Welcome to PMI’s Webinar Presentation

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

Meet the Presenter…

Steve Kleinberg, VP/COO
Cardchoice International

On the topic:
Secure Patient Payments While Maintaining PCI Compliance
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

Presented by:
Steven Kleinberg
CardChoice International
EVP/COO

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
  - New Jersey Association of Osteopathic Physicians and Surgeons

Overview

- Gain a better understanding of Payment Card Industry compliance
- Data breach statistics and examples
- Basic fixes to start securing your practice
- Healthcare statistics as they relate to patient payments
- Implementing a Credit Card on File program
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?

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®.

HIPAA Compliance
Security Regulations set by Health & Human Services Government Communities
Enforced by OCR
Compliance is a documented risk assessment and management plan

PCI-DSS Compliance
Security Regulations set by PCI Security Standards Council Private Industry
Enforced by Card Associations
Technical requirements explicitly outlining the necessity for processes
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 Merchant Environments Are The Same

COMPLEX ENVIRONMENT

SIMPLE ENVIRONMENT

HARDER TO REDUCE RISK

EASIER TO REDUCE RISK
Larger organizations require a broader scope to complete their PCI assessment.

The more features your payment environment has, the more complex it is to secure. Extra features like (Wi-Fi, cameras, or IP phones) often provide easy ways for criminals to steal your patient card data. Think carefully about whether you really need these extra features for your business.

How do you accept payments? There are three main ways:

1. A patient pays in the office face to face with their card.
2. A patient visits your website and pays online.
3. A patient calls your office and provides card details over the phone, or sends the details in the mail or via fax.

What Assesment 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:
  - **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.
- Merchants with externally facing IP addresses must perform quarterly network penetration scans to achieve compliance.
### Determining Your Self Assesment 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>E-commerce 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>Merchants 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.</td>
</tr>
<tr>
<td></td>
<td>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>
</table>
| Build and Maintain a Secure Network | 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 |
| Protect Cardholder Data            | 3. Protect stored cardholder data  
4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software or programs  
6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 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 |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes. |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel. |
**Example of Self Assessment Questionnaire C**

**Build and Maintain a Secure Network and Systems**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>PCI DSS Question</th>
<th>Expected Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>Do firewall and router configurations restrict access to the network?</td>
<td>Yes, No, Can't say</td>
</tr>
<tr>
<td>1.2.1</td>
<td>(a) Are inbound and outbound access controlled to that which is necessary for the authorized data?</td>
<td>Yes, No, Can't say</td>
</tr>
<tr>
<td>1.2.2</td>
<td>(b) Are inbound and outbound access controlled to that which is necessary for the authorized data?</td>
<td>Yes, No, Can't say</td>
</tr>
</tbody>
</table>

**Example of Good Passwords**

<table>
<thead>
<tr>
<th>Password</th>
<th>Time to Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>bigmac</td>
<td>0.077 seconds</td>
</tr>
<tr>
<td>B1gMac1</td>
<td>14 seconds</td>
</tr>
<tr>
<td>B1gMac2</td>
<td>14 minutes</td>
</tr>
<tr>
<td>leB1gMac</td>
<td>15 hours</td>
</tr>
<tr>
<td>B1gMacfries</td>
<td>412 years</td>
</tr>
<tr>
<td>Bigmacandfries</td>
<td>511 years</td>
</tr>
<tr>
<td>B1gMac6fries</td>
<td>344,000 years</td>
</tr>
</tbody>
</table>
WHY Is It Important For Your Practice To Be PCI Compliant?

Of the 940 breaches attributed to hacking, 21.4 percent involved phishing and 12.4 percent involved ransomware/malware.

2017 Data Breaches – Identity Theft Resource Center
## Healthcare Industry Accounts for 23.7% of 2017 Breaches

### Top 25% of 2017 Healthcare Breaches

<table>
<thead>
<tr>
<th>Breach ID</th>
<th>Company or Agency</th>
<th>State</th>
<th>Breach Category</th>
<th>Individuals Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITRC20170127-02</td>
<td>Commonwealth Health Corporation / Med Center Health</td>
<td>CA</td>
<td>Medical/Healthcare</td>
<td>81,550</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>Atrium Health, Inc. / Atrium Health</td>
<td>NC</td>
<td>Medical/Healthcare</td>
<td>24,889</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,708</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
<tr>
<td>ITRC20170127-02</td>
<td>MedStar Health System</td>
<td>MD</td>
<td>Medical/Healthcare</td>
<td>25,848</td>
</tr>
</tbody>
</table>

### Totals for Category: Medical/Healthcare

- # of Breaches: 374
- # of Records: 5,062,031
- % of Breaches: 23.7%
- % of Records: 2.8%
Actual Breach Examples

1.4 million patient records breached in UnityPoint Health phishing attack

How it Happened
According to the notice, the health system’s business email system was hit by a series of targeted phishing emails that looked like they were sent from an executive within UnityPoint. An employee fell victim to the emails, which gave hackers access to internal email accounts from March 14 until April 3.

What Was Stolen
The hacked accounts included protected health information, including names, addresses, medical data, treatment information, lab results and/or insurance information. For some of the 1.4 million patients, their payment card and Social Security number were included in the breach.

Action Taken
UnityPoint reset passwords on the compromised accounts, conducted mandatory phishing education for employees, added security tools to identify suspicious emails and implemented multi-factor authentication, officials said.
OCR Investigates Banner Health breach

How it Happened
In June 2016, hackers got into Banner’s payment processing system at 27 locations or their food and beverage outlets, which they used as a gateway into the network and eventually the servers containing patient data. The health data breach exposed 3.7 million patient records and was discovered on July 13, 2016 but an investigation from a third party revealed that the initial breach started on June 17, 2016.

What Was Stolen
Affected records may have had names, dates of birth, addresses, physicians’ names, dates of service, clinical information, social security numbers, 21,000 credit card numbers and possibly health insurance information.

Action Taken
While the details are still a bit fuzzy, data security expert Bill Kleyman, maintained that this is a lesson for other healthcare organizations to ensure that they are constantly reviewing where their valuable data is being stored. Furthermore, they need to ensure they know how that data is being protected and where there is access.

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.

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>
June 30th was the deadline for disabling SSL/early TLS

What is TLS?
Transport Layer Security (TLS) is a cryptographic protocol used to establish a secure communications channel between two systems.

Implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Start Securing Your Practice Today With These Basic Fixes

<table>
<thead>
<tr>
<th>How to Safeguard your Business Against Breaches</th>
<th>Cost</th>
<th>Ease</th>
<th>Risk Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use strong passwords and change default ones</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Protect your card data and only store what you need</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Inspect payment terminals for tampering</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Install patches from your vendors</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Use trusted business partners and know how to contact them</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Protect in-house access to your card data</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Don’t give hackers easy access to your systems</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Use anti-virus software</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Scan for vulnerabilities and fix issues</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Use secure payment terminals and solutions</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>Protect your business from the Internet</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
<tr>
<td>For the best protection, make your data useless to criminals</td>
<td>0</td>
<td>✓</td>
<td>000</td>
</tr>
</tbody>
</table>
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](http://www.americanexpress.com/datasecurity)
- Discover Financial Services: [www.discovernetwork.com/fraudsecurity/disc.html](http://www.discovernetwork.com/fraudsecurity/disc.html)
- JCB International: [www.jcb-global.com/english/pci/index.html](http://www.jcb-global.com/english/pci/index.html)
- Visa Inc: [www.visa.com/cisp](http://www.visa.com/cisp) (U.S.)

Additional information: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

---

Patient Payments Are a Growing Problem

- 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

2. MGMA

![Rapid Growth of Patient Responsibility](chart.png)
High Deductible Insurance Plans - Increasing the Patient Portion of Your Revenue

SOURCE: NCHS, National Health Interview Survey, 2010–2017, Family Core component

Percentage of persons under age 65 enrolled in a high-deductible health plan

What are you doing today to reduce the amount of statements you are sending?

Determine Your Cost of Sending Statements

How Many Statements Do You Send Per Month? 900
What is Your Cost to Generate Statements? On Average - $5.00
What is Your Average Receivable? $150.00

In this example is costs the practice $4500/revenue cycle to bill $135,000 hoping to collect 50 to 70 percent.

Then the process starts again next month
The Importance of Providing an Estimate at Point of Service

Start concentrating on the 2/3 of patients that want to pay

68% of consumers willing to pay at point of service by credit / debit card or check, if a good-faith estimate is provided:

- 52% by credit or debit
- 16% by check

Of the 52% agreeing to pay by Credit or Debit card at point of service:

- 25% would pay up to $200
- 27% would pay $500 or more

Source: 2009 McKinsey survey of retail health care consumers

Visa AuthorizeFirst Specifically For Healthcare Industry

Visa® identified healthcare as a market needing significant improvement

Visa AuthorizeFirst Healthcare Transaction Guidelines
Tools and Best Practices for Processing Pre-authorized Healthcare Transactions

As the healthcare industry continues to work towards achieving real-time claim adjudication, Visa introduces the Consumer AuthorizeFirst Healthcare Transaction process. This transaction process provides the patient with a new payment option using their Visa card. Yes, This Is Legal.
AuthorizeFirst is intended for use by healthcare merchants

<table>
<thead>
<tr>
<th>MCC</th>
<th>DESCRIPTION</th>
<th>MCC</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4119</td>
<td>Ambulance Services</td>
<td>8042</td>
<td>Optometrists and Ophthalmologists</td>
</tr>
<tr>
<td>5975</td>
<td>Hearing Aid Sales, Service and Supplies</td>
<td>8043</td>
<td>Opticians</td>
</tr>
<tr>
<td>5976</td>
<td>Orthopedic Goods, Prosthetic Devices</td>
<td>8044</td>
<td>Optical Goods and Eyeglasses</td>
</tr>
<tr>
<td>7277</td>
<td>Counseling Services—Debt, Marriage and Personal</td>
<td>8049</td>
<td>Podiatrists and Chiropractors</td>
</tr>
<tr>
<td>8011</td>
<td>Doctors and Physicians</td>
<td>8050</td>
<td>Nursing and Personal Care Facilities</td>
</tr>
<tr>
<td>8021</td>
<td>Dentists and Orthodontists</td>
<td>8062</td>
<td>Hospitals</td>
</tr>
<tr>
<td>8031</td>
<td>Osteopaths</td>
<td>8071</td>
<td>Medical and Dental Laboratories</td>
</tr>
<tr>
<td>8041</td>
<td>Chiropractors</td>
<td>8099</td>
<td>Medical Services and Health Practitioners</td>
</tr>
</tbody>
</table>

How Does It Work?

1. CCOF is presented to patient as a payment option for out-of-pocket expense
2. Setup Pre-Authorization Payment Option (Single or recurring Options)
   - Provide patient with maximum estimated amount owed
   - Patient provides payment (Credit / Debit or Checking / Savings)
   - A copy of the signed agreement is given to the patient
3. Claim is Adjudicated
   - Match the claim remittance (835/ERA) to the corresponding Pre-Authorization form
   - Provider submits a card authorization for up to the maximum agreed amount
   - Payment is processed and provider receives funds within 24-48 hours
Paper CCOF Setup

Pre-Authorized Healthcare Form

ABC Medical Services

I authorize ___________ to keep my signature on file and to change my credit card account as indicated below.

Check One: 🗳 Visa 🗳 MasterCard 🗳 Discover 🗳 Amex

Below are the following payment options:

- $275.00 (indicate one) for visits only.
- No visits this year.
- Reimbursement charges (exceeding $____) every

I assign my insurance benefits to the provider listed above. I understand that this form is valid for one year unless I cancel this authorization through written notice to the healthcare provider.

Steven Tyler

Patient

123 Sunset Avenue

Any City, MI 76543

Date: 03/20

Authorized: Steven Tyler

Patient Signature

Do Not Store CCOF Form In Patient Records. Store in a locked cabinet and only allow access to the authorized personnel who processes credit card payment.

ABCMedicalServices

X

275.00

Steven Tyler

123 Sunset Avenue

Any City, MI 76543

Date: 03/20

Authorized: Steven Tyler

Patient Signature

Reduce the scope of PCI compliance

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
- Allows for the use of HSA/FSA payments

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

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
- Fewer bills going to collections or write-offs

Benefits of Account on File For Patient

Increased Convenience
- Authorization and transaction occurs only after a claim has been adjudicated
- Removes the inconvenience of paying an estimated amount at the time of service
- Eliminates the need to adjust estimated payments after a claim has been adjudicated
- Reduces delinquency or collection agency
- Saves time by eliminating the need to mail in
- Eliminates worry about missed billing due dates or payments
- For providers offering a payment plan, CCOF allows patients to make billing arrangements that fit their budget

Security
- Offers patient protection for charges that the patient did not approve
- Eliminates writing sensitive credit card information on mailed payment forms
- Eliminates the risk of providing credit card information over the phone to unknown personnel

Rewards
- Patients may take advantage of program benefits and earn rewards when they pay with their credit card
How To Provide A Patient Estimate

- **Basic**: Educated estimate or fixed amount
- **Moderate**: Generate a top 10 procedure list and keep it at the front desk
- **Advanced**: Generate an 80%-90% top receivable amount from your previous statements
- Use the data from electronic verification to accurately estimate out of pocket expense

- **Remember**: You are not required to provide an exact amount, just an estimate
- **Remember**: 52% of patients if given a good faith estimate at the point of care would provide a credit card on file

Work With Your Front Desk Staff

- Prepare scripts for your staff to learn
- Role play with them to become more familiar with scripts
- Reward staff for getting credit cards on file
  - i.e., a gift card to a favorite restaurant
- Set goals to benchmark their success
  - Try to get 10% of all patients then adjust up
Example of Simple Script: Front Desk

Front Desk:
Hi John. I see you owe a co-pay of $30 today. How would you like to pay for this portion of your visit? We accept cash, check, and of course credit and debit cards.

John:
credit card please

Front Desk:
Additionally, John, our office has listened to our patient’s request and is going green. We are trying to eliminate paper waste and as part of our efforts, we now require a credit card on file for your remaining balance. We estimate your portion of the bill not to exceed $250 and will only bill you up to the maximum allowable amount of $250. Once the insurance company generates the Estimate of Balance, we will go ahead and automatically bill the balance up to the agreed amount of $250.

Parting Thoughts

- You are not a bank and can not continue to shoulder the patient portion of their outstanding debt.
- Do not let your patients leave without communicating their responsibility to pay their potion and always ask to place their credit card on file for the outstanding balance.
- I can guarantee you this: If you ask 0% of your patients to place a credit card on file at the point of care, You will have ZERO patients say YES.
- Knowing what you know now, in my opinion, letting your patients leave with out committing to pay their portion is the equivalent to allowing them to medically shoplift at your practice.
Questions?

Contact:
Steven Kleinberg
skleinberg@cardchoice.com
Phone: 866.350.3200