HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

The "Stark" Reality of Managing Compliance

Session 4, March 5, 2018

Leslie M. Cumber, Esq., Gordon Feinblatt LLC

Amy S. Leopard, Esq., FHIMSS, Bradley, Nashville

COMMITMENT

www.himssconference.org

#HIMSS18

Speaker Introduction

Leslie M. Cumber, Esq.

GORDON·FEINBLATT LLC
ATTORNEYS AT LAW

Amy S. Leopard, Esq., FHIMSS

Bradley

Conflict of Interest

Leslie M. Cumber, Esq.

Has no real or apparent conflicts of interest to report.

Amy S. Leopard, Esq., FHIMSS

Has no real or apparent conflicts of interest to report.

Disclaimers

- Nothing in this presentation constitutes legal advice. Consult with a lawyer before making decisions that may implicate legal requirements.

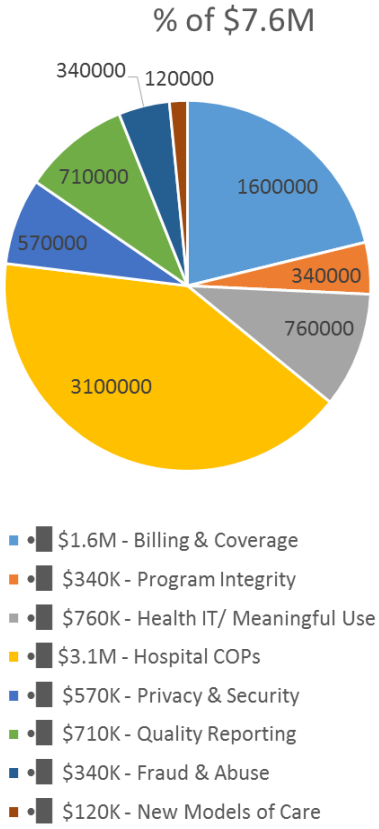
Agenda

- Agency roles in compliance
- Compliance issues in Health IT – how and why they arise
  - Medicare audits, false claims violations, privacy and security
- Implementing an effective compliance program given available resources

Learning Objectives

1. Apply privacy, security and compliance concepts in the face of the advancing wave of health IT
2. Identify how to implement and maintain a culture of compliance, making it an everyday occurrence and not a periodic burden
3. Recognize relevant areas of compliance for your setting and design effective systems to address them

The Problem

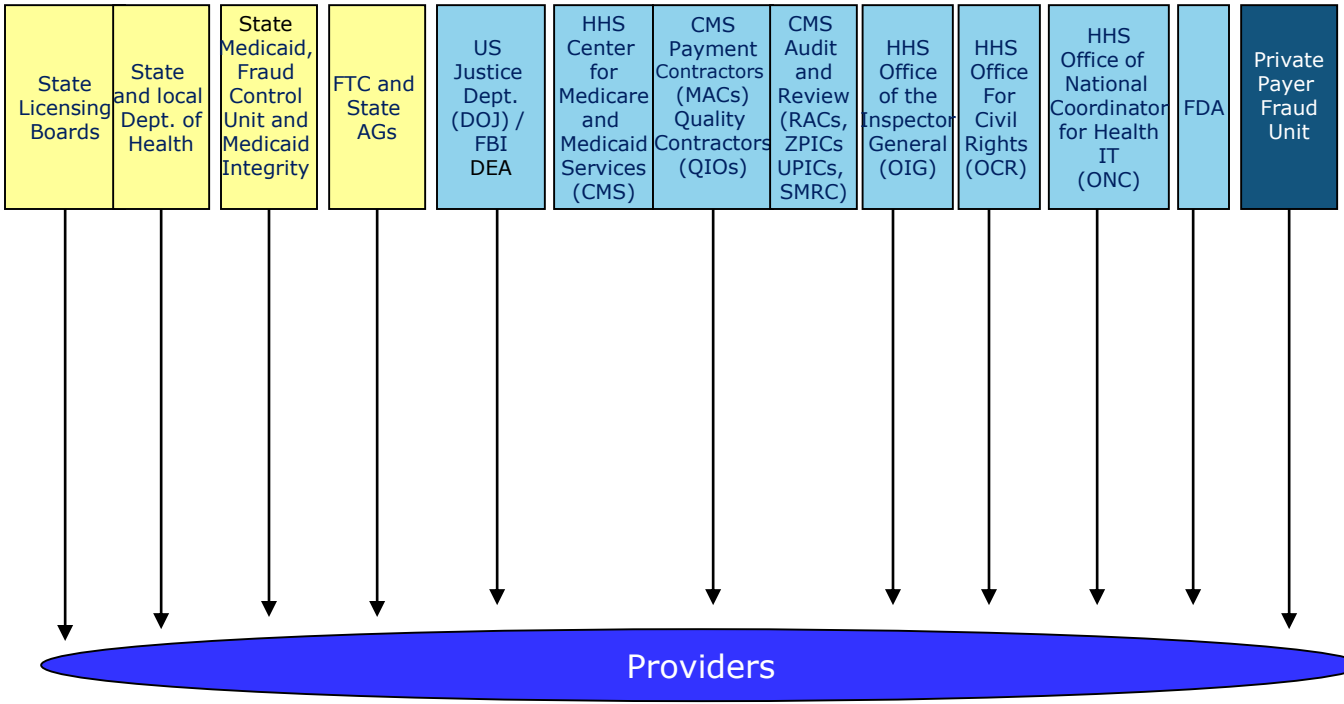


HIT falls within 27% of Hospital Regulatory Burden

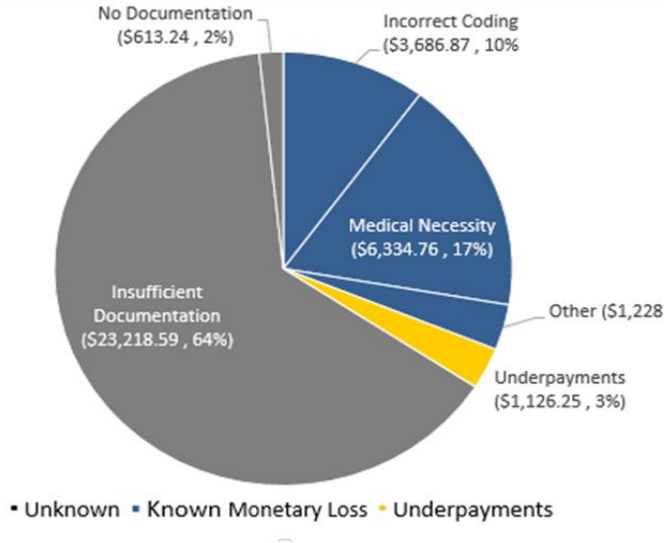
- $3.1M - Hospital Conditions of Participation (COPs)
- $1.6M - Billing & Coverage
- $760K - Health IT/ Meaningful Use
- $710K - Quality Reporting
- $570K - Privacy & Security
- $340K - Fraud & Abuse
- $340K - Program Integrity
- $120K - New Models of Care

Source: *AHA Report: Regulatory Overload – Accessing Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers (10/17).*

Who are the players?



Documentation Errors = Improper Medicare Payments



Most Medicare FFS improper payments result from **documentation errors.**

CMS cannot determine whether the items or services were

- medically necessary
- billed at the appropriate level
- actually provided

Kim Brandt, CMS Principal Deputy Administrator for Operations

https://blog.cms.gov/2017/11/15/cmss-2017-medicare-fee-for-service-improper-payment-rate-is-below-10-percent/

Figure: FY 2017 Medicare FFS Improper Payments (Millions) and % of Improper Payments by Monetary Loss and Type of Error

EHR Technology Concerns

- "…troubling indications providers are using technology to game the system, possibly to obtain payments to which they are not entitled.
- **False documentation of care is not just bad patient care; it's illegal . . .**
- A patient's care information must be verified individually to ensure accuracy: *it cannot be cut and pasted from a different record of the patient*, which risks medical errors as well as overpayments."

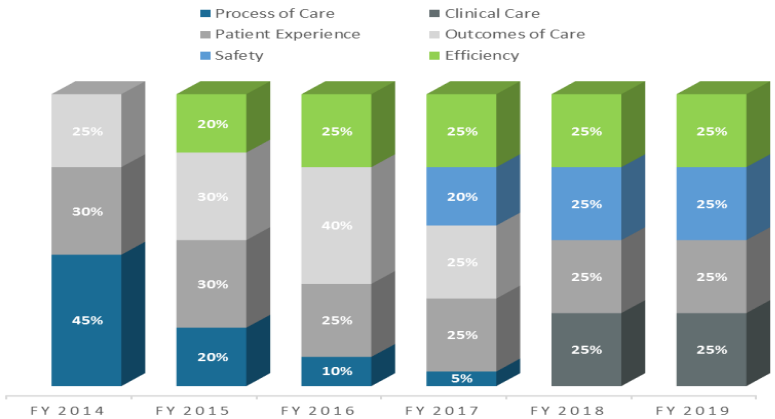
Source: *Joint Letter from HHS and U.S. Attorney General, Sept. 2012*
www.modernhealthcare.com/Assets/pdf/CH82990924.PDF

- Concerns besides Cloning/Improper Copy Paste :
  - Drop Down Menus
  - Prepopulated Templates and Default Settings
  - Pull forward
  - Integrity of Amendments
  - Authorship Integrity (multiple authors, shared passwords, unlicensed provider entries)
  - Note Fatigue
  - Late Entries

See: *Integrity of the Healthcare Record: AHIMA Best Practices for EHR Documentation* (2013)

Quality Reporting as a Medicare Payment Issue

Hospital Value-Based Purchasing Performance Scoring



Includes Value-Based Purchasing Program, Hospital Readmissions Reduction Program, and Hospital-Acquired Conditions Program.

Mandatory Risk Programs = 6% of Hospital Revenue at Risk

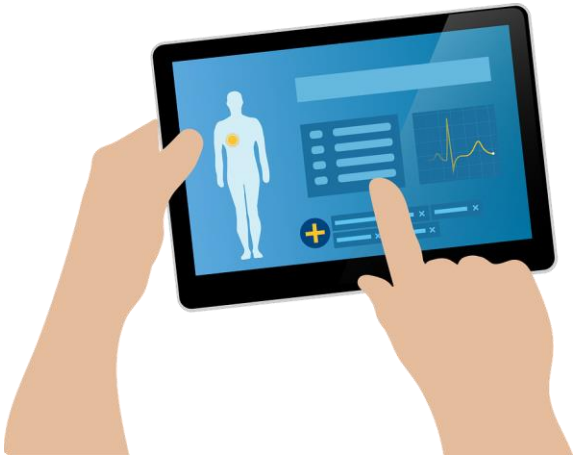
Hospital Acquired Condition Penalties

Readmission Penalties

- **Quality data must be accurate**
- **Significant interplay between compliance and quality reporting as providers submit data on quality, severity, mortality, LOS, readmissions, continuum of care, that are material to Medicare payment.**

False Claims Act Liability extends to those who

- Knowingly*
  - Present (or cause to be presented) a false or fraudulent claim for payment
  - Make or use (or cause to be made or used) a false record or statement material to a false or fraudulent claim
  - Conceals or knowingly and improperly avoids or decreases an obligation to federal government
- Or conspire to do so . . .
- FCA also covers
  - Obligation to report and refund overpayments
  - No need to deal directly with government for liability to attach if "cause" the submission of a false claim
- Criminal statutes and state false claims statutes



Knowledge: Actual knowledge, reckless disregard or deliberate ignorance

Vendor FCA Liability

Knowingly* *Causes to be presented* a false or fraudulent claim for payment or *Causes to be made* a false record or statement material to a false or fraudulent claim

See eClinicalWorks (Settlement May 2017)

- EHR vendor entered $155M FCA settlement with Corporate Integrity Agreement
- Allegations that *caused submission of false claims* for Medicare/ Medicaid EHR Incentive Payments
- Based on providers using EHR software not meeting HHS certification requirements(standardized drug codes, audit log of user actions, reliable record of imaging orders and drug interaction checks, data portability)

https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations

Effective Compliance Plans

- Implement written policies, procedures, and standards of conduct
- Designate a compliance officer and compliance committee
- Conduct effective training and education
- Develop effective lines of communication
- Conduct internal monitoring and auditing
- Enforce standards through well-publicized disciplinary guidelines
- Respond promptly to detected offenses and undertake corrective action

Implement Written Policies, Procedures, and Standards

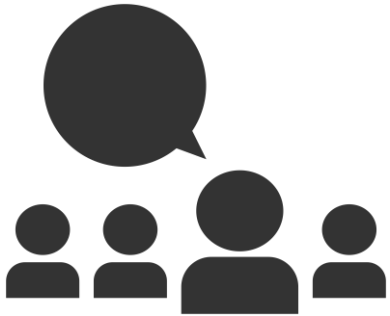
- Memorialize the organization's expectations with regard to compliance
  - Billing and Documentation Practices
  - Privacy Practices, Security Policies and Administrative Safeguards
  - Reporting Procedures for both
- Code of Conduct
- Review with employees annually, and within 3 months of a new hire's start date

Designate a Compliance Officer and/or a Compliance Committee

- In house or outsourced
- HIPAA Privacy and Security Officers must be designated
- Assign duties
  - Administration
  - Monitor and Audit
  - Enforce
  - Review and analyze

Conduct Effective Training and Education

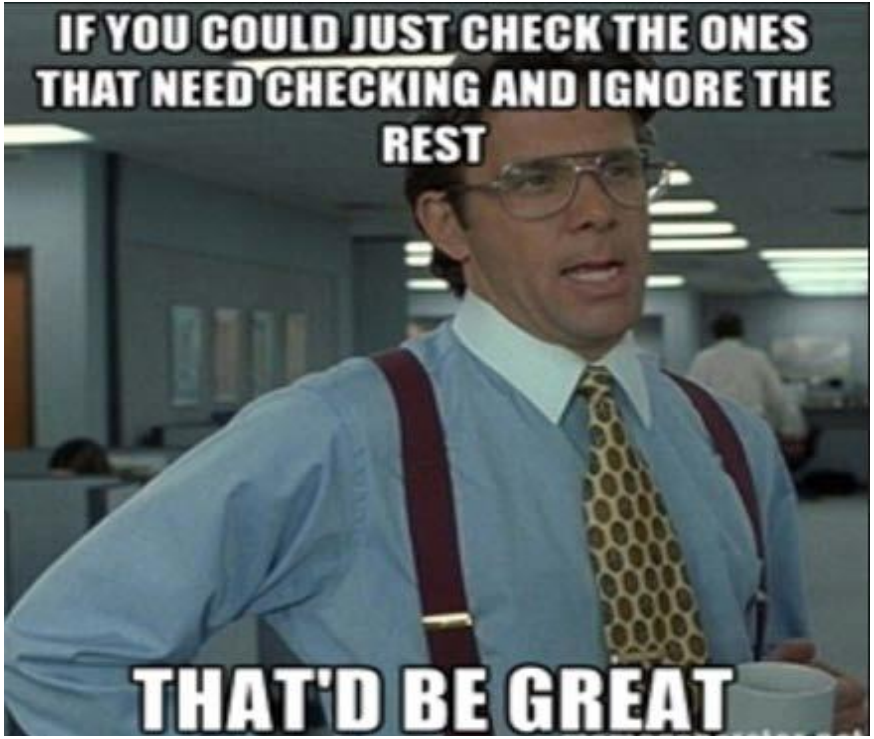
- Education and training programs should include:
  - Information regarding how the organization's compliance program operates
  - Information on specific laws and regulations that impact the organization
    - (e.g. reimbursement, coding, prompt payment requirements, HIPAA risk and role-based training, security awareness, etc.)
  - Consequences of noncompliance (e.g., recoupment, fines, penalties, exclusion) to both the organization and the individual



Develop Effective Lines of Communication

- Communication policies that encourage employees and business partners to report suspected wrongdoing
- Reporting mechanisms should be publicized, available to all levels and to affiliates, and appropriate to organization's size
  - 60-day Report and Return of Overpayments
  - HIPAA Security Incidents/Breach Notification
- Effective response to reports
  - Tracked for possible patterns
  - Investigated
  - Shared

Auditing

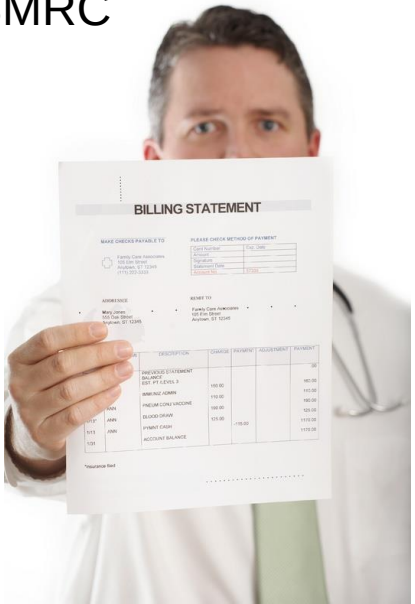


Conduct Internal Monitoring and Auditing

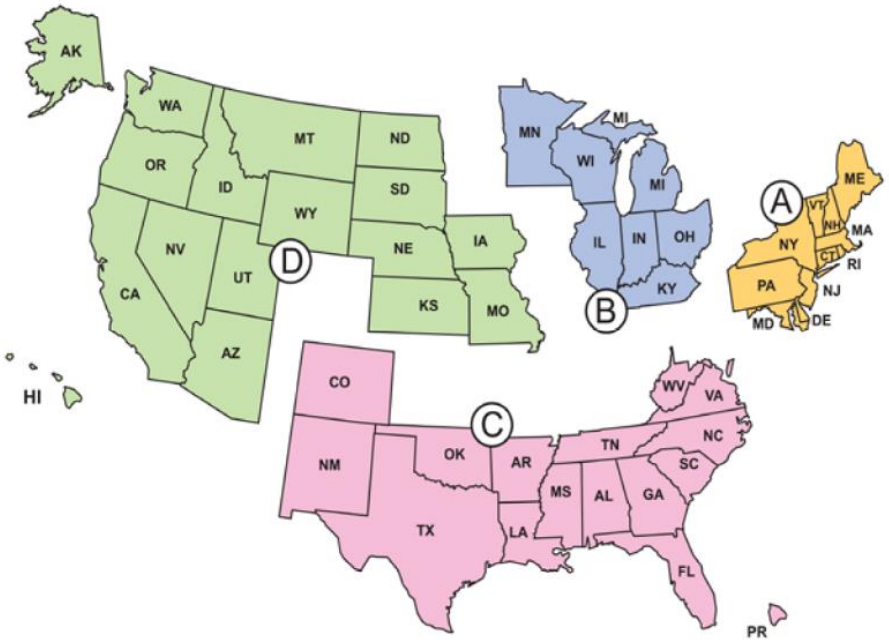
- Monitoring
  - Review internal procedures
  - Review CPT/HCPCS updates, NCDs and LCDs, MLNs, Payer manuals and policy updates
- Auditing
  - Proactive reviews of coding, contracts, quality of care, etc.
  - Identify your organization's areas of greatest risk
- HIPAA Information System Activity Review
  - Drills and HIPAA Incident Response Tabletops

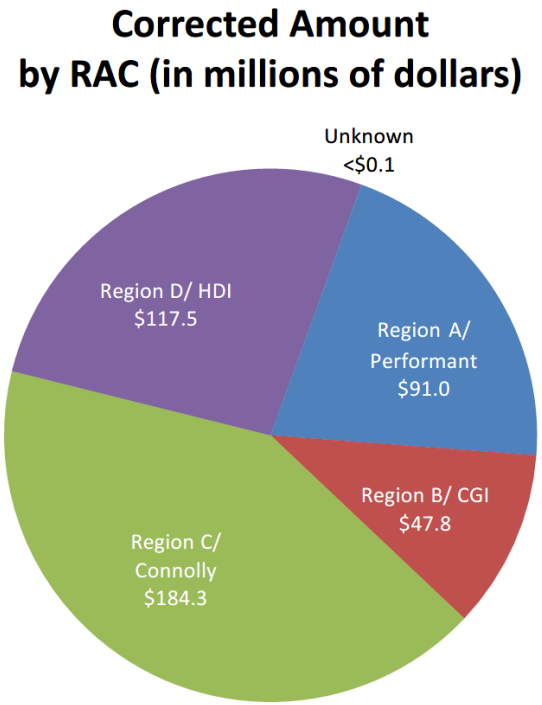
Medicare Audits

- The Auditors
  - MACs, RACs, ZPICs, UPICs, and the SMRC
  - QIO
- Types of Review
  - Pre-payment
  - Post-payment
  - Quality



- Audit Risk Areas
  - Lack of documentation
  - Unbundling
  - Upcoding
  - Medical Necessity documentation
  - Inappropriate balance billing
  - Routine waiver of copayments/deductibles





Source: The Recovery Auditing in Medicare Fee-For-Service for FY 2015 Report to Congress

Medicare Audits – Best Practices

- Do your homework
  - Review relevant medical literature, national coverage determinations, local coverage determinations, *Coding Clinics,* the CPT codebook, etc.
- Retain an expert
- Make every plausible challenge to audit findings
- Don't be afraid to negotiate
  - Corrective action plans
  - Payment plans

MCD UPDATE STATUS

MCD UPDATE	DATA CAPTURED THROUGH	REFRESHED ON MCD
National Coverage Information	Current	Real Time
Local Coverage Information	2/19/2018	Every Thursday
National Coverage Downloads	2/19/2018	Every Thursday

HIPAA Auditing

Bradley

HIPAA Audit Protocol: OCR Phase 2 Audit Program

See HHS Office for Civil Rights Official Audit Protocol at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

Key Activity	Established Performance Criteria	Implemented	In Process	Not Implemented	Audit Inquiry	Notes: Response, Document sources, and next steps
Security Management Process - Risk Analysis	§164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the CE or BA. **OCR Phase 2 Desk Audits:** Minimal levels of Compliance in certain areas **Security** • Security Risk Analysis • Security Risk Management **Breach Notice** • Content and Timeliness • BA Notice to Covered Entity				*Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI (ePHI) it creates, receives, maintains, or transmits?* *Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?* *Determine how the entity has implemented the requirements:* •Obtain and **review** risk analysis policies and procedures. •**Evaluate** and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated. •Obtain and **review** the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. **Evaluate** and determine whether the risk analysis or other documentation contains: • Defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI • Details of identified threats and vulnerabilities • Assessment of current security measures • Impact and likelihood analysis • Risk rating	**Privacy Risks** • BAs • Access • Restrictions on Disclosure • Minimum Necessary

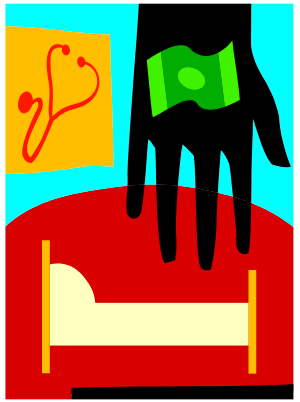
Enforce Standards Through Well-Publicized Disciplinary Guidelines

- Guidelines should include sanctions for:
  - failure to comply with code of conduct/internal policies
  - failure to detect noncompliance when routine observation or due diligence would have provided notice
  - failure to report actual or suspected noncompliance
- Review guidelines at least annually

Documentation Integrity

- Difficult for software purchasers to know exactly how software generates information
- “Prudent hospitals thoroughly assess . . . software that impact(s) coding, billing, generation or transmission of info relating to federal healthcare programs.”

OIG Supplemental Hospital Compliance Program Guidance 70 Fed. Reg. 4858, 4862 (2005)



- CMS: “use program integrity-related EHR software features and capabilities to ensure integrity . . . Some EHR features may create information integrity concerns; however, providers can mitigate these concerns by implementing proper policies and processes."
- Use Vendor Tiering based on Data Classification and Risk to Organization
  - OCR Cloud Guidance recommends written confirmation re: how each party will address security
  - Assess and understand role-based access control, attribution, data entry, editing and preservation, activity logs, and date and time stamping.
  - Consider additional assurances on applicable Security Standards for High-Risk Tiers (EHR)
    - Shared Risk Framework

Undertake and Document Corrective Action

- When?
  - Vulnerabilities, noncompliance, or potential violations are identified
  - HIPAA – environmental and operational changes, breach post mortem
- How?
  - Staff education
  - Repayment of overpayments
  - Disciplinary action
  - HIPAA Sanctions

General Tips

- Identify *your* risk areas
- Manage financial relationships
- When in doubt, ask for help
  - Just because your competitor is doing it, doesn't mean you can or should
- Document, document, document

General Cyber Tips – cont'd

- See HIMSS Annual Cybersecurity Survey to identify risks
  - Consider risks of new technologies AI, Robotics, IOT . . .
  - Consider new risks: Information Blocking
- Many different cybersecurity frameworks available to manage risks
  - HIPAA, GLB, FISMA, PCI
  - NIST Cybersecurity Framework, 800-53 and 53A Security Controls
  - ISO 27000 family – IS Management Systems
- Track progress

Compliance Resources

- OIG
  - https://oig.hhs.gov/compliance/101/index.asp
  - https://oig.hhs.gov/compliance/provider-compliance-training/
- Health Care Compliance Association (HCCA)
  - www.hcca-info.org/AboutHCCA/AboutHCCA.aspx
- OCR *Guidance on Risk Analysis Requirements under the HIPAA Security Rule*
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- ONC/OCR *Security Risk Assessment Tool*
  - www.healthit.gov/providers-professionals/security-risk-assessment
  - See also NIST *Guide for Conducting Risk Assessment September 2012*
- OCR *Security Rule Guidance Material*
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
- OCR *Protocol for the HIPAA Audit Program*
  - www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol2.html

HIPAA References

- HHS OCR free training resources
  - https://www.hhs.gov/hipaa/for-professionals/training/index.html
- HIPAA *Access Guidance and FAQs*
  - https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- HHS Cloud Guidance:
  - www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- HHS Ransomware Guidance
  - www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
  - *See also NIST Special Publication 800-88 Guidelines for Media Sanitization*
- HHS Data Blocking FAQ
  - www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

Questions

- Leslie Cumber, lcumber@gfrlaw.com
  Twitter: @lesliecumber
  LinkedIn: www.linkedin.com/in/lesliecumber

GORDON·FEINBLATT LLC
ATTORNEYS AT LAW

- Amy Leopard, aleopard@Bradley.com
  Twitter: @Amy_Leopard
  LinkedIn: www.linkedin.com/in/leopardhealthlaw

Bradley

Please complete the online session evaluation