4 Things to Consider when Securing Patient Payments

It may not surprise you to learn that data security is identified as one of the top 5 priorities by healthcare IT professionals.[1] With a heavy focus now on patient clinical data, it's important not to overlook vulnerable payment data. Here's some helpful considerations when it comes to protecting card data.

1. **A layered security approach offers the best defense**
   As the name implies, a layered approach involves combining multiple security measures to defend against attacks on card processing systems. Technologies such as EMV, encryption and tokenization can be combined to provide end-to-end security. You can combat fraudulent card use at the point of service with EMV and prevent card data theft with encryption and tokenization. Leverage these technologies to safeguard both card present (in-office payment) and card not present (phone, online) environments.
2. **PCI compliance gets easier with stronger security**
   Achieving PCI compliance is a notoriously time-intensive process. Implementing the latest security technologies can decrease the effort and resources required to establish and maintain compliance. Encryption and tokenization remove card data from your environment by rendering it unusable to thieves – this effectively reduces the scope of your payment network making your compliance process simpler.
3. **EMV devices do more than just process chip cards**
   If you're unsure about investing in EMV devices, perhaps this information will change your thinking. Most EMV devices are manufactured to include encryption technology. If you're relying on older mag stripe devices, payments may not be encrypted at the time of swipe

leaving card data exposed to hackers. And as more businesses upgrade their security technologies, the organizations that lag will be most vulnerable to attack.

4. **Your patients are concerned about security too!**
   As consumers become increasingly accustomed to using chip cards, they will expect to see EMV devices wherever they pay for services – including healthcare. Your patients want to know their card data is safe. In fact, over half of consumers believe 'chip' cards will make their transactions more secure.[2] EMV is one of the most visible signs that a business cares about consumer payment data. Adopting the latest security technologies gives your patients and your business peace of mind.

Elavon
A U.S. Bancorp Company

1 Modern Healthcare. "Cybersecurity rising as health IT concern." February 27, 2016
2 HarborTouch Report. "More than Half of U.S. Consumers Lack Awareness of EMV 'Chip' Credit Cards as October 2015 Transition Deadline Looms", September 2015.

Elavon 2 Concourse Parkway Atlanta, Georgia, 30328, USA