



Data security in the digital age

Not long ago, information produced in a laboratory was written or printed on paper and stored in a folder or file cabinet—and data security meant simply keeping your data under lock and key. Today, lab data are calculated, stored, manipulated, and shared using sophisticated digital devices, connected instrumentation, and instantly accessible platforms. While this move to digital is revolutionizing how science advances, it also presents new challenges for labs in storing, securing, and protecting important scientific and operational data.

One of the biggest challenges is in choosing the right set of data security solutions. Because of the constantly evolving, complex, and potentially threatening digital landscape, many smart labs choose to form partnerships with digital solutions providers like Thermo Fisher Scientific.

As leaders in serving science, we prioritize the security of our customers' information, so we've compiled some tips here for you about what you should look for when deciding how to implement or improve your lab's digital solution. Simply put: you shouldn't take chances with your data. You need to make sure your lab's information is protected by a robust and up-to-date set of security standards, including encryptions and physical safeguards to help keep your data reliably secure and to protect transmissions from being intercepted during a data transfer.



- **Industry standards**—we recommend that you make sure the solution you choose operates under industry standards such as ISO 27001 certification, SSAE 16 certification, and Advanced Encryption Standard (AES) 256-bit encryption. Our own lab data security program, for example, uses the Amazon Web Services™ platform, which has these certifications and safeguards. Following robust industry standards means your security—from identity and access management, data encryption, network firewalls, scheduled audits, data backup and recovery, and data sharing—will be secure and regularly updated to meet new challenges and threats.
- **Data encryption**—encryption is the process that transforms data into secret code so that they can't be hacked or stolen. Unscrupulous actors are trying to break digital codes, so it's critically important to protect your data with trustworthy and sophisticated encryption measures. One way to do this is to follow the lead of organizations that have a lot at stake in protecting their data. That's why our own approach to encryption is very similar to those employed by leading institutions like the CDC and the FDA. We mentioned that we protect data uploaded to our platform using industry-standard AES 256-bit encryption, but we also add extra protection layers such as encryption using HTTPS/Secure Sockets Layer (SSL) with a 2048-bit SSL certificate.

Additionally, you need to make sure that you set up a sophisticated monitoring regime to detect and address threats in real time. For example, the underlying systems within our platform use a host-based intrusion detection system (IDS) to monitor and analyze all traffic to detect possible intrusion. The IDS automatically feeds data

into a Security Event and Incident Management (SEIM) system for real-time alerts and notifications. Choosing a data security solution that has sophisticated encryption and extra layers of protection like these can help thwart attacks and keep your data out of the wrong hands.

- **Compliance**—since digitally stored lab data can travel around the world instantly, protecting your information means navigating a complex set of international standards. We recommend you choose a platform that is certified according to International Organization for Standardization (ISO)/IEC 27001:2013 specifications. ISO/IEC 27001 is a global standard for information security management systems (ISMS). The ISMS is a framework of policies and procedures that includes legal, physical, and technical controls involved in an organization's information risk management processes. ISO/IEC 27001:2013 certification means that your solution includes steps to help keep information assets secure on the global stage. Look for a partner that has a platform with these international certifications to enable compliance with information security regulations that may be specific to certain industries or regions, so that your data are secure at home and beyond.

Ensuring the safety of your data is critical and not worth risking with a sub-standard data security solution. Our customers rely on us to store and protect their information, provide them with resources to enable data integrity, and offer them the utmost confidence in the security of their data. While we're not the only company who can help protect your precious data, we take our responsibility to serve our customers seriously, and we're always here to talk with you about any challenges you're facing with your own data security.

To find out more about the importance of data security, go to thermofisher.com/connect

ThermoFisher
SCIENTIFIC