

HIPAA & Mobile Devices

The Facts About Mobile Security & Compliance



Fact #1: HIPAA has included mobile since it took effect in 1996

By now, anyone working in the healthcare field should be familiar with HIPAA. The act applies to health care providers, plans and clearinghouses who transmits health information in electronic form, and requires security measures to ensure that patient data are private and secure.

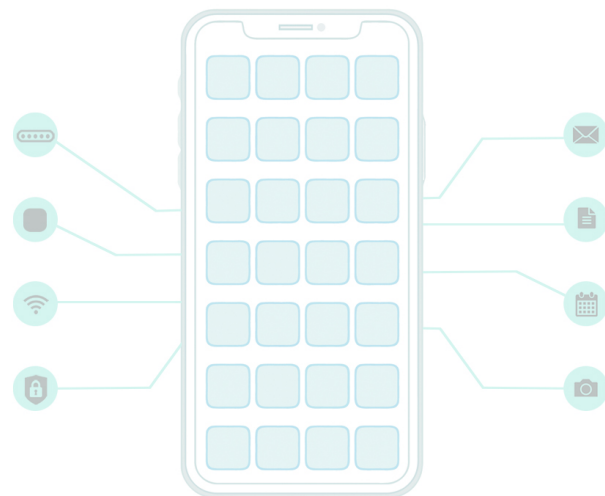
What may not be as widely known is that HIPAA requirements have applied in principal to mobile devices since the act came into effect on August 21, 1996, with the Final Omnibus Rule of 2013 adding still more amendments covering the use of mobile devices. The HIPAA Journal states plainly that with respect to mobile devices, the result is the same for healthcare organizations whether they employ a BYOD or supply mobile devices to their staff: "Mobile devices are a potential minefield of HIPAA violations."

In other words, if your HIPAA compliance measures do not yet include mobile devices, you are out of compliance.

Fact #2: Mobile devices are 60% of HIPAA-covered endpoints

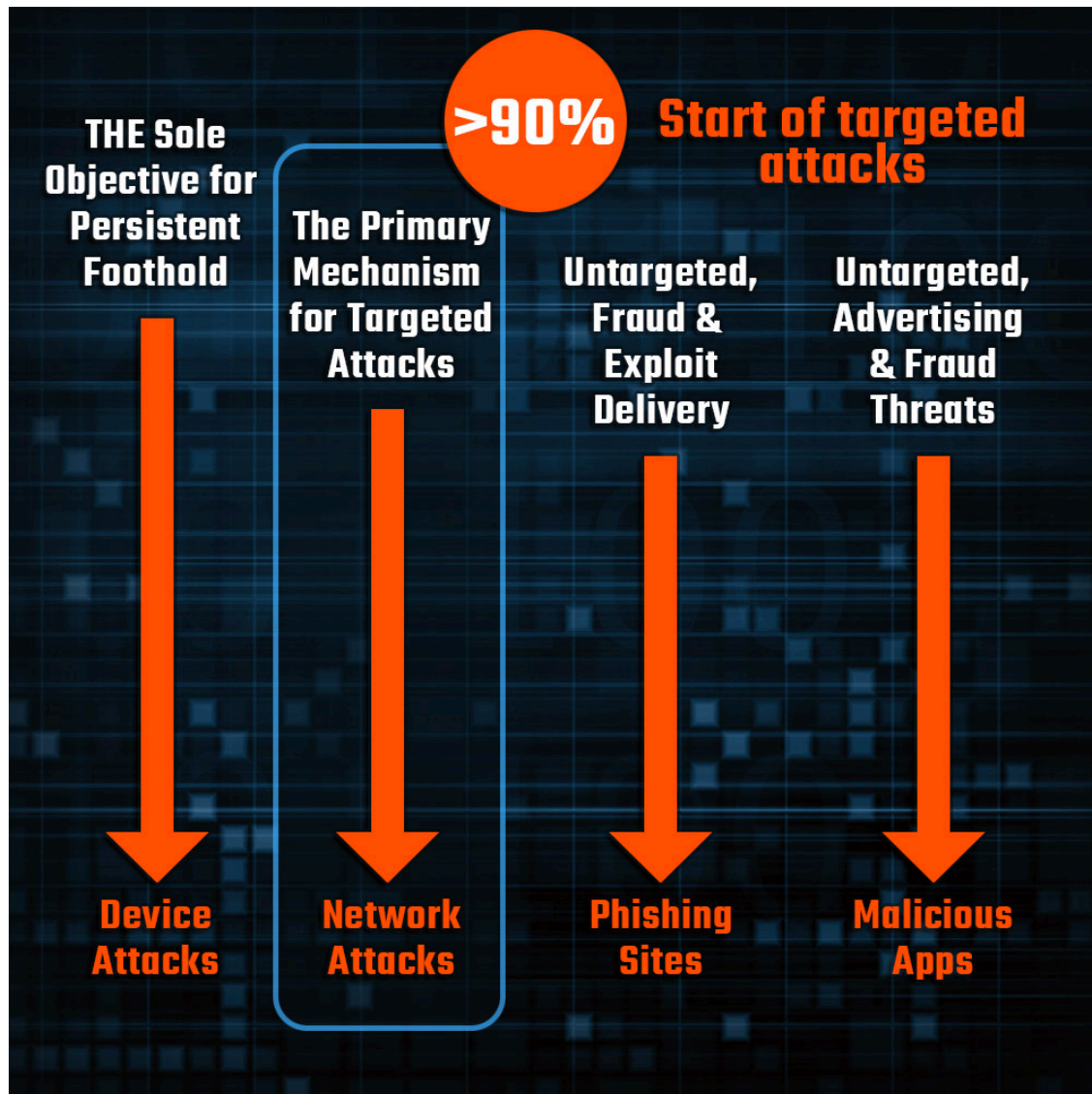
HIPAA compliance violations are being reported at the rate of more than one per day, hitting historical highs in the last two years. So, it is not surprising that most enterprises subject to HIPAA have invested significant resources toward achieving compliance. The problem arises when enterprises focus on protecting endpoints without realizing that **mobile devices are endpoints**, both with respect to HIPAA and in general.

Mobile devices are now in wide use as a platform for productivity in healthcare. That means that the traditional computing devices (e.g., servers, desktops and laptops) that enterprises have focused their security and compliance efforts on are only about 40% of their enterprise's endpoints. The other 60% of devices that connect to your network—mobile devices—must be made HIPAA-compliant as well.



Fact #3: Mobile endpoints are under attack

One critical difference between mobile devices and other types of endpoints is the variety of attack vectors that mobile devices are exposed to. Ensuring the integrity of mobile devices requires protecting them against all of these forms of attack.



Fact #4: Mobile requirements for mobile are explicit

In order to meet the HIPAA requirements for secure endpoints—including mobile devices—and help ensure texts, messages, emails and files are protected, healthcare organizations must implement the following:

SECTION	SUBSECTION	PROVISION
164.308		Administrative safeguards
	(a)(1)(ii)(D)	Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	(a)(5)(ii)(A)	Install periodic security updates.
	(a)(5)(ii)(B)	Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.
	(a)(5)(ii)(C)	Enable logging and log alerting on critical systems
	(a)(6)(ii)	Standard: Security incident procedures. Implement policies and procedures to address security incidents.
	(a)(6)(ii)	Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Fact #5: Zimperium is the solution for mobile HIPAA compliance

Zimperium leverages a patented, machine learning-based engine to detect mobile device, network, phishing and app attacks in real time. The engine runs efficiently on smartphones and tablets without violating user privacy. To date, it has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting HIPAA mobile requirements.

Mobile apps containing and processing patient data must be secured against attacks as well, even on patient-owned devices. Zimperium has the solution.

Contact Zimperium for HIPAA mobile compliance

When you are ready to ensure compliance with HIPAA mobile requirements, please [contact us](#) for a custom evaluation.



Learn more at: zimperium.com

Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244