Welcome to PMI’s Webinar Presentation

Brought to you by:
Practice Management Institute®
pmiMD.com

Meet the Presenter…

Steven Kleinberg, EVP/COO
CardChoice Merchant Services, LLC

On the topic:
PCI Compliance: Securing Patient Data
Welcome to Practice Management Institute’s Webinar and Audio Conference Training. We hope that the information contained herein will give you valuable tips that you can use to improve your skills and performance on the job. Each year, more than 40,000 physicians and office staff are trained by Practice Management Institute. For 30 years, physicians have relied on PMI to provide up-to-date coding, reimbursement, compliance and office management training. Instructor-led classes are presented in 400 of the nation’s leading hospitals, healthcare systems, colleges and medical societies.

PMI provides a number of other training resources for your practice, including national conferences for medical office professionals, self-paced certification preparatory courses, online training, educational audio downloads, and practice reference materials. For more information, visit PMI’s web site at www.pmiMD.com

Please be advised that all information in this program is provided for informational purposes only. While PMI makes all reasonable efforts to verify the credentials of instructors and the information provided, it is not intended to serve as legal advice. The opinions expressed are those of the individual presenter and do not necessarily reflect the viewpoint of Practice Management Institute. The information provided is general in nature. Depending on the particular facts at issue, it may or may not apply to your situation. Participants requiring specific guidance should contact their legal counsel.

CPT® is a registered trademark of the American Medical Association.
PCI Compliance – Securing Patient Data

CardChoice International
- Registered ISO/MSP of BMO Harris Bank, Chicago, IL
- Trusted Advisor to:
  - American Medical Billing Association
  - Practice Management Institute
  - New York State Society of CPA’s
  - HealthPac

Overview

- Gain a better understanding of Payment Card Industry compliance
- Identify how patient data can be stolen
- Tips on securing your practice from a breach
- Financial impact of a post breach
- What is EMV and it’s impact on Fraud Liability Shift
- Is it ok to store patient payment information on file?
Assessing Your Risk Tolerance

PCI Breaches Can Be Costly
Fines Up To $500,000

Who’s Risk is it Anyway?

Closing The Door on Data Risk

The door is never 100% closed
What is PCI Compliance?

PCI stands for Payment Card Industry. The PCI security standards are technical and operational requirements set by the PCI Security Standards Council to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions.

Who Needs To Be Compliant?

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data

- Manufacturers/Resellers
- Software Developers
- Payment Application Vendors
- Merchants & Service Providers
- PCI Security Standards Council
- PCI-DSS

Ecosystem of payment devices, applications, infrastructure and users

HIPAA vs PCI Compliance

The Council is responsible for managing the security standards, while compliance regulations are enforced by the founding members of the Council - American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

<table>
<thead>
<tr>
<th>HIPAA Compliance</th>
<th>PCI-DSS Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Regulations Set By Health &amp; Human Services Government Communities</td>
<td>Security Regulations Set By PCI Security Standards Council Private Industry</td>
</tr>
<tr>
<td>Enforced by OCR</td>
<td>Enforced by Card Associations</td>
</tr>
<tr>
<td>Compliance is a documented risk assessment and management plan</td>
<td>Technical requirements explicitly outlining the necessity for processes</td>
</tr>
</tbody>
</table>
One Way of Thinking About PCI Assessment

Pilots perform a preflight assessment before takeoff, but are constantly monitoring systems during flight and prepared with written procedures in the event of a failure.

Not All Merchants Are The Same

Larger organizations require a broader scope to complete their PCI assessment.
What Assessment Level (Size) Merchant Are You?

There are four PCI compliance levels and their compliance requirements vary. Merchants are assigned to a level based on their combined transaction volume — including credit, debit and prepaid cards — over a 12-month period. The four levels (from fewest to most transactions) and their requirements are: Merchants with externally facing IP addresses must perform quarterly network penetration scans to achieve compliance.

Level 4: Small businesses that process less than 20,000 eCommerce transactions. All other businesses that process up to 1 million transactions annually. Level 4 businesses must complete an annual risk assessment using the appropriate PCI Self-Assessment Questionnaire (SAQ). Quarterly PCI scans, administered by an approved scanning vendor, may also be required.

Level 3: Mid-sized eCommerce companies that process between 20,000 and 1 million transactions annually — fall into this level. Level 3 companies are required to complete an annual risk assessment using the appropriate SAQ. Quarterly PCI scans, administered by an approved scanning vendor, may also be required.

Level 2: Level 2 companies conduct between 1 million and 6 million transactions yearly.

Level 1: “Big box” stores and major corporations are Level 1 companies, which are defined as having a minimum of 6 million transactions per year.

Determining Your Self Assessment Questionnaire?

<table>
<thead>
<tr>
<th>SAQ</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises. Not applicable to face-to-face channels.</td>
</tr>
<tr>
<td>A-EP*</td>
<td>Merchants who outsource all payment processing to PCI DSS validated third-parties, and who have a website(s) that doesn’t directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises. Applicable only to e-commerce channels.</td>
</tr>
<tr>
<td>B</td>
<td>E-commerce merchant using only: ○ Imprint machines with no electronic cardholder data storage, and/or ○ Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>B-IP*</td>
<td>Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>P2PE-HW</td>
<td>Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.</td>
</tr>
<tr>
<td>D</td>
<td>SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.</td>
</tr>
</tbody>
</table>
12 Requirements For PCI-DSS

The PCI Data Security Standard is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI-DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>12. Maintain a policy that addresses information security for all personnel.</td>
</tr>
</tbody>
</table>

Example of Self Assessment Questionnaire C
Example of Good Passwords

Complex passwords don’t have to be complicated

Complex passwords don’t have to be complicated

- bigmac = 0.077 seconds (not a dictionary word)
- B1gMac = 14 seconds (upper, lowercase, number)
- B1gMac1 = 14 minutes (7 characters)
- iB1gMac = 15 hours (8 characters)
- B1gMacfries = 412 years (11 characters)
- Bigmacandfries = 511 years (14 characters, but only letters)
- B1gMac&fries = 344,000 years (12 characters)

WHY Is It Important For Your Practice To Be PCI Compliant?

Breaches Exposing Social Security Numbers Credit Card/Debit Cards (2010 - 2015)

- Exposed SSN:
  - 2010: 62.1%
  - 2011: 61.8%
  - 2012: 48.0%
  - 2013: 48.0%
  - 2014: 41.5%
  - 2015: 49.3%

- Exposed CC/DC:
  - 2010: 25.7%
  - 2011: 26.4%
  - 2012: 14.4%
  - 2013: 15.6%
  - 2014: 17.6%
  - 2015: 20.5%

2015 Data Breaches – Identity Theft Resource Center
The healthcare industry has been a big target of attackers in recent years and that did not change in the first half of 2016. Healthcare led all industries with 263 data breaches, which accounted for about one quarter (27%) of the total.*

Over the past 12 months, hackers have continued to go after both low-hanging fruit and unprotected sensitive personal data that can be used to steal identities," Jason Hart, VP and CTO for data protection at Gemalto

*Gemalto – 2016 It’s All About Identity Theft Report
Actual Breach Examples

**Akorn Inc. has customer database stolen, 50,000 records offered to highest bidder**
Hacker responsible says they compromised the company to teach them a lesson in security
*As reported in CSO Online*

**Former Northwest Primary Care Employee Stole 5,372 Patient Records**
The data theft occurred over two years ago between April and December 2013, although NWPC was only made aware of the theft on October 13, 2015. The former employee had been subjected to a background check prior to being employed and references had been obtained from past employers
*As reported in the HIIRA Journal*

**FBI alerts Owensboro Health to Breach at Muhlenberg Hospital; Breach Began in January, 2012 - 84,681 Records**
OH Muhlenberg, LLC was notified by the FBI of "suspicious third party activity on the Hospital's computer network". It was discovered that key logging malware had infected a number of computers.
*As reported in IT Governance USA*

**Sutter Health Physician Suffers Second 2015 Data Breach 1342 Records Compromised**
This is not the first time the offices have suffered at the hands of burglars, and in only January of this year the same facilities were broken into and 350 patient charts were stolen along with a credit card register.
*As reported in the HIPAA Journal*

---

3rd Party Malware Intrusion

Russian cyber criminals injected malware into MICROS support servers using remote administration tools to access the point of sale device.

Point-of-sale based malware has driven most of the credit card breaches over the past two years, including intrusions at Target and Home Depot, as well as breaches at a slew of point-of-sale vendors. Once the attackers have their malware loaded onto the point-of-sale devices, they can remotely capture data from each card swiped at that cash register.

**MICROS Deployed at Over 330,000 Sites Across 180 Countries**
Close to 150,000 Patient Medical Records Potentially Affected by Bizmatics PrognoCIS EHR Data Breach

By researching the breach incidents filed to the Office Civil Rights, it appears that data breaches affecting at least six healthcare providers stem from the Bizmatics data server hack, which, according to letters sent to Bizmatics clients, occurred in January 2015. According to the OCR breach portal, those breaches potentially impact the Protected Health Information of 149,776 individuals.

List Of Breached Practices

- Vincent Vein Center - Grand Junction, CO - 2,250 patients
- Eye Associates of Pinellas - Pinellas Park, FL - 87,317 patients
- ENT and Allergy Center - Fayetteville, AK - 16,200 patients
- Health Solutions - Easton PA - 19,776 patients
- Longevity Institute - Westlake Village, CA - 4,836 patients
- Pain Treatment Centers of America (PTCOA) and Interventional Surgery Institute (ISI) Arkansas - 19,397 patients

Subcontractor leaks approximately 10,000 patients records at 29 facilities throughout the U.S. and approximately 40 employed physicians

Tenet Health officials said the data was not stolen from its databases, but rather from a company called InCompass Healthcare. Turns out, InCompass disclosed a breach in August 2014, which reportedly occurred after a subcontractor of one of the company’s service providers (24 ON Physicians) failed to secure a computer server containing account information. The Subcontractor was PST Services, a medical billing service.
Common Myths of PCI

**Myth 1 – One vendor and product will make us compliant**
Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI. You should implement a holistic security strategy that focuses on the “big picture” related to the intent of PCI requirements. This approach includes people and processes, not just technology.

**Myth 2 – Outsourcing card processing makes us compliant**
Outsourcing simplifies payment card processing but does not provide automatic compliance. Don’t forget to address policies and procedures for cardholder transactions and data processing.

**Myth 3 – PCI DSS will make us secure**
Successful completion of a system scan or PCI DSS assessment is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

**Myth 4 – We don’t take enough credit cards to be compliant**
PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.
Common Myths of PCI - Continued

Myth 5 – We completed a SAQ so we’re compliant
After that moment of a completed SAQ, only another assessment or post-breach forensic analysis can prove PCI compliance. But a single system change can make you non-compliant in an instant. True security of cardholder data requires non-stop assessment and remediation to ensure that the likelihood of a breach is kept as low as possible.

Myth 6 – PCI DSS makes us store cardholder data
Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card, or equivalent data from a chip.

Myth 7 – PCI DSS is too hard
Understanding and implementing the 12 requirements of PCI can seem daunting, especially for merchants without a large security or IT department. However, PCI mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations.

Top 10 PCI-Failing Scan Findings

<table>
<thead>
<tr>
<th>No</th>
<th>Vulnerability Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Web Application Transmits Login</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>TLSv1.0 Supported</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SSL/TLS Weak Encryption Algorithms</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>HTTP TRACE/TRACK Methods Enabled</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Reflected Cross-Site Scripting (XSS)</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SSLv3 Supported</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>SSL Certificate Public Key Too Small</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Windows DCE Service Accessibility</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>OpenSSH SSHFP DNS resource record</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Insecure Certificate Signature Algorithm</td>
<td></td>
</tr>
</tbody>
</table>
Top 10 To Do List - Pass PCI Compliance

1. Maintain a current network diagram.
2. Provide security training to employees annually.
4. Eliminate electronic storage of customer credit card data.
5. Maintain an incident response plan.
6. Segment your credit card network from Wi-Fi networks.
7. Test your Internet connection to protect it from hackers.
8. Isolate your payment devices from other computers.
9. Only permit authorized business traffic into your network.

Additional Information/Resources

The PCI Security Standards Council sets the standards for PCI security but each payment card brand has its own program for compliance. Specific questions about compliance should be directed to your acquiring financial institution.

Links to payment card brand compliance program include:

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp (U.S.)

Additional information:
www.pcisecuritystandards.org
What Is EMV?

EMV stands for - Europay, MasterCard and Visa. It is also referred to as a chip card or smart card. It is a fraud-reducing technology that embeds a chip on the card. It can help protect issuers, merchants and consumers against losses from the use of counterfeit and lost or stolen payment cards at the point-of-sale.

Why EMV Technology

The EMV Chip Specifications are designed to significantly improve the security for face-to-face payment transactions by providing features for reducing the fraud that result from counterfeit and lost and stolen cards.

New features that improve payment security are as follows:

- The terminal can now authenticate the chip card to verify that the card is genuine
- When an EMV card is used for payment, the card chip creates a unique transaction code that cannot be used again
- The unique transaction code makes it virtually impossible to duplicate stolen card data
- More robust cardholder verification methods to protect against lost and stolen card fraud

United States Accounts For Over 50% Of All Fraud

- As criminals recognize EMV implementations are underway, they look towards merchants that haven’t adopted EMV technology and card-not-present merchants.
- Businesses still using magnetic stripe only terminals, are on the hook for fraud costs if someone uses a counterfeit or lost or stolen EMV payment card.
The USA Lags Last With EMV Transactions

To encourage the timely adoption of EMV, the card associations shifted Fraud Liability to the merchant for the first time in October of 2015.
**EMV Transaction**

**How To Use**

- **Insert Card**
  Instead of swiping, you'll insert the card into the terminal, chip first, face up.

- **Leave the Card in the Terminal**
  The card must remain in the terminal during the entire transaction.

- **Sign the Receipt or Enter a PIN**
  Either sign the receipt or enter your PIN to complete the transaction.

- **Remove Your Card**
  When the purchase is complete, remember to take your card with you.

*Remember: The chip card still has a magnetic stripe, just in case you need to use it with a traditional terminal.*

---

**EMV FAQ**

**What is a Chip Card?**
Chip cards are regular plastic credit or debit cards with an embedded microchip. A chip card also has a magnetic stripe on the back of the card.

**Where can I use my Chip Card?**
You can use your chip card anywhere credit cards are accepted. You can swipe your card just like you do today using the magnetic stripe on the back of the card, if a chip-activated terminal is not yet available.

**What if my Chip Card doesn’t work when I insert it into the chip terminal?**
Some merchants may have chip terminals, but they may not yet be activated to accept chip cards. If you are unable to insert your chip card into a chip terminal, you can always swipe your card to complete the transaction.

**Are Chip Cards more secure than magnetic stripe cards?**
Chip Card technology offers another layer of security when used at a chip-activated terminal, because it generates a unique, one-time code that is needed for each transaction to be approved.
New Technology and Regulations are a Game Changer

Is storing your patient’s payment on file a good thing?

Three factors billers and providers need to know

1) 68% of patients will pay at point of care if given a good faith estimate of EOB
2) 50% of all bills are paid online while check usage decreased to less than 23%
3) Technology provides billers and providers with a competitive edge

The Flamingo Las Vegas Hotel put your payment card on file before giving you your room key.

Adopting Account On File (AOF) Today is Critical

- Provider collection rates run at 50% to 70% for small-dollar liabilities
- 3.3 statements on average before payment is received
- It costs $5 - $20 to collect from patients who do pay
- Visa identified healthcare as a market needing significant improvement

Source: 2009 McKinsey survey of retail health care consumers
Source: 2008 McGraw-Hill
Source: Visa - AuthorizeFirst Transaction Guidelines

Rapid Growth of Patient Responsibility

Source: 2009 McKinsey survey of retail health care consumers
Yesterday’s Paper AOF Setup

Pre-Authorized Healthcare Form

I authorize ABC Medical Services to keep my signature on file and to change my credit card account as indicated below:

Check One: □ Visa □ MasterCard □ Discover □ Amex

Select one of the following payment options:

☐ I authorize the credit card charges in the amount of $275.00 to be paid within 90 days of the date of this form. I understand that this form is valid for one year unless I cancel the authorization through written notice to the healthcare provider.

I authorize the credit card charges for services receiving treatment of $______ every ________

________________________

Steven Tyler

Patient Signature

ABC Medical Services

Do Not Store CCOF Form In Patient Records

Reduce the scope of PCI compliance

Quick Checkout – Automate Payment Plans Securely

[Webinar/Audio Conference]
January 31, 2017

Practice Management Institute
www.pmiMD.com
Technology Allows For Safe Credit Card Storage

Reduce the scope of PCI – Store sensitive payment data offsite in a secure vault that can be recalled for future patient payments

Benefits of Account on File For Provider

Secures Payments
- Provide additional payment options
- Enable patients to make payment arrangements while they are still at your office

Reduces Costs and Accounts Receivable
- Reduce the number of statements mailed & stream-line the post-visit billing process
- Improve cash flow

Improves Payment and Processing Efficiencies
- Lower bad debt
- Provide timely payment for services after adjudication
- Reduce manual resources needed to process, track, and research delinquent fees
- Enable your staff to control and manage cash
- Automats reconciliation by processing payments after a claim is fully adjudicated
- Potential to increase average transaction size by 20% - 30%
Tips, Tools and Techniques

Here’s what you can do right now:

- Use the latest anti-virus software and keep patches up to date
- Review system logs manually or use an automatic tool to check for suspicious activity
- Update all default and staff passwords with secure passwords
- Consider implementing a:
  - PCI-approved point-of-interaction (POI) device with SRD functionality
  - PCI-approved point-to-point encryption (P2PE) solution
- Confirm that all third party vendors are properly implementing and maintaining security controls outlined in the PCI Data Security Standard (PCI DSS)

Questions?

Contact:

Steven Kleinberg
skleinberg@cardchoice.com
Phone: 866.350.3200