The “Stark” Reality of Managing Compliance

Session COM4, March 5, 2018

Leslie M. Cumber, Health Care Attorney, Gordon Feinblatt LLC
Amy S. Leopard, Esq., FHIMSS, Bradley, Nashville
Conflict of Interest

Leslie M. Cumber,
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.
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
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

### Who are the players?

<table>
<thead>
<tr>
<th>State Licensing Boards</th>
<th>State and local Dept. of Health</th>
<th>Medicaid Integrity Program and state Fraud Control Unit</th>
<th>DEA</th>
<th>OIG</th>
<th>DOJ</th>
<th>FBI</th>
<th>CMS</th>
<th>CMS Payment Contractors (MACs)</th>
<th>QIOs</th>
<th>ONC</th>
<th>RACs, ZPICs UPICs, SMRC</th>
<th>Private Payer Fraud Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The diagram illustrates the various entities involved in health information and technology, with arrows indicating the flow or relationship between them.
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**

“…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.”

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

Quality Reporting as a Medicare Payment Issue

Hospital Value-Based Purchasing Performance Scoring

Mandatory Risk Programs = 6% of Hospital Revenue at Risk

- Hospital Acquired Condition Penalties
- Readmission Penalties

• Significant interplay now between compliance and quality reporting as providers submit data on quality, mortality, readmissions, severity, LOS, continuum of care, that are material to Medicare payment.

• Quality data must be accurate

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

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 (May 2017)

– EHR vendor entered $155M FCA settlement with Corporate Integrity Agreement

– Allegations it 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)

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
Implementing Written Policies, Procedure, and Standards

• Memorialize the Organization’s expectations with regard to compliance
  – Privacy Practices
  – Billing Practices
  – Reporting Procedures
• 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
• 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 (e.g. reimbursement, coding, prompt payment requirements, security awareness, etc.) that impact the organization
  - The 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

• Effective response to reports
  – Tracked for possible patterns
  – Investigated
  – Shared
Auditing and Monitoring

If you could just check the ones that need checking and ignore the rest, that'd be great.
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
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
- Inappropriate balance billing
- Routine waiver of copayments/deductibles
Medicare Audits – Best Practices

• Do your homework
  – Review relevant medical literature, local coverage determinations, 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
Medicare Audits – Best Practices

• Do your homework
  – Review relevant medical literature, local coverage determinations, 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
## HIPAA Auditing

### HIPAA Audit Protocol: OCR Phase 2 Audit Program


<table>
<thead>
<tr>
<th>Key Activity</th>
<th>Established Performance Criteria</th>
<th>Implemented</th>
<th>Not Implemented</th>
<th>Audit Inquiry</th>
<th>Notes: Response, Document Sources, and Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process - Risk Analysis</td>
<td>§192.108(1)(v)(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.</td>
<td></td>
<td></td>
<td>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 it creates, receives, maintains, or transmits?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>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?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Determine how the entity has implemented the requirements:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Obtain and review risk analysis policies and procedures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Evaluate and determine whether the risk analysis or other documentation contains:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Details of identified threats and vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Assessment of current security measures</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Impact and likelihood analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Risk rating</td>
<td></td>
</tr>
</tbody>
</table>
Enforce Standards Through Well-Publicized Disciplinary Guidelines

• Guidelines should include sanctions for:
  – failure to comply with the 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
Health IT and Documentation

- 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.”


EHR Documentation Integrity

- "Providers and others should use program integrity-related EHR software features and capabilities to ensure the integrity of EHR documentation.

- Some EHR features may create information integrity concerns; however, providers and others can mitigate these concerns by implementing proper policies and processes."

- Ask questions about role-based access control, attribution, data entry, editing and preservation, activity logs, and date and time stamping.
Undertake Corrective Action

• When?
  – Vulnerabilities, noncompliance, or potential violations are identified

• 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
Compliance Resources

• OIG
  – https://oig.hhs.gov/compliance/provider-compliance-training/

• Health Care Compliance Association (HCCA)
  – http://www.hcca-info.org/AboutHCCA/AboutHCCA.aspx

Other Good Sources:

• OCR Protocol for the HIPAA Audit Program
  – www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol2.html

• 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
HIPAA References

- HIPAA Access Guidance
  - [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs)

- HHS Cloud Guidance:
  - [www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html](www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html)

- HHS Ransomware Guidance
  - [www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf](www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf)

- OCR Security Rule Guidance Material
  - [www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html](www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html)
  - See also NIST Special Publication 800-88 Guidelines for Media Sanitization

- HHS Data Blocking FAQ
Questions

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

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

Please complete the online session evaluation