Barracuda Web Application Firewall:

Safeguarding Healthcare Web Applications and ePHI

Whitepaper

The Health Insurance Portability and Accountability Act

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to safeguard the privacy and confidentiality of Protected Health Information (PHI). The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 further strengthened the enforcement of HIPAA. This enforcement is carried out by the Office for Civil Rights (OCR) by investigating complaints and conducting compliance reviews.

Covered entities under HIPAA includes health plans, health care clearinghouses, general hospitals, pharmacies and any health care provider that conducts certain health care transactions electronically, as well as business associates such as contractors and sub-contractors that provide services to covered entities or access PHI.

Anyone who believes that HIPAA privacy and security rules have been violated by a covered entity can file a complaint at the online OCR complaint portal.

121,576: The number of complaints received by OCR since 2003

69% of the complaints investigated resulted in corrective action

12,974: The number of complaints in 2014, up 33% from 2013

Healthcare: An Easy and Profitable Target

Today, healthcare security practitioners are confounded by a heterogeneous mashup of legacy, acquired and custom applications and infrastructure. Often, regulation itself comes in the way of swift security patches and upgrades. Custom applications like medical billing, patient portals, insurance claim portals and the increasing use of cloud services and mobile devices has opened up additional application attack surfaces. However, security safeguards in healthcare applications have traditionally lagged behind other industries providing easy pickings for the attackers.

For the attackers, it makes sound economic sense to go after healthcare. They use stolen, individually identifiable health information for identity theft and financial fraud. This information fetches higher returns on the criminal underground compared to credit card data as it has a longer shelf life. Attacker costs for successful breaches are relatively low and they can stay undetected for long periods. This, in turn, allows them to steal larger volumes of sensitive data.

94% of Healthcare organizations are victims of cyber-attacks
– Ponemon Institute

Healthcare compromises are rampant and a looming nightmare
– SANS research findings

FBI has repeatedly warned healthcare of increasing targeted threats citing lax security controls
– FBI PIN #: 140408-009

Penalties and Costs for HIPAA Violations

Unlike PCI-DSS that regulates entities dealing with credit cards, HIPAA is a federal law. An investigation by the OCR can result in both civil and criminal penalties. Lawsuits can be filed under the HITECH act and possible class action lawsuits could be brought under the bureau of negligence.

As a result of the HITECH amendments to HIPAA in 2009, covered entities can no longer bar the imposition of civil money penalties by demonstrating ignorance to HIPAA violations. Based on the level of culpability, civil monetary penalties are classified into four tiers with increasing fines. Maximum penalties can go up to $1.5 million for all violations of an identical provision.

Civil Money Penalties

TIER	PENALTY
Didn't know & wouldn't have known with reasonable diligence	$100-$50,000 per violation. Max: $1.5 million / year
Reasonable cause and not willful neglect	$1000-$50,000 per violation. Max: $1.5 million / year
Willful neglect but corrected within required time	$10,000-$50,000 per violation. Max: $1.5 million / year
Willful neglect and not corrected	$50,000 or more per violation. Max: $1.5 million / year

As for criminal offenses, there are three tiers, with the maximum jail sentence capping out at 10 years.

Criminal Penalties

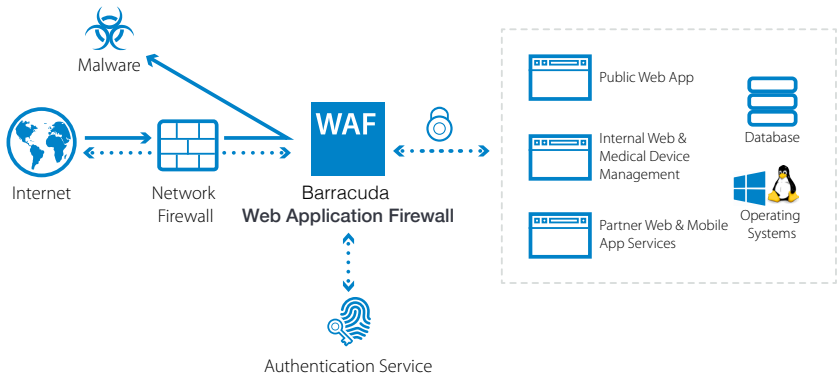
TIER	PONTENTIAL JAIL SENTENCE
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

In addition, the U.S. Department of Health & Human Services (HHS) also has the authority to impose expulsion from the Medicare Program that could send health care providers out of business.

However, penalties may not represent the highest financial burdens. There could be several other costs that include: notification and remediation expenses, disrupted operations, plummeting stock prices, loss of patient trust, and erosion of future business due to negative publicity.

Barracuda Web Application Firewall Safeguards ePHI in Your Web Infrastructure

The Barracuda Web Application Layer Firewall is an application layer firewall that secures your web applications against attacks originating from the Internet as well as from within the organization. It acts as a reverse proxy to your web applications by blocking inbound attacks and preventing data leakage through web applications.



Next-gen Firewalls do not protect an organization's web applications because they only throttle and control outbound access to third party SaaS applications. IPS and IDS solutions provide multi-protocol inbound protection, but when it comes to web applications they are limited to known attacks in common applications, offering no protection against evasion techniques and targeted threats.

The Barracuda Web Application Firewall provides sophisticated web application protection for commercial, off-the-shelf, third-party and bespoke web applications. It provides comprehensive protection against the OWASP Top 10 attacks, including SQL injection and cross-site scripting that target your applications, databases and users for identity theft or intellectual property theft.

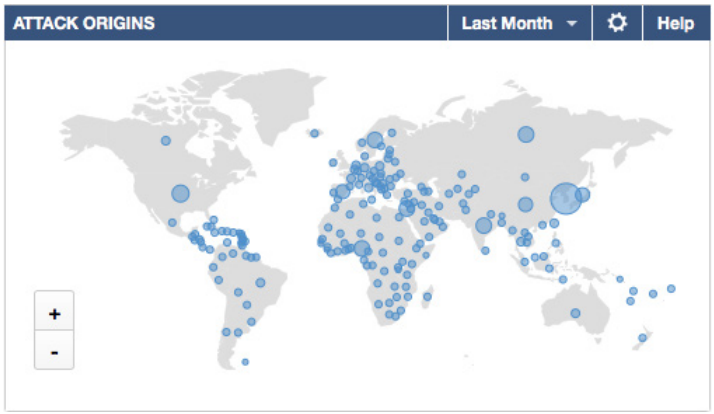
The following HIPAA citations are directly addressed by the Barracuda Web Application Firewall:

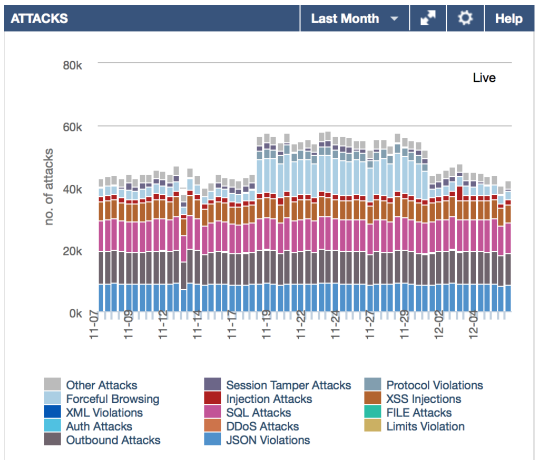
HIPAA CITATION	DESCRIPTION	WEB APLLICATION FIREWALL STATION
164.308(a)(1)	Policies and procedures to manage security violations	Aids the security management process by preventing web app attacks. It also provides virtual patching, vulnerability scanner integration, SIEM integration, and log aggregation
164.308(a)(4)	Policies and procedures to authorize access to PHI	Reverse proxy isolates PHI from other operations. Role-based-access control allows granular policies to access PHI
164.312(a)(1)	Technical (administrative) policies and procedures to manage PHI access	Supports integration with authentication directories, Single Sign-on, two-factor authentication mechanisms
164.312(a)(2)(i)	Assign unique IDs to support tracking	Access logging includes username, IP address, geo-location, browser types, time, date, session, etc.
164.312(a)(2)(iv)	Mechanism to encrypt and decrypt ePHI	Can dynamically encrypt / decrypt ePHI in URLs, parameters, hidden form fields or session IDs
164.312(b)	Procedures and mechanisms for monitoring system activity	Comprehensively logs all requests and violations to web applications as well as to the management UI
164.312(d)	Procedures to verify identities	Support for SAML, PKI, LDAP, RADIUS and other authentication schemes
164.312(e)(1)	Measures to guard against unauthorized access to transmitted PHI	Supports strong PKI to ensure secrecy during ePHI transmission over public networks
164.312(e)(2)(i)	Measures to ensure integrity of PHI on transmission	Along with strong PKI, prevents session theft, session riding, URL tampering and hidden form field tampering

Barracuda Web Application Firewall Benefits for Healthcare:

- **Instant remediation without any code changes:** Provides continuous protection against known and unknown web application threats in real time without requiring code changes or even access to the code.
- **Threat visibility including SSL inspection:** While web application attacks are one of the fastest growing threat vectors, legacy security solutions including IPS solutions are blindsided by attack obfuscations and SSL encryption. The Barracuda Web Application employs extensive anti-evasion checks and inspects inside SSL traffic providing real-time insights into threat visibility.
- **Protection in on-premises, private or public clouds:** Availability in all sizes across physical, virtual and public cloud marketplaces (AWS, Azure, vCloud) ensure that organizations considering cloud migration are fully protected irrespective of deployment models.
- **Protection for web-based APIs and IoT server infrastructure:** This includes a complete suite of protection for REST protocols and Web Services that use JSON or XML data over HTTP, which are commonly used to support mobile devices and medical devices.

- **Protection for vulnerable web server infrastructure:** Being a reverse proxy, it shields vulnerable web server infrastructure - web servers, network and SSL stacks, application framework and operating systems from attacks tunneled via web applications.
- **Cryptographic URL and hidden form field encryption:** Manipulating URLs to access unauthorized data is a very common threat in legacy healthcare applications. By encrypting the URLs and hidden form fields, attackers are prevented from targeting this vector.
- **File upload protection:** Healthcare workflows commonly require the upload and distribution of files over web applications. File upload integrity checks ensure they are free from malware and fake extensions.
- **Speed up application delivery:** Includes server load balancing, caching, compression, and content based routing to increase application response times.





About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com