Welcome to PMI’s Webinar Presentation

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

Meet the Presenter…

Regina Mixon Bates,
IRO, CPC, CPC-I, CMC,
CMOM, CMIS, TPA

On the topic:
HIPAA Security Essentials for Portable Devices
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.
Overview

- HIPAA regulations for portable devices
- Monitoring your staff for the usage of portable devices
- Laptops, Emails and Mobile devices- Allowed usage, security risks and penalties involved.
- Guidelines on ensuring proper controls – storing unencrypted PHI
- Learning from findings of HHS through various breaches.
- What policies and procedures need to be in place to reduce the risks of portable devices and systems?
- Protocols to be followed in the event of a breach- Who needs to be notified and timelines involved.
- Compliance issues to watch out for – when using e-mail and texting to communicate with each other
- Social Media
- Developing the policies that protect you and your patients
- Best practices to create a policy framework for security
HIPAA’s Impact on Our Work Environment

– Internal Compliance
  • Safeguards, audits and enforcement more important than ever

– Mobile Devices
  • Biggest Risk

– Patient/Family Interaction
  • Sending PHI via email

– Interaction with Colleagues/other health care providers, payors, agencies
  • Use appropriate safeguards

– Interaction with Business Partners
  • BA Agreements; Assess risk; HIPAA liability for actions of agents

– Social Media
  • Common and easy; another big risk

HIPAA Privacy/Security Rules

General Rule: Covered entity workforce members may only use or disclose protected health information as permitted under HIPAA

Which Includes:

Covered Entity- health care provider (individual and organization) that exchanges health information electronically in a transaction for which HHS has adopted standards

Protected Health Information- individually identifiable health information. Information is “individually identifiable” unless all 18 identifiers are removed and no actual knowledge that the health information could be used alone or in combination with other information to identify the individual.
HIPAA Privacy/Security Rules

• HIPAA Security Compliance Requirements:
  – Privacy Officer must be named
  – Privacy Policies and Procedures must be implemented and enforced
  – Workforce members must be trained
  – Unique designations must be identified (hybrid entities, affiliated covered entities)
  – Workforce members’ access to PHI must be designated
  – Other administrative/operational matters (e.g., notice of privacy practices, business associate agreements, accounting of disclosures, breach notification processes, risk assessments)

HIPAA Security/Privacy Rules

• Treatment, Payment, Healthcare Operations:
  – In general, Covered Entities may use/disclose PHI without a patient’s authorization for TPO
    • Treatment purposes
    • Payment purposes
    • Operations purposes
      – E.g., Case management, care coordination, peer review, training, legal, auditing, business management
HIPAA Security/Privacy Rules

- **Reasonable Safeguards**: Covered Entities must implement reasonable administrative, technical and physical safeguards to protect patient privacy:
  - Examples: HIPAA compliance policies; erasing hard drives before returning leased equipment with PHI; software installed on mobile devices, not discussing any PHI in a public place or where it could be overheard; using proper disposal methods; securing paper and electronic records.

The Hippocratic Oath and Doing No Harm In The Information Age

Does data security fall under your Hippocratic Oath responsibility?

- Some key principles of the modern Hippocratic Oath include:
  - Prevent and treat
  - Share medical knowledge
  - Ask questions
  - Remember patients are also people
  - *Preserve patient privacy*
HIPAA and Data Security

• From my day to day experience, HIPAA isn’t a major concern to many healthcare organizations and/or providers.
• It’s important to remember HIPAA does apply to all covered healthcare providers and organizations.
• The HIPAA Security Rule in particular contains some of the most important considerations for data security that can help you ensure your patient healthcare data stays private.

As patient records go digital, hacking health records for profit is becoming more prevalent.
• If patients have their medical records stolen due to your noncompliance with HIPAA, negligence with data security, or pure laziness, you will drastically and negatively affect their lives…not to mention your organization’s brand.
Biggest Risk Areas: Mobile Devices and Laptops

• In recent years the medical profession has become aware of the opportunities and challenges associated with mobile devices and Laptops.
• As technology has advanced, many hospitals and health care organizations have found it necessary to create their own policies in order to protect physicians and patients alike.

Biggest Risk Areas: Mobile Devices and Social Media

• Mobile Devices
  – It has become common for health care providers to communicate with patients using mobile devices or to access/relay PHI to other providers using mobile devices.
  – The unauthorized disclosure of ePHI is a big risk when using mobile devices because they are small, portable, highly visible, unlikely password protected, unlikely to have encrypted PHI, and likely to connect with Wi-Fi (further risking interception).
Statistics on Mobile Device Data Breaches

• Privacy Rights Clearinghouse and the Open Security Foundation: Analysis of data concluded that mislaid, stolen or discarded portable devices caused records with personally identifiable information of 80.7 million individuals to be breached.

• Approximately 40% of the breaches involving 500 or more individuals that were reported to HHS involved mobile devices.

Statistics on Mobile Device Data Breaches

• Today more than 99 percent of new malware is designed to target mobile devices

• The number of documented vulnerabilities for iOS Apple iPhone and iPads have increased 82 percent in recent years.

• Programs entice hackers even more, with the holy grail now being to infiltrate a company’s perimeter through mobile devices, either through social engineering scams that get access to company data through a mobile device, or just by sitting across the street and attacking the company’s WiFi through an infected mobile phone.
Statistics on Mobile Device Data Breaches

• Cross-platform Attacks:
  – Hacking Gangs are also using malware on PCs to infiltrate mobile phones in hybrid attacks on user’s banking accounts as well as EMR/EHR.
  – A piece of malware dropped on the user’s laptop can detect when the user is surfing his banking website and/or logging into your online EMR/HER systems.

Most Recent Breaches Reported

<table>
<thead>
<tr>
<th>Breach Report Results</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Subsequence Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDIeverywhere, Inc.</td>
<td>TX</td>
<td>Business Associate</td>
<td>1996</td>
<td>08/10/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
<td>Other</td>
</tr>
<tr>
<td>City of Pella</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>3400</td>
<td>08/03/2017</td>
<td>Hacking IT Incident</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Braun Dermatology &amp; Skin Cancer Center</td>
<td>DC</td>
<td>Healthcare Provider</td>
<td>1200</td>
<td>07/26/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>PixelS Surgery Associates of South Dakota</td>
<td>SD</td>
<td>Healthcare Provider</td>
<td>10223</td>
<td>07/27/2017</td>
<td>Hacking IT Incident</td>
<td>Network Server</td>
<td></td>
</tr>
<tr>
<td>Christine D. Coxon, APC &amp; Ann H. Hauser, MD P.A.</td>
<td>WA</td>
<td>Healthcare Provider</td>
<td>1500</td>
<td>07/02/2017</td>
<td>Hacking IT Incident</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Archiris, Inc.</td>
<td>IN</td>
<td>Healthcare Provider</td>
<td>15580</td>
<td>07/26/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>BlueCross BlueShield of TN, Inc.</td>
<td>TN</td>
<td>Health Plan</td>
<td>2117</td>
<td>07/26/2017</td>
<td>Unauthorized Access/ Disclosure</td>
<td>Paper/Files</td>
<td></td>
</tr>
<tr>
<td>The University of Vermont Medical Center</td>
<td>VT</td>
<td>Healthcare Provider</td>
<td>2300</td>
<td>07/25/2017</td>
<td>Hacking IT Incident</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Performance Physical Therapy and Wellness</td>
<td>CT</td>
<td>Healthcare Provider</td>
<td>571</td>
<td>07/25/2017</td>
<td>Unauthorized Access/ Disclosure</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Massachusetts Department of Public Health - Beth Israel Hospital</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>1170</td>
<td>07/25/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Kalida Health</td>
<td>NY</td>
<td>Healthcare Provider</td>
<td>2788</td>
<td>07/25/2017</td>
<td>Hacking IT Incident</td>
<td>Email</td>
<td></td>
</tr>
</tbody>
</table>
Other Data Breaches: Real World Cases

- $1.7M settlement with WellPoint for lack of administrative and technical safeguards surrounding an online application database. HHS also found a lack of sufficient policies and procedures. Breach affected over 600,000 individuals.

- $1.2M settlement with health plan for failing to erase ePHI stored on photocopiers before returning the machines to leasing agent. HHS also cited failure to implement policies and procedures, and failure to perform adequate risk assessment. Breach affected 344,579 individuals.

- $1.5M settlement with Mass. Provider who had unencrypted personal laptop stolen, contained PHI of more than 500 patients and research subjects, including patient prescription and clinical information.

Other Data Breaches: Real World Cases

- What happens when someone’s health information is illegally sold or fraudulently used?

**Bad credit:** Say an attacker sells your patient’s information to someone who racks up a bunch of unpaid medical bills, and opens up credit cards or other credit purchases under your patient’s name and social security number. This can seriously ruin the real patient’s credit. Bill collectors could come knocking. The victim could be denied a job due to bad credit and his insurability could be affected.
The Three Most Common Mobile Security Breaches

- **Device loss and theft** - The most common mobile “breach” is a staff member leaving a phone on the bus or in a taxi. This could allow access to company data but is more likely to lead to a flurry of expensive foreign calls and the loss of the device.
- Password protection helps limit the costs and dangers of losing a phone.
- If your business relies on sensitive data then think about software that allows remote control of phones so you can delete files or even disable the phone permanently. Failing that, make sure staff use passwords to protect their devices and consider further passwords for access to important applications.

- **Malware** - Even more malicious malware might take over a phone’s data connection, send spam emails, infect other devices on the network or even harvest passwords.
- This is an increasing problem as hackers begin to target mobile devices instead of desktop computers.
- Your staff must be as careful with downloading software as they are with laptops and desktop.
The Three Most Common Mobile Security Breaches

• **Unsecured networks** - Another danger is the rogue Wi-Fi network, set up by hackers to trap people logging on at airports, stations or coffee shops. This has been common in Asia but is less often used, so far, in North America or Europe.

• Either teach your staff to treat Wi-Fi access with caution – or give them unlimited data contracts so they don’t need to use such open access points.

Protocols - In The Event Of A Breach

• A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.

• An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors
Protocols - In The Event Of A Breach

• The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
• The unauthorized person who used the protected health information or to whom the disclosure was made;
• Whether the protected health information was actually acquired or viewed; and
• The extent to which the risk to the protected health information has been mitigated.

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media.

– Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.
Protocols - In The Event Of A Breach

• Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.

25

Protocols - In The Event Of A Breach

• These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include:
  – A brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).
Protocols - In The Event Of A Breach

• Covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out the breach form.

  – Breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Fines

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
Why Create (and follow) Mobile Device Polices

• HIPAA allows providers to communicate with patients and with other providers and to share ePHI using mobile devices as long as “reasonable safeguards” are applied when doing so.

• However, there is no specific requirement to have or not to have a social media/networking and mobile device policy.

• Given today’s environment of near-constant use of social media/networking, common access to PHI via mobile and highly portable devices, and where the vast majority of reported breaches stem from inappropriate safeguarding of ePHI, there is not any clear direction from the government which has resulted in a covered entity’s failure to implement the reasonable safeguards required under HIPAA.
Tips to Keep Your Device Safe

• Make sure your software is up-to-date
• Create Strong Passwords
  – Password should be long and not reference anything personal. They should include Upper and Lower case letter, numbers and characters.
  – For Example: OnthewaytotheMoonI8ightLunch@1oam (The number 0 become the letter “O”, the letter “O” becomes number 0, the letter e become the number 8)
• Avoid unencrypted public wireless networks.
  – Such Wi-Fi networks require no authentication or password to log into, so anyone can access them— including the bad guys

Tips to Keep Your Device Safe

• Don’t mess with the security settings.
  – Most of the default browser settings in Android, iPhone, and Blackberry phones are fairly secure out of the box.
• Paying to access a Wi-Fi network doesn’t mean it’s secure.
• URLs beginning with ‘https:’ are safer (but not foolproof).
• Use VPN.
  – If you have access to a VPN (virtual private network), use it. A VPN provides secure access to an organization’s network and allows you to get online behind a secure layer that protects your information.
Tips to Keep Your Device Safe

• Turn off cookies and autofill.
  – If your mobile device automatically enters passwords and login information into Websites you visit frequently, turn that feature off.

• Watch your apps!
  – You should be selective about the apps you download, particularly in the Android market, because “the Android app market is a little bit more open,” without the strict developer guidelines found in Apple’s App Store. Do some due diligence before downloading apps. Make sure that you trust the developer and have taken the time to review some of comments.

Mobile Device Policies

• Mobile Devices come in a variety of forms, processing capabilities, and wireless accessibility
  – Policies should include but are not limited to, laptop computers, smart phones, USB thumb drives, external hard drives, tablet computers (e.g., iPad, Motorola Xoom), and even e-readers like the Kindle or the Nook.
Mobile Device Policies

When writing your policies consider an annual agreement and signing of the organization's "rules of behavior" that would include:

- Requirements for password protection
- Lock-out features and specifications
- Appropriate use of texting
- Appropriate use of camera and video
- Appropriate use of sensitive information
- Alteration of factory defaults and operating systems (i.e., jail-breaking)
- Appropriate use of applications and conditions of downloading software
- Reservation of rights by the healthcare facility to examine the system for compliance and investigation of incidents
- Procedures during employee or contractor termination

Standards of Encryption

- Encrypting the data on your mobile device with a valid encryption process consistent with FIPS 140-2 can help you meet HHS Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
- The National Institute of Standards and Technology (NIST) has issued FIPS 140-2, Security Requirements for Cryptographic Modules.
HIPAA and Social Media

• **Social Media**
  – Staff and providers must not post or share information about patients that could potentially identify a patient

Statistics on Social Media

Data Breaches

• Research indicates that 35% of practicing physicians have received friend request from a patient or patient’s family member, and 16% of practicing physicians have visited an online profile of a patient or patient’s family member.
• Can work experiences be shared without violating patient privacy?
  – One meta-analysis of physician blogs found that nearly 17% included enough information about patients for them to be identified.
Social Media Data Breaches: Real World Example

Dr. Alexandra Thran, a 48 year old emergency room physician formerly at Westerly Hospital, Westerly, RI, posted a few notable cases she had seen in the ER on Facebook. She avoided using patient names or ages. Apparently, "unauthorized third parties" were able to determine one patient's identity from the post. When Dr. Thran learned of this, she immediately deleted her account.

Westerly Hospital concluded that Dr. Thran used her Facebook account "inappropriately." Both the hospital and Dr. Thran agreed that she had "no intention to reveal any confidential patient information."

The hospital's solution? Terminate Dr. Thran's hospital privileges.

The Rhode Island Board of Medical Licensure found Dr. Thran guilty of "unprofessional conduct." The Board handed out a $500 fine with instructions for her to attend a CME course dealing with physician-patient confidentiality issues.

Social Media Data Breaches: Real World Example

• Even acts of kindness can have complicated and unintended outcomes.
  – For example, a staff member who communicates with a patient or family through an online support community could set up scenarios for boundary issues and claims of care disparity.

• There are times when social media delivers unintended and unexpected outcomes that are wholly positive.
  – A woman and her mother leaving the Mayo Clinic stopped in the lobby to listen to an elderly couple playing the piano. The woman asked the couple to play another song and took a video of them with her phone. She posted the video to YouTube, where more than 7.5 million people have viewed it.
What Safeguards Should be in Place for Social Media Policies & Procedures?

- Restrict the types of information workforce members can share via social media
- Prohibit social media use during the work day
- Keep personal and professional sites separate
- Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practices published by the Federation of State Medical Boards


Where/How To Start Your Social Media Policy

- Policies surrounding social media should address the following issues, at minimum:
  - Who can access social media from the organization's network
  - Activation of network settings that allow only designated staff to access social media (e.g., marketing staff) to help protect privacy and confidentiality
  - Inappropriate uses of social media, either on the organization's network or a personal device (e.g., disparaging and defaming the employer, divulging trade secrets and other proprietary information, or violation of privacy rights)

Ramifications for inappropriate use, which should relate to existing company policy stating a violation can and may lead to discipline, up to and including termination
Where/How To Start Your Social Media Policy

- Responsibility of employees that witness inappropriate use
- Modification of other policies related to codes of conduct, disciplinary action, handbooks, e-media use, discrimination, or harassment
- Ensuring that staff members understand and acknowledge that they are not speaking on behalf of the organization when they post on their personal social media sites
- Responsibility of employees outside the realm of their employment (e.g., their actions on social media may put them at risk for civil liability)

Protecting Yourself from a Mobile Device or Social Medial HIPAA Breach

- Create (and follow) HIPAA Privacy and Security policies specifically addressing the exchange of PHI using mobile devices and social media
- Ensure all staff and personnel receive copies of your HIPAA Privacy and Security Manuals, including policies relating to mobile devices and social media
Protecting Yourself from a Mobile Device or Social Media HIPAA Breach

• Impose appropriate safeguards on use of both mobile devices and social media
• Consider annual testing for employees
• Audit to ensure staff and personnel with access to ePHI on mobile devices have implemented the appropriate safeguards

Best Practices Moving Forward

• **Data security is fundamental**
  — Conduct data security review often
• **Plan ahead**
  — Create a plan to review your data security status and policies and create routine processes to access, handle and store the data safely as well as archive unneeded data.
• **Know what data you have**
  — Know what data you have and what levels of protection are required to keep the data both confidential and safe from loss
• **Scale down the data**
  — Keep only the data you need for routine current business, safely archive or destroy older data
• **Lock up!**
  — Physical security is the key to safe and confidential computing. All the passwords in the world won’t get your laptop back if the computer itself is stolen. Back up the data to a safe place in the event of loss.
Best Practices Moving Forward

- Require providers to register their mobile devices if Bring Your Own Device ("BYOD") is allowed
- Require use of passwords or other use authentication
- Install and enable encryption for ePHI including text or SMS messages
- Install and activate remote wiping and/or remote disabling ability
- Disable and do not install or use file sharing applications
- Install and enable a firewall
- Install and enable security software (and update it)
- Do not share ePHI over public Wi-Fi
- Delete all stored ePHI before discarding or reusing the mobile device.

Questions?

HIPAA Background Information
HIPAA Statutory and Regulatory Background Information

- Aug. 8, 1996- HIPAA signed into law
- Feb. 17, 2009- ARRA HITECH signed into law
- Aug. 24, 2009- HITECH Breach Notification Interim Final Rule (effective Sept. 23, 2009)
- July 14, 2010- Proposed Regulations to implement a number of HITECH’s Privacy, Security and Enforcement provisions

HIPAA: Background Information

- The Privacy Rule: addresses the Use and Disclosure of PHI by Covered Entities and Business Associates and establishes individuals’ privacy rights to understand and control how their health information is accessed, used or disclosed.
- The Security Rule: establishes requirements for protecting electronic PHI.
- The Enforcement Rule: establishes both civil money penalties ("CMPs") and federal criminal penalties, as well as procedures for agency enforcement and factors for assessing CMPs.
- The Electronic Transactions and Code Sets Rules: HIPAA adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data (claims and encounter information, payment and remittance advice, claims status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment). Certain standards must be used when conducting a standard transaction electronically. HIPAA also adopted specific code sets for diagnoses and procedures to be used in all transactions (HCPCS,CPT-4, CDT, ICD-9, ICD-10 and NDC).
- The Breach Notification Rule: requires notification to HHS, the individual and potentially the media following a Breach of Unsecured PHI.
We offer services in the following areas of Practice Management and Operation:

- Practice Assessment, Education and Management Oversight
- New Practice Set-up
- Baseline Chart Audits
- One-on-one Physician Training/Education
- MACRA: MIPS and APM’s Consulting Services
- IRO (Government Approved Independent Review Organization) Services
- HIPAA, OSHA, and OIG Compliance Documentation, Planning, and Implementation
- Physicians and Midlevel Nationwide Placement

We also offer a series of seminars for Physicians and Staff
Thank you for attending!!

Visit us online: www.ppsosgroup.com

You can contact us at: info@ppsosgroup.com

770.333.9405

FIND US ON

Facebook, LinkedIn, Twitter, Fix my Practice Blog and YouTube:

https://www.facebook.com/pages/The-Physicians-Practice-SOS-Group/280246238670673
LinkedIn: The Physicians Practice S.O.S. Group
https://twitter.com/PPSOSGRP
http://www.youtube.com/user/ppsosgroup

Taking the Business of Medicine to the Next Level