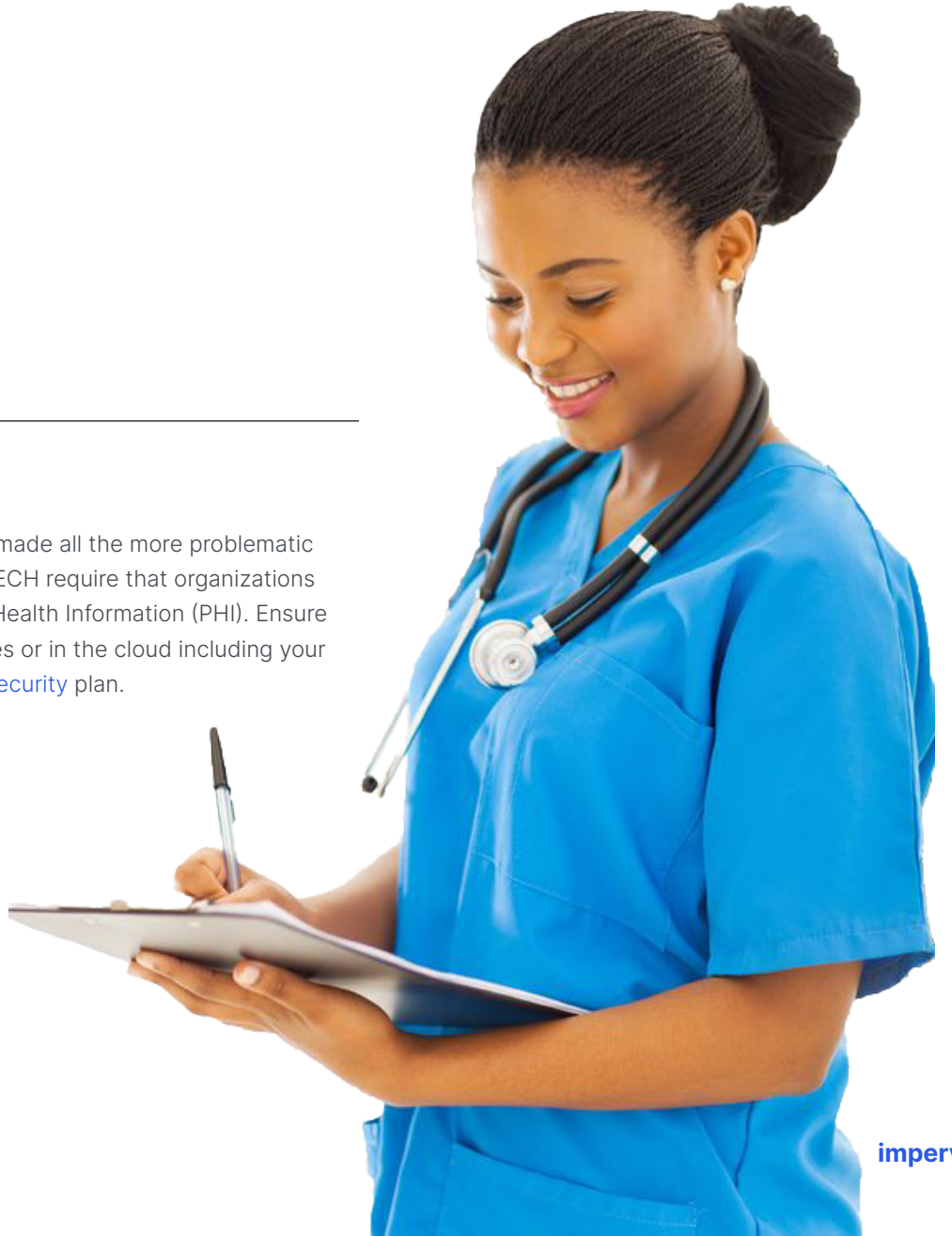
imperva

EBOOK

A 10 Step Guide to Protecting Your Healthcare Data and Applications

Protect patient PHI

Data breaches are one of the top security risks for healthcare providers, made all the more problematic by the COVID pandemic. Strict healthcare regulations like HIPAA and HITECH require that organizations have comprehensive security measures in place to safeguard Protected Health Information (PHI). Ensure compliance by protecting your sensitive patient data whether on-premises or in the cloud including your EMR solution like Epic, Cerner, or any other, with a comprehensive data security plan.



Secure your APIs

APIs are transforming how data is shared across healthcare organizations and have become an integral mechanism in healthcare today. They enable the sharing of patient data between providers to support a holistic approach to patient care and they also support improved clinical research through automation and faster access to patient information. If APIs are not secured properly your organization risks exposing sensitive patient or clinical information if your APIs come under a cyber attack. Business Logic gaps, Broken Object Level Authorization (BOLA), and third-party API management are just some of the reasons healthcare APIs can be vulnerable to malicious threat actors. Eliminate data leakage and API abuse with a solid API Security solution.

17% of API attacks in the last year were business logic attacks

Eliminate online fraud

Automated fraud driven by bad bots is common in the healthcare industry and bot traffic accounted for 42% of all traffic in 2022 with 32% of that traffic made up of bad bots. Automated fraud targeting the healthcare sector including account scraping and credential stuffing can have severe consequences including reduced access to critical data or blocking delivery of patient care. Protect your websites, mobile applications, and APIs from automated attacks with an Advanced Bot Protection solution.

Digital modernization makes Hospitals and healthcare providers a top target for cyber criminals intent on accessing to sensitive patient data and causing disruption. Here are 10 easy steps for hospitals and healthcare providers to follow to protect their data and applications.

Ensure Website Availability

If your website performance is impacted this can also impact how patients access critical services. Invest in a strong Web Application Firewall to ensure patients and providers have uninterrupted access to important information and services. When choosing a WAF, rather than opting for a basic solution, aim for a comprehensive security platform that offers protection from the latest threats such as DDoS, Bot and API attacks.

One Security Platform

In a busy industry like healthcare time management and operational efficiency are crucial and using a single stack security platform with attack analytics built-in makes life easier for everyone. Our comprehensive WAF and API Protection (WAAP) platform makes this possible with a unified platform providing WAF, DDoS, Bot and API protection to safeguard your organization against the latest OWASP threats.

Protect your entire healthcare network infrastructure from DDoS attacks

It is not only websites that are at risk of DDoS attacks. Attackers often target an organization's network layer too using DNS flood and amplification tactics to overwhelm your network with traffic to bring it to a standstill. When this happens healthcare staff are prevented from accessing any of the systems infrastructure they need to keep normal hospital operations up and running. Never assume your network layer is covered by your Cloud WAF or ISP DDoS solution. Check that your network infrastructure is sufficiently protected from DDoS attacks too.

Back-up your DDoS Protection

Depending on the criticality of your services - and for healthcare providers this is likely to be 100% criticality - consider a secondary DDoS solution in the event that your primary DDoS protection provider experiences an outage. While this sounds unlikely it has been known to happen. Ensure business continuity when you come under DDoS attack by implementing a Contingency DDoS solution.

Protect your website from DDoS attacks

Downtime is not an option - unlike other industries the healthcare sector cannot afford any downtime. If a website or healthcare network is taken offline by a DDoS attack this can have serious consequences for a hospital including preventing delivery of critical patient care. Ensure you have a DDoS protection that can mitigate an attack seamlessly with minimal disruption to services.

Rule out vulnerabilities in the healthcare supply chain

The Med-tech industry is booming as new companies emerge to develop new applications and technologies to support the healthcare industry. However, introducing DevOps and application development also adds an element of risk to the healthcare supply-chain as applications can be left vulnerable to attack when security processes are not updated as changes are made. Build security into your application runtime environment with Runtime Application Self-Protection (RASP).

Ensure continuity of services.

Finally, make sure you have a robust business continuity plan in place including backing up your systems and databases to avoid losing essential clinical data when a DDoS attack is used as a smokescreen for other cyber attacks.

If you are a healthcare provider and are considering a review of the efficacy of your security measures, Imperva can help. Every day we deliver end-to-end protection and compliance for critical healthcare data and applications around the world, and we have been named a security efficacy and operational efficiency leader in the **2022 Cloud WAF CyberRisk report** based on testing conducted by SecureIQLab. This puts us streets ahead of any other security vendor when it comes to protecting sensitive patient data and ensuring continuity of patient care.

Find out more about our security solutions for the health-care sector here.

Copyright © 2023 Imperva. All rights reserved

imperva.com
+1.866.926.4678