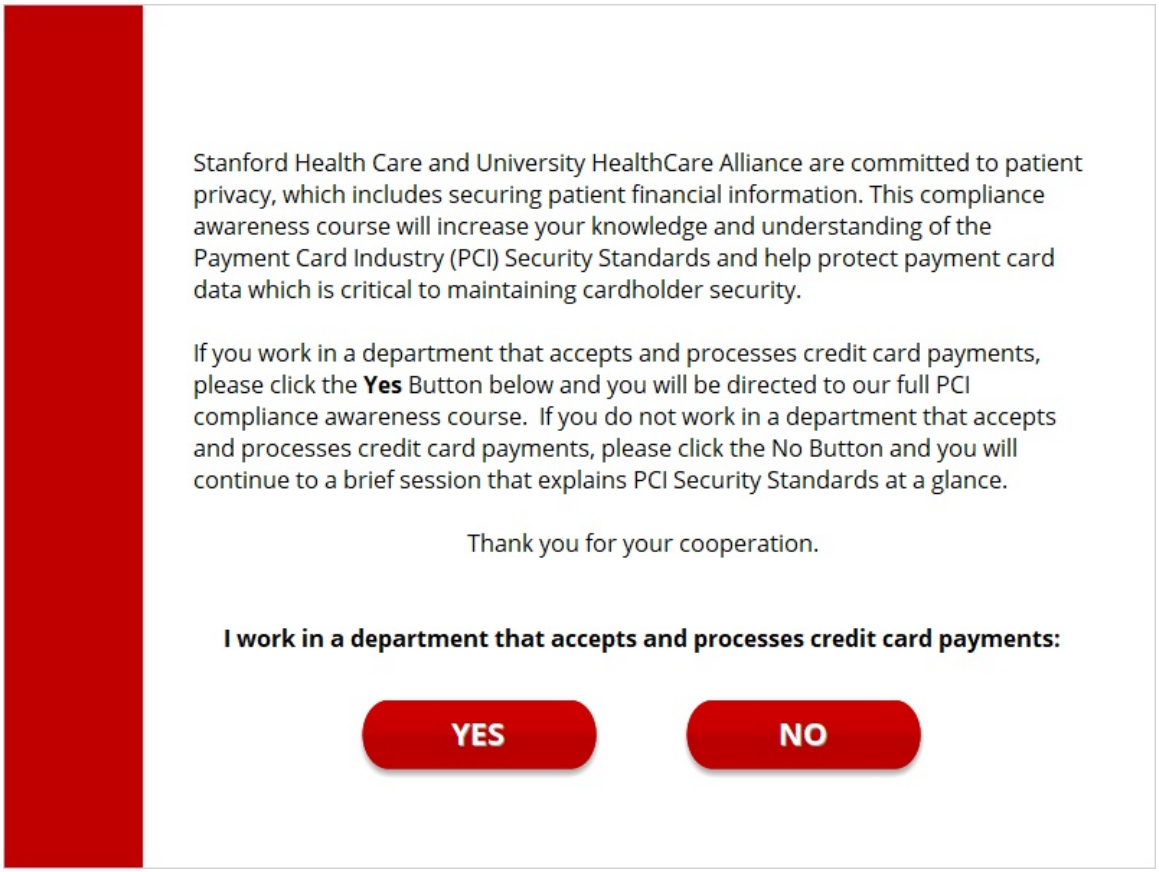
UNIVERSITY HEALTHCARE ALLIANCE

Payment Card Industry (PCI)

Security Standards

rev 01.11.18



NOTE:

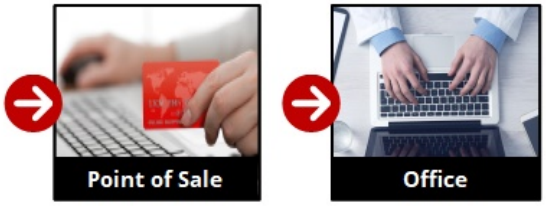
For all UHA-Affiliated Providers, the above answer should be "NO". The screens that follow are from the interaction that results from the NO selection above.

PCI Security Standards at a Glance

With the growing threat of identity theft and data leaks, customers rely on us to keep their payment card account information safe and secure. That's why we follow the Payment Card Industry Data Security Standards (commonly known as the PCI Security Standards). The PCI Security Standards provide clear guidelines for how we manage payment card data, including network security parameters, data encryption and storage practices, system access controls, and network monitoring and testing.

You play an important role in applying the PCI Security Standards-and building our customers' trust-when you follow best practices for protecting cardholder data.

To learn more about applying the PCI Security Standards, click the **Point of Sale** and **Office images** on the top right. *When you are finished, you may click the Next button to continue.*



POINT OF SALE

At the point of sale, the PCI Security Standards require you to take several precautions to protect cardholder data, including:

- Turning screens so that they are only visible to you and the current customer.
- Ensuring all documents containing cardholder data are kept in secure areas and out of plain view.
- Ensuring any cardholder data obtained is kept secure. This includes not reading cardholder data out loud even for confirmation purposes.

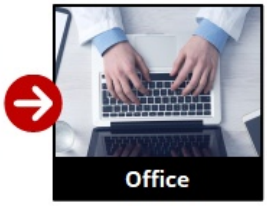
If you have not yet clicked the **Office** Image yet, please do so now.

PCI Security Standards at a Glance

With the growing threat of identity theft and data leaks, customers rely on us to keep their payment card account information safe and secure. That's why we follow the Payment Card Industry Data Security Standards (commonly known as the PCI Security Standards). The PCI Security Standards provide clear guidelines for how we manage payment card data, including network security parameters, data encryption and storage practices, system access controls, and network monitoring and testing.

You play an important role in applying the PCI Security Standards-and building our customers' trust-when you follow best practices for protecting cardholder data.

To learn more about applying the PCI Security Standards, click the **Point of Sale** and **Office images** on the top right. *When you are finished, you may click the Next button to continue.*



OFFICE

While working in the office, the PCI Security Standards require you to take several precautions to protect cardholder data, including:

- Ensuring all documents containing cardholder data are stored and disposed of securely and out of plain view.
- Discussing cardholder data in private locations. Always take measures to limit cardholder information spoken aloud.
- Using locking screensavers when you are away from your desk to prevent unauthorized access to data on your computer.

If you have not yet clicked the **Point of Sale** Image yet, please do so now.