

# Protecting life-sciences and healthcare data against a cyber-attack pandemic



## Patient-centric solutions across the continuum of care

The COVID-19 pandemic has helped bring to the forefront another pandemic affecting the life sciences and healthcare industries: Cyber-attacks. Attempts to steal COVID 19 vaccine technology, clinical trials data sets, individual vaccination records and disrupt vaccine distribution supply chains rattled the industry and national governments. Ransomware attacks at hospitals jeopardize care and place patient's lives in danger. One thing is to have a credit card cloned, but it is a lot more serious when lives are at risk.

### A deadly pandemic

Cyberattacks on healthcare facilities in 2020 have affected 17.3 million people as a result 436 data breaches in the US alone according to the US Department of Health and Human Services (HHS). That should not come as a surprise given that health care in the United States alone represents over \$3 trillion in spending per year. The risks to health and life sciences organizations include:

- Ransomware attacks that can jeopardize critical care to patients
- Loss of critical intellectual property (IP) on new treatments, drugs, and research
- Loss of sensitive personal health information (PHI) and non-compliance
- Security of remote workers and telemedicine

A successful attack can cost patient lives or the loss of years in R&D for life-saving new drugs and treatments. It also puts in check the speed of innovation in the industry.

### Drive towards innovation

Life sciences and healthcare organizations have been going through a major digital transformation. In the drive to provide better care to patients, cost savings, and faster time-to-market for treatments, they have been:

- Adopting hybrid and cloud-based workloads, with 93% of Pharma and 72% of biotech in the cloud now for core applications according to IDC
- Expanding use of telemedicine during the Covid pandemic, transforming healthcare access
- Increasing use of advanced IoT devices, such as remote care, diagnostic, and implanted appliances
- Leveraging big data analytics to identify trends across populations and insights from clinical trials
- Digitalizing health records for portability and patient accessibility
- Adopting Artificial Intelligence for treatment and research

As a result, data - especially sensitive data - is now distributed and stored across a variety of cloud environments and internal systems and accessed from a wide range of applications, devices and workers.

## Cybersecurity complexity

The complexity of securing the modern Hybrid IT and innovations being adopted is growing exponentially. The speed of change has forced organizations to “bolt on” security point products or use cloud native security to meet specific security or compliance requirements on both new platforms and legacy systems that cannot be replaced. Consequently, IT has to manage multiple data security solutions protecting different platforms and different environments.

Another challenge is that digital health records now travel throughout the health care delivery chain. Hospitals, labs, insurances providers, drug makers, pharmacies, all have and share sensitive data that could be stored in thousands of different repositories.

## Regulatory challenges and executive orders

Compliance has always been a part of life in health care. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States protect critical health patient data while privacy legislations such as GDPR and CCPA, broaden the scope and levy substantial fines for non-compliance.

Going beyond privacy regulation, governments are now making explicit cybersecurity recommendations. While the May 12, 2021 White House Executive Order on improving the Nation’s Cybersecurity is targeted at government agencies, the order and ransomware memo to business leaders explicitly mentions that it provides “the private sector with a template for its response efforts”.

Among other directives, the executive order gave agencies 180 days to “adopt multi-factor authentication and encryption for data at rest and in transit...” and “...prioritize identification of the unclassified data considered to be the most sensitive and under the greatest threat”.

## Thales Cybersecurity Recommendations





To face these challenges, life sciences and health care organizations need to implement solutions that allow them to identify sensitive data, simplify compliance, and maintain the speed of transformation.

### Discover and classify all sensitive data

The first step in a process to protect the “crown jewels” of an organization, be they IP, PII, or PHI, is to know where the crown jewels are. CIOs must adopt solutions that provide complete visibility into sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores including the cloud, big data, and traditional environments.

### Protect data and secure access across Hybrid IT

The target of almost every attack is data, be it personal information or intellectual property. The number one priority of cyber security is the protection of data in the cloud, data lakes, or on-premises. Security should be added to the data layer in addition to the end-point or perimeter. Both structured and unstructured files must be protected with technologies such as encryption and tokenization, and access to repositories protected with strong authentication and key management.

> [cpl.thalesgroup.com](http://cpl.thalesgroup.com) <    

**Contact us** – For all office locations and contact information, please visit [cpl.thalesgroup.com/contact-us](http://cpl.thalesgroup.com/contact-us)

## Centralize data security governance

Every data security regulation and mandate requires organizations to be able to monitor, detect, control, and report on unauthorized access to data and encryption keys. It is essential to centralize security governance in a single pane of glass. The organization needs to automate the protection and access to data based on granular security policies. The automated solution should centrally manage encryption keys and configure access policies, so organizations can protect and control access to sensitive data in the cloud, on-premises, and across hybrid environments.

## Adopt a zero-trust model

CIOs need to adopt a zero-trust model for their organization’s security architecture. Access should be given on a “least privileged basis” and multi-factor authentication (MFA) should be adopted across the organization to prevent unauthorized access. Identity management and access control rules for all platforms should be centralized and be determined by a dynamic policy, enforced on a per-session basis, and updated based on information.

## Protect IoT devices

In an age when an IoT device can be a pacemaker implanted in someone’s body, IoT security is paramount. Each IoT device needs a unique, cryptographically-based identity that is authenticated when a connection is attempted. Organizations should be able to track each device throughout its lifecycle, communicate securely with it, and prevent it from executing harmful processes. All this should be based on a secure root of trust for secure key management and authentication.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.