

PCIDSS Changes 2024

PCI DSS version 4.0 goes into effect on **March 31, 2024**, and has 63 new requirements. Some requirements are effective immediately, but the bulk isn't effective until March 31, 2025, giving businesses a year-long transition period to implement the more challenging requirements.

PCIDSS stands for Payment Card Industry Data Security Standard, which is a set of requirements for ensuring the security of cardholder data. The PCI Security Standards Council (PCI SSC) is responsible for developing and maintaining the PCI DSS, and they have recently released version 4.0 of the standard, which introduces some significant changes from the previous version 3.2.1.

According to the web search results, some of the main changes in PCI DSS 4.0 are:

- The standard introduces two methods for achieving compliance: the defined method and the customized method. The defined method is similar to the current approach, where organizations must follow specific testing procedures and guidance for each requirement. The customized method allows organizations to use alternative ways to meet the intent and objectives of each requirement, as long as they can demonstrate how their approach provides the same or better level of security. [The customized method is intended to provide more flexibility and innovation for organizations that use new or emerging technologies that may not be compatible with the defined method¹.](#)
- The standard emphasizes the importance of security as a continuous process, rather than a point-in-time assessment. Organizations are expected to monitor and measure their security performance on an ongoing basis, and to adjust their security controls as needed to address changes in their environment, threats, and risks. [The standard also introduces new requirements for establishing roles and responsibilities, documenting policies and procedures, and reporting on security activities²³.](#)
- The standard updates and expands the scope of the requirements to cover new technologies and threats, such as mobile devices, cloud services, internet of things (IoT), phishing, social engineering, and e-commerce payment applications. [The standard also revises the authentication requirements, including requiring multi-factor authentication \(MFA\) for all remote access to the cardholder data environment, and increasing the minimum password length to 12 characters¹²⁴.](#)

The PCI DSS 4.0 will become effective on March 31, 2024, and will replace the current version 3.2.1, which will be retired on the same date. However, organizations will have the option to use either version for their assessments until then. [Additionally, some of the new requirements in PCI DSS 4.0 will be considered as best practices until March 31, 2025, and will become mandatory on April 1, 2025²³⁴.](#)

I hope this information helps you understand the changes in PCI DSS 4.0 and how they may affect your organization. If you have any questions, please feel free to ask me. 😊

PCI DSS VS. HIPAA

We live in an age where ecommerce and online shopping is an integral part of our everyday lives. Garage Sales turned into Ebay. Costco turned into Amazon. Whether we like it or not our lives in many ways revolve around online businesses in more ways than one. We take online shopping for granted when in reality there is so much more going on behind the scenes of being able to process a payment online.

The Payment Card Industry is dominated by a few key brands: American Express, Visa, and Mastercard to name a few. In 2004, credit card fraud was on the rise with the increase in online shopping, the major credit card brands banded together to form the Payment Card Industry Data Security Standards or PCI DSS. While there are well over a thousand validation points within the PCI DSS, they can be reduced to 12 requirements that the Payment Card Industry requires companies to uphold in order to process payments with their credit cards. Any business that wants to accept payments online must uphold these standards. Luckily many plug-ins such as Stripe or Square allow companies to use their service for a small fee and take advantage of this.

In addition to the PCI DSS, any company conducting business in the United States that is handling any sort of protected health information (PHI) is required to maintain the standards as laid out in the **Health Insurance Portability and Accountability Act** (HIPAA). While HIPAA was originally in 1996, it has been adapted and expounded upon heavily, most considerable in 2013 the Final **Omnibus Rule** which extended the requirements of HIPAA to not just covered entities such as hospital or dental practices, but anyone who comes in contact with PHI throughout the course of their business (business associates). This now requires not just Doctor's or healthcare professionals to be HIPAA compliant, but now their IT services, accountants, and even **software developers** who conduct business with these covered entities are held to the standards of HIPAA.

While there is a bit of overlap between the PCI DSS and HIPAA, compliance with one is nowhere near compliance with both. While they are both pretty exhausted for their respective industries, entities within the healthcare industry are required to maintain compliance with both in order to do business. Below we will briefly outline the requirements of both and identify some key differences.

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS is made up of 12 key requirements to ensure secure data transfer when processing online payments online. These 12 requirements are as follows:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

Health Insurance Portability and Accountability Act (HIPAA)

In contrast, the requirements of HIPAA have much less to do with payment information and more to do with a person's PHI. The **requirements of HIPAA** are as follows:

1. Appoint a Privacy Officer
2. Privacy Policies
3. Security Procedures
4. Business Associate Agreements in Place
5. Annual Training
6. Regular Risk Assessment
7. Established Breach Notification Protocol

PCI DSS goes into much more detail and has quite a few more regulations than HIPAA in regard to the respective data at hand. Because payment information is considered PHI, the HIPAA

requirements do apply to payment information however they do not encompass all the requirements of PCI DSS. As seen, there are quite a bit more regulations on payment card information than protected health information. One could make the argument that payment card information is vastly more important to secure over PHI however, according to experts, PHI is **between 10 and 20 more valuable** than a credit card number when sold online. Because of this, other countries and even states have noticed the need for increased security measures for PHI and have introduced more stringent policies such as **GDPR** in the EU or CCPA in California to name a few that build on the foundation set by HIPAA. With the value of PHI much higher than that of payment card numbers and legislation being a bit more up in the air, this does create a market need for

Ultimately, PCI DSS and HIPAA both aim to secure entirely different types of information while attempting to meet a similar need: data security. While there is a degree of overlap, it is not enough to constitute any sort of real benefit from focusing on one over the other. In fact, simply becoming compliant for either leaves you exposed to noncompliance in the event of an audit.