physical disaster is always a reality. The mining sector in particular faces this issue, since the environmental conditions are often prone to earthquakes and mine collapse amongst other natural disasters. In addition, turbulent political climates can create man-made disasters. Without effective management, including offsite back and DR, an incident could result in significant volumes of lost data as well as the institution of financial penalties due to non compliance.

Purpose-built data management for the medical industry

The ultimate goal is to protect data, not just store it. A purpose-built data management solution capable of enterprise-grade data management as well as the ability to handle clinical image archiving is the solution. Data management platforms designed for the medical industry integrate directly with PACS and are capable of working with digital imaging communications in medicine (DICOM) format, so they give mining healthcare facilities the ability to secure back end storage. This includes encryption so that it complies with laws like HIPAA and the GDPR, while remaining accessible and available.

In addition, multiple copies of data can be maintained offsite, either in the cloud or at another data centre, so that facilities can recover easily from a disaster or a ransomware attack with a clean set of data that includes all medical imaging archives.Data deduplication, compression and other data management technologies can be employed to prevent data volumes from spiralling out of control.

Importantly, a purpose-built solution will enable data management tools to access data from and return it to PACS without corrupting it. It allows data to be indexed to make it searchable outside of PACS software for simplified access and compliance. If implemented at a mine's head office, it provides a centralised repository of clinical data from various differe sites that can read and access data independent of software. This is crucial in an industry where data needs to be stored decades but where technology and software are constantly evolving and may cause access problems further down the line

For healthcare facilities at mines, data management is critical. Not only does it help to ease compliance with multiple regulations, it improves data access and provides a layer of protection in the event of disaster, ransomware attack or othe data loss event. This ensures maximum uptime and minimal impact to patients should such an event occur.

ABOUT THE AUTHOR

Hemant Harie is the managing director at Gabsten Technologies.