# Texas Tech University Health Sciences Center Call Center Compliance

## *PCI DSS Compliance for Call Centers*

PCI compliance for Call Centers is especially critical to maintain customer trust and business reputation. Schools and Departments are responsible for ensuring compliance with TTUHSC OP 50.37 – Payment Card Processing by TTUHSC Departments.

## *Identify Call Center Management and Processes*

Call Centers must identify their operations, management, and processes by emailing merchantID@ttuhsc.edu for a review of the Call Center's compliance controls.

## *Reduce scope by not recording credit card information*

According to the PCI standards, recorded calls are subject to the same rules as any other method of capturing and storing customer card authentication data. Some recording systems provide call center representatives with a button, allowing them to pause the recording when credit card numbers are spoken, while others integrate with operating systems to automatically pause the recording based on actions taken by the representative. It is best if call recording is automatically muted when account numbers, security codes, and other sensitive information is spoken. Departments that prevent recording payment information reduce scope as those calls are not in scope for a PCI audit.

## *Establish access controls*

In any call center environment, representative and supervisor desktops should have role-based access to limit the number of staff exposed to sensitive data and ensure individual staff members only have access to what they need to do their job. For example, a patient representative might be able to view patient details, but they may not be able to update or delete them. A team supervisor may be able to view the performance of the team that they are assigned to, but they should not be able to view the performance of other teams within the same Call Center or project.

## *Limit access to credit card information*

In addition to role-based security, Call Centers should a consider the points at which any staff comes in contact with data to ensure proper security and compliance. Access to sensitive customer and payment data should be restricted including physical access, e.g., limiting access to key areas of the building. Personal items or bags should be prohibited at the workstation.

### *Establish strong passwords*

Departments should also make sure that all passwords are strong, e.g., a mix of numbers, and lower- and upper-case characters that are changed regularly.

### *Ban pen and paper*

One of the easiest ways to stay PCI compliant is to stop representatives from using pen and paper and use a whiteboard instead. This step will limit the physical storage of customer details. Just be sure to maintain a number of white board rules like ensuring they cannot be removed from a representative's desk and also ensuring that they are cleaned regularly.

### *Ban mobile devices*

Another really straightforward and sometimes overlooked step is to ban mobile phones in the call center. By taking this step you can eliminate any potential for sensitive call center information being leaked onto an agent's personal device.

### *Continuously Enforce PCI*

Don't consider PCI compliance as just an annual exercise. This approach can lead to problems and potential compliance failure. Instead PCI DSS compliance should be looked at as an ongoing process. Compliance is not a project you can complete and never revisit. Compliance needs to be updated on an ongoing basis, enforced continuously, and reassessed on an annual basis.