



## STREAMLINE COMPLIANCE

# Streamline healthcare audit and compliance reporting

Imperva provides industry-leading cyber security solutions that help healthcare organizations streamline data store audits and compliance

## Auditors are moving beyond the application layer and demanding actual data security

Across healthcare organizations, data is the lifeblood of all business operations. Data spans patient-protected health information (PHI), clinical research data, and billing and insurance details. All of it must be kept as secure as possible while being readily accessible to authorized users and third parties.

Healthcare companies face additional security pressures stemming from the proliferation of privacy regulations crafted specifically for healthcare data. These regulatory requirements mandate the reporting of data breaches and impose associated fines for failure to protect sensitive information.

Most healthcare organizations have embarked on IT modernization programs. This modernization has spread data across a hybrid environment of on-premises and cloud-based data stores. Combined with relentless attacks by bad actors, the dearth of available cybersecurity professionals, and the acceleration of medical data exchange protocols, it can seem impossible to ensure healthcare data security and compliance.

Imperva, a worldwide leader in data and application security for the past 20 years, has a solution specifically tailored for healthcare organizations.

### **Safeguard confidentiality**

Safeguard the confidentiality, integrity, and availability of all PHI created, received, maintained, or transmitted.

### **Protect against threats**

Identify and protect against anticipated threats to the security or integrity of the information.

### **Prevent improper use**

Protect against reasonably anticipated impermissible uses or disclosures information.

# Imperva Data Security Fabric provides a framework for meeting HIPAA and HITECH data audit and protection requirements

Imperva Data Security Fabric (DSF) streamlines data-related compliance processes for assigning policy controls, enforcing separation of duties, retaining audit records, archiving, and reporting. It does this by automating tasks and providing easy access through interactive tools. Tasks that formerly required days to complete can be executed in minutes, saving time, shortening audit cycles, and significantly reducing compliance overhead costs.

## Imperva Data Security Fabric reduces the complexity of protecting sensitive data across your enterprise and cloud environments.

<b>Identify</b> Identify and locate all “individually identifiable health information”	<b>DSF Data Discovery and Classification</b> Discover ungoverned data, classify all data, and assess vulnerabilities
<b>Assess vulnerabilities</b> Maintain safeguards to prevent unauthorized use or disclosure of PHI	<b>DSF Data Risk Analytics</b> Identify and report data access anomalies and unauthorized behavior
<b>Set Controls</b> Implement policies that allow only authorized persons to access PHI	<b>DSF Data Access Control</b> Set policies and continuously monitor who is accessing sensitive data
<b>Audit and secure</b> Deploy mechanisms to examine and report on systems containing PHI	<b>DSF Data Activity Monitoring</b> Gain a clear actionable picture of compliance and security status
<b>Measure and report</b> Demonstrate consistent protection and policy enforcement to regulators	<b>DSF Templatized Reports</b> Generate on-demand compliance reports for PCI, HITECH, and HIPAA

## The new healthcare compliance imperative: protect data at the source

Many organizations have implemented perimeter security, data loss prevention, intrusion prevention/detection systems and endpoint protection. However healthcare organizations have complex IT environments that demand new data security requirements to protect data at the source. Multiple relational and non-relational data stores, instances and versions (often from different vendors), geographically distributed systems, and cloud, hybrid, and multicloud deployments require coordinated policies, monitoring and enforcement. Without directly protecting data at the source, gaps could exist between systems and applications leaving data stores vulnerable to attack.

Imperva works with leading EHR/EMR systems (such as Epic Systems and Oracle Cerner) to provide audit and compliance capabilities beyond the application layer — and secure the underlying database. Imperva protects data and satisfies compliance mandates wherever data resides: on-premises, in the cloud, multicloud, hybrid, or any other combination.

For more information about Imperva solutions for Healthcare, visit: [imperva.com/solutions/healthcare-protection/](https://imperva.com/solutions/healthcare-protection/)