TODAY’S SESSION

1. A quick recap of HIPAA: then to now
2. Self-Assessment: Are you up-to-date with current HIPAA requirements?
3. Enforcement is increasing: Lessons learned from recent cases

HIPAA COMPONENTS

Signed into law by President Clinton on 8/22/1996

   - Provides privacy protections for written, verbal and electronic health information
   - Created federal Rights for patients regarding their personal health information

   - Provides for the security of information in electronic form (emails, claims transmittal info, electronic medical records)

+ American Recovery & Reinvestment Act’s HITECH Act (2009)
+ Strengthened enforcement, increased penalties for non-compliance, mandated reporting of “breaches” of health information by providers, required AUDITS
WHAT IS ‘HITECH’?

- HITECH = Health Information Technology for Economic and Clinical Health Act.
- What changed?
  + Fines increased substantially
  + Office for Civil Rights now required to audit entities for compliance with HIPAA
  + State Attorneys General can now bring actions under HIPAA
  + Notification to individuals & federal gov’t required when breach of patient information occurs (sometimes media as well)

WHY UPDATE YOUR HIPAA?

- Final Rule changes required this as of 9/2013
- 118,939 complaint investigations since April 2003
- 25 enforcement actions included Resolution Agreements with settlement amounts owed (24) or a Civil Money Penalty being owed to feds (1)
  + Ranging from $50K to $4.8M
- Enforcement statistics are increasing
  + Making examples of entities through enforcement actions – small physician practices, government entities, health plans

OCR ENFORCEMENT ACTIONS

<table>
<thead>
<tr>
<th>Year</th>
<th>No Violation</th>
<th>Resolved After Intake</th>
<th>Violation Found</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>24%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**HISTORY OF AUDIT PROGRAM**

- **ARRA** requires HHS to audit Covered Entity (CE) & Business Associate (BA) compliance with Privacy, Security and Breach Notification Rules
- 1st Round of “PILOT” audits finalized December 2012
- 115 CEs audited (no BAs)
- In-person audits performed by contractor KPMG
- **VERY BROAD FOCUS**
  - Compliance with ALL of HIPAA assessed
  - 169 requirements assessed (audit protocol available on OCR website*)
- No enforcement actions as a result (yet) only “technical assistance” provided where deficiencies found

**KPMG AUDIT FINDINGS:**

- Physician practices LEAST compliant of all groups audited
  - Security Risk Analysis NOT done properly or at all by majority (80%) of Practices audited
    - Risk analysis
    - Media disposal
    - Audit controls
    - Monitoring
  - Privacy Rule failings:
    - Notice of privacy practices
    - Access rights of individuals
    - Minimum necessary
    - Authorization provisions

**WHAT HAS HAPPENED SINCE “PILOT” AUDITS**

- ‘After Action Report’
- In March 2013 HHS sent Audit Evaluation Survey to 115 audited CEs with purpose of:
  - Measuring effect of Audit program on CEs
  - Gauging attitudes towards the document request, communications received, on-site visit, audit-report findings and recommendations, etc.
  - Obtaining estimates of costs incurred by CEs in time and money spent responding to audit
  - Seeking feedback on effect of Audit program on day-to-day business operations
  - Assessing whether improvements in HIPAA compliance were achieved as a result of the Audit program
WHAT TO EXPECT WITH NEXT ROUND OF AUDITS

- Summer 2015 – OCR is working with other government agencies to issue pre-audit surveys “soon”.
- Approx. 200 entities audited – CEs (150) and BAs (50)
- Likely 15-day timeframe to respond once notified!
- Audits will be more focused than Pilot Round
  + Security: Risk analysis and risk management
  + Breach: Content and timing
  + Privacy: Notice and access
- Mainly “desk audit” – no auditor on site, at least initially

ARE YOU UP-TO-DATE WITH CURRENT HIPAA REQUIREMENTS?

NEW HIGH RISK AREAS UNDER HITECH

1. Incident (Breach) Investigation, Mitigation and Notification
2. Business Associates
3. Patients’ Rights
4. Marketing and “Sale” of PHI
5. Other goodies
HIGH RISK AREA #1: BREACH NOTIFICATION

- A breach under HITECH is:
  - any unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the PHI

- You must assume that an incident that violates the Privacy Rule is a reportable breach to the affected individuals, HHS/OCR and potentially the media (if >500 patients in one state/jurisdiction)

WHAT TO DO ABOUT BREACHES

- You may begin notification to patients, federal government and media, if necessary, OR

- Use 4-factor risk assessment to see if you can determine there is A LOW PROBABILITY THAT THE PHI WAS COMPROMISED – if so, reporting is not required by HIPAA

- Note: reporting may still be required under state breach notification laws

4 FACTORS OF RISK ASSESSMENT

- TYPE?
  - The nature and extent of the PHI involved
  - Consider types of identifiers and likelihood of re-identification

- WHO?
  - The unauthorized person who used the PHI or to whom the disclosure was made

- HOW OR HOW MUCH?
  - Whether the PHI was actually acquired or viewed

- MITIGATION!
  - The extent to which the risk to the PHI has been mitigated

Note: reporting may still be required under state breach notification laws
REPORTING A BREACH - REMINDER

- HITECH requires Your Practice to REPORT to:
  + The patient(s) affected
  + The federal government
  + The media (sometimes)

- 500 or more clients’ data = immediate notification to the feds and to prominent media outlets

- Most important – document your risk assessment thoroughly for those breaches you determine to be non-reportable

  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

WHAT TO DO - BREACHES

- Have an incident response policy that involves security, privacy, legal, facilities security, etc. – anyone who needs to be involved when an incident occurs

- Have a breach notification policy – what does it look like when you have a reportable breach?
  + Who gets notified
  + Who notifies
  + Who works with the press, etc.

- Document, document, document

- TRAIN YOUR WORKFORCE MEMBERS ON IT

HIGH RISK AREA #2: BUSINESS ASSOCIATES

- Your BAs (vendors who touch your Practice PHI) are now directly liable to the federal government (OCR) for compliance with HIPAA

- Definition of BAs expanded to include any entity which, on behalf of a CE, creates, receives maintains, or transmits PHI for a function or activity regulated by the Privacy Rule

- Subcontractors of your BAs now also BAs if they touch your Practice PHI

- You must ensure you are entering into compliant BA Agreements with ALL your BAs
  + Note: downstream BAs responsible for entering into BAs with subcontractors
**HOW TO AUDIT? BUSINESS ASSOCIATES**

- Jury is still out on how much oversight of your BAs is required
  - HIPAA doesn’t require any specific monitoring - only to terminate the contract (if possible) if you know they are violating HIPAA
- Due diligence up front (before hiring them) certainly recommended
- Consider survey of all BAs or random audits of more high-risk BAs (i.e. those who have lots of your PHI/sensitive PHI) to ensure they understand HIPAA compliance requirements

**HIGH RISK AREA #3: PATIENTS’ RIGHTS UNDER HIPAA**

1. **Access**, copy, and inspect . . .
2. **Amendment** . . .
3. **Accounting of certain disclosures** . . .
4. **Request privacy protections** . . .
5. **Complain** about alleged violations . . .
6. **Notified** when a breach occurs . . .
   . . . of their healthcare information.

**PATIENTS’ RIGHT:**

1. Right to **access**, copy, and inspect their healthcare information
   - Know what your Designated Record Set (DRS) is and document it in a policy
   - Provide access to the DRS when requested by your Patients
   - SELF-AUDIT: “Request for Access to and/or Obtaining a Copy of PHI”
   - SELF-AUDIT: Policy on Charges (if any) for Copies of Medical Records
   - SELF-AUDIT: Provision of Medical Record In Electronic Format
PATIENTS’ RIGHT:

2. Right to request an amendment to their healthcare information
   + Provide amendment to the DRS when requested by your Patients
   + Certain circumstances allow you to deny the request

   □ SELF-AUDIT: Policy on Handling Requests for Amendment of PHI

PATIENTS’ RIGHT:

3. Right to obtain an accounting of certain disclosures of their healthcare information
   (awaiting Final Guidance on HITECH changes)
   Currently does not include disclosures for treatment, payment or health care operations (TPO); can go back 6 years. (HITECH law required TPO disclosures from electronic medical record; may go back 3 years; still awaiting final guidance on these changes.)

   □ SELF-AUDIT: Policy on Keeping Log of Disclosures of a Patient's Record

PATIENTS’ RIGHT:

4. Right to request privacy protections for PHI
   + Patient has right to request this; Practice does not have to agree but must respond to Patient stating so
   + Make sure you train on and operationalize the new Patient Right to restrict PHI from going to an insurance company if the Patient pays for the service out of pocket and in full at the time of service

   □ SELF-AUDIT: Policy on Restriction on Uses/Disclosures of PHI
   □ SELF-AUDIT: Request for Alternative Means of Communication
   □ SELF-AUDIT: Request to Send Patient Information Directly to a 3rd Party
PATIENTS' RIGHT:

5. Right to complain about alleged violations of the regulations and the entity's own information policies

SELF-AUDIT: Privacy Rights Complaint Form

PATIENTS' RIGHT:

6. The right to be notified when a breach of their unsecured PHI occurs

This must now be stated in your Notice of Privacy Practices!

HIGH RISK AREA #4:
MARKETING AND ‘SALE’ OF PHI

- Marketing now requires authorization from patients if you receive payment from a 3rd party to send a communication to the patient encouraging them to use/purchase a product or service
  - Even if the communication is for health care operations or treatment purposes
  - Limited exceptions exist such as for prescription refill reminders
- You may not “sell” your patients' PHI to a third party without asking the patients if you may do so and getting their written authorization
  - Exceptions exist (i.e. for research purposes if certain conditions are met)
### OTHER GOODIES . . .

**WHAT CHANGED – DECEASED PATIENTS**

- May now share decedent’s PHI with family member, close friend or other individual involved in individual’s treatment or payment before his/her death
  - State law isn’t very friendly in this regard as most Power of Attorneys/Medical POAs expire upon death
  - Many entities were previously left not being able to discuss deceased patient with family members they had been dealing with prior to patient’s death
  - Will most likely use this when a family member calls to make sure a bill gets paid
- Also – Definition of PHI no longer includes information on individuals dead more than 50 years (HIPAA “FUN FACT”)
  - Mostly helpful to researchers

### FRIENDLY REMINDER - STAFF TRAINING

- **Must train:**
  - All workforce members on P&Ps regarding PHI safeguards in order for them to carry out their duties
  - Each new workforce member within a reasonable period of time after he/she joins the entity
  - Each workforce member whose functions are affected by material change in policies or procedures – within a reasonable period of time

### FRIENDLY REMINDER – MINIMUM NECESSARY POLICY

- **Limit any use or disclosure of PHI to the minimum necessary to accomplish the intended purpose**
- Practice workforce members should only have access to those systems that they need to in order to do their job!
- **WHAT TO DO:**
  - Have a policy/policies for routine uses and disclosures of PHI that explains what workforce members should do/discard/etc. when handling PHI
  - Train members to handle PHI specific to their daily job functions on a NEED TO KNOW basis only!
FRIENDLY REMINDER - SANCTIONS

- Have a policy and apply it to workforce members CONSISTENTLY who violate your P&Ps (receptionists to providers)
- Must train workforce to understand sanctions may apply
- WHAT TO DO:
  + Apply sanctions consistently
  + Document all sanctions taken!
- One of the first things you may be asked for in an audit!

FRIENDLY REMINDER - SOCIAL MEDIA AND YOUR WORKFORCE

- KEY: Staff CANNOT take and post pictures, videos, comments, stories, etc. (PHI) of their work areas, patients, patients’ families, injuries, tattoos, surgeries, etc. WITHOUT WRITTEN AUTHORIZATION FROM THE PATIENTS THEMSELVES
- Having no social media policy is not OK in today’s new world
  + Tell your staff what they can and cannot do and what your expectations are

Security Rule Design

- Administrative Safeguards 23 Specifications
  - 12 Required
  - 11 Addressable

- Physical Safeguards 16 Specifications
  - 5 Required
  - 5 Addressable

- Technical Safeguards 9 Specifications
  - 4 Required
  - 5 Addressable
STANDARDS - ADMINISTRATIVE

- Security management process
  + Risk analysis
  + Risk management
  + Sanction policy
  + Information asset activity review
- Assigned security responsibility
- Workforce security
  + Authorization and/or supervision
  + Workforce clearance procedure
  + Termination procedures
- Information access management
  + Isolating health care clearinghouse functions
  + Access establishment and modification
- Security awareness and training
  + Security reminders
  + Protection from malicious software
  + Login monitoring
  + Password management
- Security incident procedures
  + Response and reporting
- Contingency plan
  + Disaster recovery plan
  + Emergency mode operations plan
  + Applications and data criticality analysis
- Evaluation
  + Business associate contracts and other arrangements
    + Written contract or other arrangement

STANDARDS - PHYSICAL

- Facility Access Controls
  + Contingency operations
  + Facility security plan
  + Access control and validation procedures
  + Maintenance records
- Workstation Use
- Workstation Security
- Data Storage Security
- Device and Media Controls
  + Disposal
  + Media re-use
  + Accountability
  + Data backup and storage

STANDARDS - TECHNICAL

- Access Control
  + Unique user identification
  + Emergency access procedure
  + Automatic logoff
  + Encryption and decryption
- Audit Controls
- Integrity
  + Mechanism to authenticate EPHI
- Person or Entity Authentication
- Transmission Security
  + Integrity controls
  + Encryption
MISCELLANEOUS

- Policies and Procedures
  - Implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications and other requirements

- Documentation Requirements
  - Maintain P&P in written form
  - Maintain written documentation of any required action, activity or assessment
  - Make certain that workforce members who have responsibility for implementing security have access to P&P, etc.
  - Review periodically
  - Update in response to environmental or operational changes that affect security of EPHI

Keep it all for 6 years from date of creation or date last in effect (whichever is later)

HIPAA SECURITY RULE

- Security program should be flexible, scalable based on the size and complexity of your organization

Examples of general Policies needed:
- Security Officer Roles and Responsibilities
- Protection of Electronic Documents containing PHI
- Password Management
- Facility Security
- Further customization based on your practice’s Risk Assessment is required by your Security Officer

MORE POLICIES NEEDED - ACCESS TO SYSTEMS CONTAINING PHI

- Electronic User Access Agreement
  - Have employees sign one of these yearly acknowledging they understand your workstation policies

- Workforce Member Acknowledgment of Training
  - Make sure employee trained on Privacy and Security policies and procedures
### ANOTHER ‘MUST HAVE’ POLICY - MOBILE DEVICES

- Make sure your workforce knows if they can use their own device to access Practice information or not.
  - If they can, have them sign an End User Agreement specific to using their own device to access Practice PHI.
- Consider the use of FIND MY PHONE and REMOTE WIPE capabilities – install the apps!
- Notify your Practice’s Security Officer immediately if a device is lost or stolen!

### FRIENDLY REMINDER - STRENGTH OF PASSWORDS

<table>
<thead>
<tr>
<th>Password:</th>
<th>Password:</th>
</tr>
</thead>
<tbody>
<tr>
<td>6cH@pW</td>
<td>8cH@RpW!</td>
</tr>
<tr>
<td>takes 8 seconds to crack using tools available on internet</td>
<td>takes 2 1/4 years to crack using tools available on internet</td>
</tr>
</tbody>
</table>

### FRIENDLY REMINDER - WORKSTATION USE

- **Automatically employed** safeguards
  - Automatic screensaver after 15 minutes
  - No "admin rights" except for specific, authorized individuals
  - Employees need to know who and how to notify when something happens!
  - Warning screen reminding users of understanding of appropriate work station use upon log-in each time
  - Security banners
FRIENDLY REMINDER - WORKSTATION USE

- **Employee responsibility** safeguards
  + Minimize PHI when possible
  + No use of workstation another user has logged onto, no use of another user’s ID/password
  + Lock computer when leaving for any period of time
  + Log off at conclusion of each day
  + BE AWARE OF YOUR ENVIRONMENT!

FRIENDLY REMINDER - EMAILING

- Confirm address before sending
- Confidentiality clause attached to all externally sent emails
- **BE VERY CAREFUL WITH SOCIAL SECURITY NUMBERS**
  - If email to many patients all at once – use "BCC" to protect privacy of email addresses!
  - Limit amount of information to minimum necessary especially in subject line!
  - When sending externally – **ENCRYPT**

E-mailing unencrypted PHI:

- Encryption of emails containing PHI is the standard and expected by OCR!
- However, Practice may send PHI in an unencrypted email if:
  1) Patient has been notified by Practice that there may be risk in sending PHI unsecured
  2) Patient still wants to receive PHI via unencrypted email
  3) Practice documents conversation with patients of risk to their PHI
  4) HHS: patient “has the right to receive PHI that way”
FRIENDLY REMINDER – VISITOR POLICY

- Visitors are required to sign-in and his/her visit validated before accessing the non-visitor areas of Your Practice’s business office
- Maintains a “Visitor Log”
- Vendor or system maintenance personnel are to be escorted and supervised while working in areas where PHI is stored within business office
- Doors are to be locked at all times when the business office is unattended
  + Please be alert & suspicious if you see someone you don’t know in your office area.

ACCESSING YOUR PRACTICE’S PHI FROM REMOTE LOCATIONS POLICY

- Providers may only log in to systems and portals for which they have authority and valid access credentials from the appropriate authorities (i.e. hospital systems)
- Any PHI (i.e. email) that is accessed from a mobile device may not be saved to that device
- Smart phone users must be sure to close connections to email and other system/portal containing PHI immediately when they are finished using the system/portal
- All mobile devices should have a password!
- If a provider is using his/her own personal phone to access Practice email, no other family members or others are allowed to access that personal device for any reason

WHATEVER YOU DO...

- Don’t forget to do and update routinely your Practice’s Security Risk Assessment
  + Guidances and resources abound – even for providers
    × http://www.healthit.gov/providers-professionals/security-risk-assessment
  + Complexity can vary with the size and resources of your Practice. Being small or not having enough money to hire it out is NOT an excuse!
OBJECTIVE 3:

LESSONS LEARNED FROM RECENT CASES

St. Elizabeth’s Medical Center in Massachusetts

- Complaint submitted to OCR that its employees were using an unsecured internet-based document sharing application to store documents containing electronic PHI
- No risk assessment performed on this operational practice
- Hospital failed to identify the incident or respond to it
- “Organizations must pay particular attention to HIPAA’s requirements when using internet-based document-sharing applications” – OCR Director Jocelyn Samuels

- Dropbox, Google Drive, SkyDrive, Minus, YouSendIt, RapidShare, ShareFile, Box, SugarSync, etc.

$218,400 Settlement!

Anchorage Community Mental Health Services (ACMHS)

- submitted breach report which affected 2,743 individuals
- 5-facility nonprofit organization providing behavioral health services to children, adults and families
- Breach occurred due to malware compromising the security of ACMHS’ IT resources
- ACMHS had adopted sample Security Rule policies and procedures in 2005, but didn’t follow them and “failed to identify and address basic risks, such as not regularly updating IT resources with available patches and running outdated, unsupported software.”
- No risk assessment done for very basic security risks

$150,000 Settlement
“Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis. This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks.”

- OCR Director Jocelyn Samuels

**FIRST ENFORCEMENT ACTION UNDER OCR NEW DIRECTOR - ACMHS**

Cornell Prescription Pharmacy, Denver, CO

- Small neighborhood pharmacy
- Local Denver news outlet found an unlocked, open container on Cornell’s premises containing PHI not shredded or secured in any other manner
- No policies and procedures, no training, etc.
- “Regardless of size, organizations cannot abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons” – OCR Director Jocelyn Samuels

**WATCh OUT FOR THE BASICS Too!**

Phoenix Cardiac Surgery

- Online patient schedule (unsecured) in "cloud"; could be seen by others through simple web search
- E-mails from internet site to staff that contained ePHI not protected (encrypted)
- Like many private practices:
  - NO implementation of HIPAA Privacy (since 2003)
  - NO implementation of HIPAA Security (since 2005)
  - Few P&Ps, no training, no security official, no security risk analysis, no business associate agreements

**PROViders ARE NOT IMMUNE!**

- Settlement! $125,000
- Settlement! $100,000
CONCENTRA PAYS $1.725M FOR STOLEN LAPTOP

- Unencrypted laptop stolen from physical therapy center in Springfield, Missouri
- No documentation as to why encryption was not "reasonable and appropriate" on the laptop; ALTERNATIVELY did not implement other safeguards instead of encryption based on its Security Risk Assessment
- No Policies and Procedures to prevent, detect, contain and correct security violations stolen from physical therapy center in Springfield MO

Covered entities must understand that mobile device security is their obligation.”

Our message to these organizations is simple: encryption is your best defense against these incidents.” - Susan McAndrew, Deputy director of Health Information Privacy, OCR

$4.8 M SETTLEMENT PAID BY 2 HOSPITALS FOR LACK OF TECHNICAL SAFEGUARDS

- Physician employed by two different hospital systems, who developed applications for both hospitals, attempted to deactivate personally-owned computer server on the network of one hospital that contained patient PHI
- This left PHI accessible on internet search engines
- Incident reported to OCR via family complaint that deceased individual’s information was out on the internet
- No accurate assessment by hospitals to identify all systems that access PHI on hospital network
- No security risk management plan in place to mitigate these types of risks

$4.8 M SETTLEMENT PAID BY 2 HOSPITALS FOR LACK OF TECHNICAL SAFEGUARDS

- Physician employed by two different hospital systems, who developed applications for both hospitals, attempted to deactivate personally-owned computer server on the network of one hospital that contained patient PHI
- This left PHI accessible on internet search engines
- Incident reported to OCR via family complaint that deceased individual’s information was out on the internet
- No accurate assessment by hospitals to identify all systems that access PHI on hospital network
- No security risk management plan in place to mitigate these types of risks

HIPAA ENFORCEMENT

- Civil Actions
  + By: Office for Civil Rights of Dept. of Health and Human Services
  + By: State Attorney’s General Office (HITECH)
  + Types: Civil Money Penalties
  + Settlements
  + Maximum now $1.5 million per violation/per year

- Criminal Actions
  + By U.S. Department Of Justice (DOJ)
  + Investigated by FBI
  + Against covered entities
  + Against individuals

- Maximum now $1.5 million per violation/per year

Penalties for violation:
- Civil Money Penalties: up to $50K fine & imprisonment up to 1 year
- Criminal Penalties: up to 10 years & up to $250K fine

Penalties for violation:
- Civil Money Penalties: up to $50K fine & imprisonment up to 1 year
- Criminal Penalties: up to 10 years & up to $250K fine
**CIVIL MONETARY PENALTY STRUCTURE**

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000 - $50,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

All such violations of identical provision in Calendar Year:

<table>
<thead>
<tr>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1.5 million</td>
</tr>
</tbody>
</table>

**SELF-AUDIT: MALPRACTICE COVERAGE**

- Make sure you're covered for a HIPAA violation
- Might require a 'rider' to your existing policy
  + For example, “Breach” rider
- Might require a policy in the physician name (if current policy in Group name) or vice versa
- Consider cyber liability insurance policy – emerging field of liability insurance

**GENERAL RESOURCES:**

- Federal Register for the Final Omnibus Rule
  + [https://www.federalregister.gov/](https://www.federalregister.gov/)
- Office for Civil Rights
  + [www.hhs.gov/ocr/](http://www.hhs.gov/ocr/)
- Office of National Coordinator
  + [www.healthit.gov](http://www.healthit.gov)
SELF-AUDIT RESOURCES

- [ ] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
  - Pilot Audit protocol – not updated to reflect Final Rule changes, but a great start
- [ ] Privacy, Breach and Security Rule Standards from Final Rule
  - Privacy Rule – 56 Standards
  - Breach Rule – 4 Standards
  - Security Rule - 18 Standards

HIPAA Security Rule Resources

- [ ] Free Security Risk Assessment tool from OCR:

Caution!: Lacks identification of threats and vulnerabilities of Practice, listing of security controls already in place AND ranking of risks so that Practice knows what to target first.

So – be sure to add these

Marcia Brauchler, MPH, FACMPE, CPC, CPC-H, CPC-I, CPHQ
Physicians’ Ally, Inc.
101 W. County Line Rd. #230
Littleton, CO 80129
(303) 586-9390
Fax: (303) 586-9393
Cell: (303) 250-3236
mbrauchler@physicians-ally.com