Industry leading Education

Pitfalls of Documentation in the Age of EHR

Tuesday, March 19th from 2:00 – 3:30 EST

The Compliancy Group Free Education Series is proud to present , The Health Law Partners, presentation of "Pitfalls of Documentation in the Age of EHR" During this session you will learn the Basics of EHR's, while exploring the issues of quality care, malpractice, privacy & security, billing fraud and abuse. This is a must attend event for new and experienced Health Professionals and Business Associates.

Presented by: The Health Law Partners

Lori A. LaSalle, Esq.
Gina R. Dolan, Esq

Certified Partner Program

Certified Partners

Get the added confidence working with The Guard network,
along with special programs for Guard users only

GENESIS 42

Genesis 42

GENESIS 42 brings over 25 years of experience in the computer technology field. We provide advice, assistance and complete solutions that enable our clients to successfully implement technology that is designed to increase profits and minimize headaches.

THE HEALTH LAW PARTNERS

The Health Law Partners

Solid Advice. Real Solutions. For Healthcare Business.

eClinicalWorks

eClinical Works

EMR Platform eClinicalWorks is a leading provider of ambulatory clinical information systems, including electronic medical records systems and community applications.

Why use our partners?

- Compliancy Group Certified
- Approved Services
- Integrated with The Guard
- Special Pricing

Learn the benefits of becoming a partner!

Todays Webinar

- **Please ask questions**
- **Todays slides are available**

http://compliancy-group.com/slides023/

- **Past webinars and recordings**

http://compliancy-group.com/webinar/

Compliancy Group

855.85HIPAA
www.compliancygroup.com

Pitfalls of Documentation in the Age of EHR

By: Lori A. LaSalle, Esq.

Gina R. Dolan, Esq.

PITFALLS OF DOCUMENTATION IN THE AGE OF EHR

HLP [=]

THE HEALTH LAW PARTNERS

Agenda

- EHR Basics;
- Quality of Care;
- Malpractice Litigation;
- Privacy and Security;
- Billing Fraud & Abuse

EHR Basics

- Types of EHR (cloud vs. on-site server);
- Contractual issues;
- Meaningful use;
- Costs of implementation.

EHR Contractual Issues

- Identify the hardware and software requirements;
- Ownership of Data;
  Termination/bankruptcy
- License (#of users, offices, terminals);
- Implementation
  - Data conversion
  - Timelines/acceptance testing
  - Interfaces

- Pricing and payments;
- Warranties
  – Performance
  – Viruses
  – Compliance with laws,
  – Infringement
  – Certification requirements
- Training & support

EHR Contractual Issues (cont'd)

- Confidentiality/Privacy & Security;

- Termination and transition
    - Provisions for breach
    - Transition of data

- Limitation of Liability/Indemnification

Medicare EHR Incentive Program

- Administered by Centers for Medicare and Medicaid Service (CMS)

- Maximum incentive payment: $44,000.00

- Payments over 5 consecutive years

- Payment adjustments will begin in 2015 for providers who are eligible but decide not to participate

- Providers must demonstrate "meaningful use" every year

N.Y.S. Medicaid EHR Incentive Program

- Administered by N.Y.S. Medicaid Agency

- Maximum incentive payment: $63,750.00

- Payments over 6 years but *do not* have to be consecutive

- No Medicaid payment adjustments

- In the first year, providers can receive an incentive payment for adopting, implementing, or upgrading EHR technology. Providers

Cost of EHR Implementation

- Electronic Health records improve are but do not save money. The money saved from administrative efficiency is replaced by IT costs.

- It is reported that for an average five-physician practice, implementation cost an estimated $162,000 with $85,000 in maintenance expenses the first year.

Quality of Care

THE HEALTH LAW PARTNERS

- Patient Communication
  - Instant messaging;
  - Asynchronous communication
  - Taking patient history;
    - Decision support functions
    - Check boxes
    - Reliance of history available on computer

Quality of Care

Study conducted at the Manhattan VA primary care clinic on whether physician experience modifies the impact of exam room computers on the physician-patient interaction.

Results:

Patients seeing residents were:

- less likely than patients seeing faculty to strongly agree that they were satisfied with their overall relationship with the physician;

- More likely to agree that the computer adversely affected the amount of time the physician spent talking;

- Faculty spent a smaller proportion of time interacting with the computer than patients seeing resident.

Malpractice Litigation

- Only addressing what there is a
box for;
- Everyone that sees the patient
cut and pastes the same physical exam note;
- Audit trails;
- Pt. being treated for rheumatoid arthritis received a default oncology dose b/c placed on the oncology floor

Privacy & Security

- HIPAA

  – Privacy and security of protected health information ("PHI")

  – Compliance standards for safeguarding and protecting PHI

- HITECH

  – _Electronic_ PHI

  – Civil monetary penalties for breaches

Privacy & Security

"Breach" (as defined by HITECH):

"An impermissible use or disclosure that compromises the security or privacy of the PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual."

Privacy & Security

- Increased risk of liability for electronic records:
  - Stolen laptops
  - Lost cell phones
  - Computer hackers

- Potential for greater impact per breach

- More serious breaches = higher penalties

Penalties enforced by the Office of Civil Rights (OCR):

- Unintentional violations: $100 to $50,000 per violation
- Violations due to reasonable cause: $1,000 to $50,000 per violation
- Violations due to willful neglect that are corrected: $10,000 to $50,000 per violation
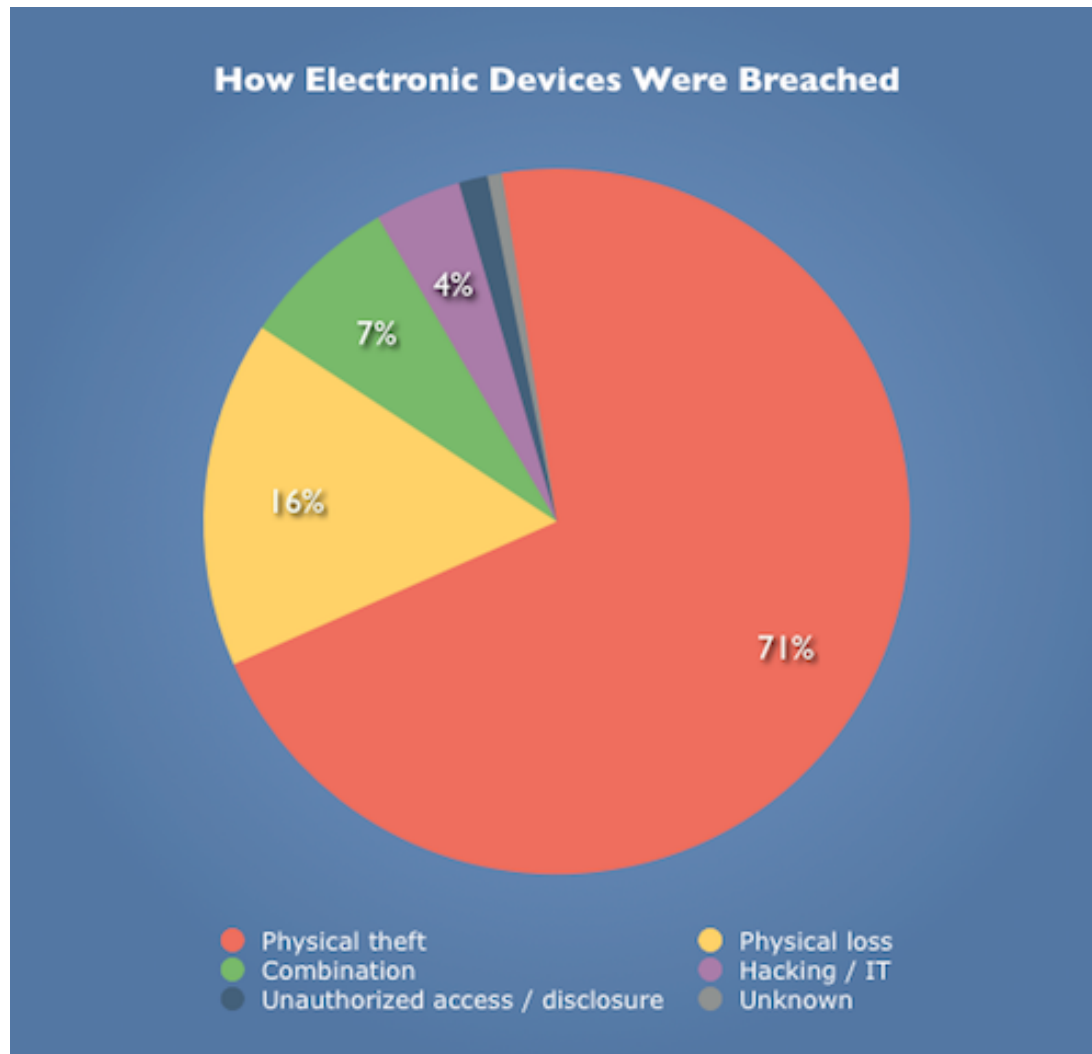- Violations due to willful neglect that are not corrected: $50,000 per violation

Privacy & Security

- HIPAA violations are happening in physicians' offices, hospitals, and at home

- The most common causes of security breaches:

  - Physical theft and loss
    - Portable devices
      (laptops; cell phones; etc.)
  - NOT hacking or IT issues!

HLP □
THE HEALTH LAW PARTNERS

Privacy & Security

How Electronic Devices Were Breached

- ● Physical theft
- ● Combination
- ● Unauthorized access / disclosure
- ● Physical loss
- ● Hacking / IT
- ● Unknown

Privacy & Security

Provider	Year	Individuals Affected	How Data Was Breached
Keith W. Mann, DDS	2009	2,000	On-premise system servers (managed by Professional Computer Services) hacked.
Daniel J. Sigman MD	2009	1,500	Backups of on-premise system were stolen from Dr. Sigman's home.
Kaiser Permanente Medical Care Program	2009	15,500	Portable hard-drive was left inside a van. Van was then stolen.
Texas Health Arlington Memorial Hospital	2010	654	Poorly trained employees marked electronic charts incorrectly in an on-premise system.
Mayo Clinic	2010	1,740	Employee found snooping on patients' records using Mayo Clinic's on-premise EHR system.
NYC Health & Hospitals Corporation	2010	1,700,000	Hard drives from an on-premise system stolen from the back of a van.
South Shore Hospital	2010	800,000	Hard drives from an on-premise system lost on their way to a contractor for destruction.

Detecting Privacy and Security Problems:

1. *HIPAA Audits*

2. *EHR Meaningful Use Incentive Payment Audits*

Privacy & Security

Mitigating Risks

- Policies and Procedures
  - Appropriate for record storage and access
  - Applicable to use of EHR and electronic devices
- Staff Training
  - HIPAA Policies and Procedures
  - Use of EHR (including risk areas)
  - Use of other electronic devices (computers/laptops; cell phones;
- Internally Monitoring Compliance
- Breach Disaster Plans
- Business Associates
  - Business Associate Agreements
  - Security plans
- **A proactive risk management approach can help mitigate potential liability!**

Billing Fraud & Abuse

- Increases in healthcare costs tied to EHR adoption?
- EHR changing the way providers are billing for their services
- New York Times Article (September 21, 2012)
  - Attributed a portion of the recent growth in health care costs to the increased use of EHR
  - Faxton St. Luke's Healthcare in Utica, N.Y
  - Baptist Hospital in Nashville, T.N.
  - Hospitals that received government incentives to adopt electronic records showed a 47% rise in Medicare payments at higher levels from 2006 to 2010, compared with a 32% rise in hospitals that have not received any government incentives
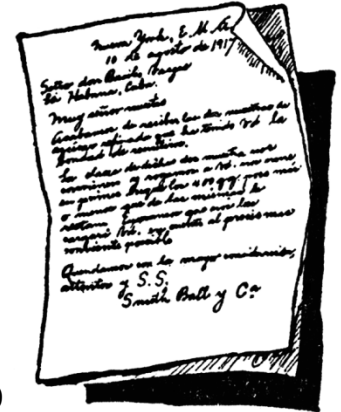
Billing Fraud & Abuse

THE HEALTH LAW PARTNERS

HHS/DOJ Letter hospital organizations (September 24, 2012)

- Concern that EHRs are being used to "game the system"
- Addressed false documentation of care issues:
  - "cloning"
  - "upcoding"
  - Use of templates and prompts
- Outlined what is being done to ensure payment accuracy and to prosecute healthcare fraud. Some of the actions being enforced by CMS include:
  - Review of billing through audits
  - Initiating more extensive medical reviews
  - Requiring individual verification of patient care information
  - Addressing inappropriate increases in coding intensity in CMS payment rules
  - Using new tools to stop Medicare payments upon suspicion of fraud in order to mine data for detection
- HHS, DOJ, FBI and other law enforcement agencies are monitoring these trends and will take action upon detection
- No actual guidance measures provided (only warning)

Billing Fraud & Abuse

- Why the increased risk?
  - General nature of EMR
  - Specific features of the EMR system
- Increased Liability:
  - Government and commercial payment audits (overpayments)
  - Civil monetary penalties and sanctions (False Claims; fraud)
  - Termination of participation (Medicare; Medicaid; commercial managed care contracts)

Billing Fraud & Abuse

Problem Areas:

1. Authorship Integrity

2. Auditing Integrity

3. Documentation Integrity

Billing Fraud & Abuse

Authorship Integrity

- Multiple individuals entering data
  - Example:
    - Nurse documents history, medication lists, complaints
    - Doctor enters own notes
  - Need audit function to demonstrate who is entering data and what is entered
  - Potential fraud allegations if there is an appearance that unauthorized individual performed services

- Electronic Signatures
  - Provider who rendered services
  - "locking" charts for billing purposes

"Cloning"

- Copying and pasting entries from:
  - Other patient charts; or
  - Previous visits
- Automatic generation of detailed patient histories
- Potential for fraudulent and abusive billing:
  - Upcoding (higher reimbursement)
  - Reimbursement for services not actually performed

Auditing Integrity

- Properly tracking changes, amendments and additions to patient records

- Changing records after authentication → potential for appearance of fraud

- <u>Example:</u> substantiating services billed but NOT actually performed

Documentation Integrity

- Templates
  - Drop-down menus of "best practices"
  - "Click-throughs"
  - Automatic generation of records
- Systems should have a limited number of auto-generated data
- Potential for fraudulent and abusive billing:
  - Upcoding (higher reimbursement)
  - Reimbursement for services (examinations) not actually performed

Questions?

*A*chieve *I*llustrate *M*aintain
Compliance Simplified!

- ✓ **HIPAA Compliance**
- ✓ **HITECH Attestation**
- ✓ **Meaningful Use core measure 15**
- ✓ **Omnibus Rule Ready**

Free Demo and 15 Day Evaluation
855.85HIPAA
http://compliancy-group.com/

New & Past Webinars
http://compliancy-group.com/webinar/

Compliancy Group

855.85HIPAA
www.compliancygroup.com

Solid Advice.
Real Solutions.
For Healthcare Business.

Speaker Contact Information:

Lori A. La Salle, Esq. – llasalle@thehlp.com

Gina R. Dolan, Esq. – gdolan@thehlp.com

1983 Marcus Avenue, Ste. 106

Lake Success, NY 11042

Phone: (516) 492-3390

Fax: (516) 492-3389

http://www.thehealthlawpartners.com/