DATA SECURITY CONSIDERATIONS WHEN IMPLEMENTING QAD ERP IN THE LIFE SCIENCES INDUSTRY

LOGAN CONSULTING

Two decades ago, when cloud-based ERP solutions were introduced, companies viewed hosted systems as the panacea for cyber security. This is not the case as 90% of data breaches are the direct result of human error. Internal business processes are still key to protecting against data breaches. Manufacturers/distributors who have faced a reportable data loss suffered both public relations damage as well as financial repercussions, as the average cost to remediate stolen or compromised data is $141 per record. Fines can be a meaningful percentage of a company's total revenue!

As we continue to advance in a digital society, manufacturers and software providers alike are becoming more aware of various security threat types, especially specific threats for the medical device and pharmaceutical industries that are reliant on production, distribution, and in some cases, personal data.

Not only are security considerations *needed before* implementing an ERP system like QAD, but data security issues need to be thought as of on-going concerns as regulating bodies all over the world are drafting new, more stringent data protection requirements for Life Sciences manufacturers. QAD's EE release is ready for this challenge!

When thinking about sensitive data in the life sciences industry, both personal and health information is what generally comes to mind. HIPAA, GDPR, and other similar regulations dictate data management of this private information, which is often referred to as protected data. Typically, protected data is not stored in an ERP system unless install-base support is offered to patients. In the medical device manufacturing and pharmaceutical industries, however, device history records (DHRs), product traceability records, and sales history records are more likely to be stored in an ERP system.

The integrity of this data must be protected and validated as there are strict accuracy and retention requirements for companies within the overall life science industry. To properly preserve these records, manufacturers need to have the right access controls to prevent accidental losses or manipulation, as well as data extraction and archival processes that are validated and verified.

If not stored in QAD, where is protected data stored? Who has access to the data, and through which tools? Are long term records verified? Are audit logs turned on? Are sensitive fields like banking routing information secured with the proper financial controls? Data security practices should be reviewed frequently across every department of an organization as processes and staffing change, but these details are often overlooked. As a result, many organizations are leaving data vulnerable to tampering or theft. Considering 90% of data breaches happen internally, companies need to carefully take inventory of sensitive data, and take note of their obligations to protect this data before implementing an ERP system.

To learn more about the relationship between data security, security frameworks, financial controls and QAD, contact an expert at Logan Consulting by clicking the LC logo on the first page.

“Data security practices should be reviewed frequently across every department of an organization as processes and staffing change