White Paper

Experian Health Security

Security is your #1 risk. We've got your back.

Introduction

At Experian Health, we know security and privacy are a top concern to providers, labs, pharmacies and other risk-bearing entities.

Protecting sensitive medical and financial information—and keeping it from falling into the wrong hands—is high priority in healthcare. As a software-as-a-service (SaaS) pioneer in our industry, we get it. And we're doing something about it.

Experian Health fully understands the security implications in a healthcare environment, and of the SaaS model. That's why we're intensely focused on security company-wide, and why protection of data is among our primary design criteria.

- Security drives our business practices, training priorities and hiring processes.
- It's central to our everyday operations and disaster planning, including how we address threats.
- It's prioritized in the way we handle customer data.
- And it's the cornerstone of our account controls, our compliance audits and our certifications.

Experian Health's services are designed to deliver better security than most traditional on-premises solutions. And our security standards set the bar for SaaS vendors in any industry, across the globe.

We make security a priority to protect your operations—and the patients you serve.

Leading the Way

Founded in 1996 and headquartered in Franklin, Tenn., Experian Health employs more than 800 people and is among the nation's fastest-growing Software-as-a-Service (SaaS) companies. Today we partner with more than 3,000 hospitals and 7,000 other healthcare organizations representing 500,000+ providers.

Named to the Forbes World's Most Innovative Companies List, the definitive ranking of 100 new-idea creation firms, Experian Health is known for its KLAS-recognized patient access heritage, advanced data insights and patented Touchless Workflow™.

A Strong Security Culture

Experian Health has created a vibrant and inclusive security culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and at company-wide events to raise awareness.

Employee background checks

Before employees join our staff, Experian Health undertakes a rigorous verification process. We confirm an individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, we also conduct criminal, credit, immigration, and security checks. The extent of these background validation is dependent on the desired position.

Security training for all employees

All Experian Health employees undergo security training as part of the orientation process and receive ongoing security training throughout their careers with the company. During orientation, new employees agree in writing to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on the job role, additional training may be required. For instance, the information security team instructs new engineers on topics such as secure coding practices, product design and automated vulnerability testing. Engineers also attend frequent technical presentations on security-related topics and receive an informative newsletter that covers new threats, attack patterns, mitigation techniques and more.

Internal security and privacy events

Security and privacy issues are ever-evolving, and we recognize that employee engagement is key to staying steps ahead. That's why Experian Health hosts regular internal conferences to raise awareness and drive innovation in security and data privacy, which are open to all employees. One example is Tech Connect, which includes a series of events covering privacy in all areas, from software development, data handling and policy enforcement to living our privacy principles. We also hold periodic Lunch and Learns focusing on security and privacy.

Dedicated Teams

Security team

Experian Health employs an exceptional team of full-time security and privacy professionals who work with our software engineering teams and systems operations division. Our team includes experts in information, application and network security, holding advanced degrees in IT and information security as well as certifications such as CISSP, CISSK, HCISPP, CEH, ECSA, CISM, CISA, CCENT, Network+, A+, Security+, and others. These highly qualified professionals work together to maintain the company's defense systems, developing security review processes, building security infrastructure and implementing Experian's global security policies. Our dedicated security team actively scans for threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Within Experian Health, members of this dedicated team review security plans for all networks, systems and services. They provide project-specific consulting services to Experian Health's product and engineering teams. After products launch, they oversee automated processes that audit data traffic to verify appropriate usage. In addition, they monitor for suspicious activity on Experian Health's networks, address information security threats, perform routine security evaluations and audits, and engage outside experts to conduct regular assessments.

Privacy team

The Experian Health privacy team operates separately from product development and security organizations, but is highly involved in every product launch. The team reviews all design documentation and performs code reviews to ensure privacy requirements are followed. Their efforts enable release of products that reflect strong privacy standards: collecting user data transparently, providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform. In addition, the privacy team conducts thought leadership research on privacy best practices for our emerging technologies.

Internal audit and compliance team

Experian Health is supported by Experian's dedicated internal audit team that reviews compliance with security laws and regulations around the world. As new auditing standards are created, our internal audit and compliance specialists determine what controls, processes, and systems are needed to meet them. This team also facilitates and supports independent audits and assessments by third parties.

Best Practice Processes

Vulnerability management

Experian Health's vulnerability management process involves actively scanning for security threats using a combination of commercially available tools, intensive automated and manual penetration efforts, quality assurance methodologies, software security reviews, and internal and external audits. The security team is responsible for tracking and following up on vulnerabilities. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner. The owner tracks the issue and follows up frequently remediation is verified.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Experian Health takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware. Our malware strategy employs infection prevention by using manual and automated scanners to scour Experian Health's search index for websites that may be vehicles for malware or phishing.

Monitoring

Our security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior. Network analysis is supplemented by examining system logs to identify unusual behavior, such as attempted access of customer data. Experian Health's security staff and network analysis is supplemented by automated analysis of system logs.

Security and privacy

We have a rigorous incident management process for security events that may affect the confidentiality, integrity or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation and documentation. Our security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Experian Health is supported by Experian staff trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Experian Health security team is available 24/7 to all employees. If an incident involves customer data, Experian Health or its partners will inform the customer and support investigative efforts via our support team.

Hardware tracking and disposal

The status of all equipment within our data centers is meticulously tracked, from acquisition to installation to retirement to destruction. Video surveillance is implemented to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it is removed from inventory and retired. Experian Health hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. It is then stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

Defense in depth

Defense in depth describes the multiple layers of defense that protect Experian Health's network from external attacks. Only authorized services and protocols that meet our security requirements are allowed to traverse it; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to authorized personnel.

Securing data in transit

Data is most vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Experian Health. Data traveling between a customer's device and Experian Health is encrypted using HTTPS/TLS (Transport Layer Security). When sending to or receiving email from a non-Experian Health user, all links of the chain (device, browser, provider of the email service) have to be strong and work together to make encryption work.

Low latency and highly available solution

Experian Health designs the components of our platform to be redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves.

Extensive Certification

Third-party certifications

PCI compliance & accreditations

Payment Card Industry Data Security Standard (PCI DSS)

Experian Health has met the requirements of the Payment Card Industry Data Security Standard (PCI DSS) as a Level One Service Provider. Among many requirements, this process includes ongoing third-party security audits, penetration testing, thorough policies and procedures, and rigorous software testing standards. This certification is specific to our financial product suite.

SOC2 Type II Report

Experian Health is contracted with a third party to annually perform a SOC2 Type ii audit. This report can be provided to customers or business partners upon request, assuming that an NDA is in place. SOC2 criteria include Privacy, Confidentiality and Security.

Electronic Healthcare Network Accreditation Commission (EHNAC)

Experian Health has been accredited from the Electronic Healthcare Network Accreditation Commission (EHNAC) as a clearinghouse (EHNAC-HNAP). An up to date status of our accreditation can be found on the EHNAC website. This accreditation status can be found under the Passport Health Communications brand via the link below. https://www.ehnac.org/accreditation-full/#

Core Certification Phase 1 & 2

Experian Health has obtained the Core Certification Phase 1 & 2 Endorsement as a Clearing House entity.

Third-party suppliers

Experian Health directly conducts virtually all data processing activities to provide our services. However, we may engage some third-party suppliers to provide services related to its services, including customer and technical support. Prior to onboarding third-party suppliers, Experian Health conducts an assessment of their security and privacy practices to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once we've assessed risks, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Regulatory compliance

Our customers have varying regulatory compliance needs. Our clients operate across regulated industries, including finance, pharmaceutical and manufacturing.

We're looking out for you

The protection of your data is a primary design consideration for all of Experian Health's infrastructure, products and personnel operations. Our scale of operations and collaboration with the security research community enable Experian Health to address vulnerabilities quickly or prevent them entirely.

We believe that Experian Health can offer a level of protection that very few public healthcare SaaS providers or private enterprise IT teams can match. Because protecting data is core to Experian Health's business, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees you to focus on your business and innovation.