CONFIDENTIALITY COALITION

HIPAA 101

What you need to know about health information privacy and security

Learn how health information is protected across a variety of settings and why the law remains relevant to current legislation.

Featuring:

surescripts
The Nation's E-Prescription Network

Cleveland Clinic

Monday, March 23, 2015
12:00 – 1:00 PM

Rayburn House Office Building, Room B338

Boxed lunch available

RSVP to cadamec@hlc.org

This event will be widely attended and has been designed to comply with House Ethics rules.

Monday, March 23 from 12:00 – 1:00 PM

HIPAA 101

What you need to know about health information privacy and security

March 23, 2015

Tina Olson Grande
Chair, Confidentiality Coalition

Membership

Aetna
Amerinet
Amgen
AmerisourceBergen
American Clinical Laboratory Association
American Hospital Association
American Pharmacists Association
American Society for Radiation Oncology
America's Health Insurance Plans
Anthem
Ascension Health
Association of American Medical Colleges
Association of Clinical Research Organizations
Athenahealth, Inc.
Augmedix
Baylor Scott & White Health
Bio-Reference Laboratories, Inc.
Blue Cross Blue Shield Association
BlueCross BlueShield of Tennessee
Boeringer Ingelheim Pharmaceuticals
Cardinal Health
CIGNA Corporation
Cleveland Clinic
College of American Pathologists
C.R. Bard
CVS Caremark
Edwards Lifesciences
Eli Lilly
Emdeon
Express Scripts
Federation of American Hospitals
Franciscan Missionaries of Our Lady Health System
Genetic Alliance
Health Care Service Corporation
Healthcare Leadership Council
Ikaria
IMS Health
Indiana University Health
Intermountain Healthcare
inVentiv Health
Johnson & Johnson
Kaiser Permanente
Marshfield Clinic
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medtronic
MemorialCare Health System
Merck
MetLife
National Association of Chain Drug Stores
National Association of Health Underwriters
National Association of Psychiatric Health Systems
National Community Pharmacists Association
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Novartis
Novo Nordisk
Owens & Minor
Pharmaceutical Care Management Association
Premier healthcare alliance
Privacy Analytics
Quest Diagnostics Incorporated
Sanofi US
SCAN Health Plan
State Farm
Stryker
Surescripts
Takeda Pharmaceuticals North America
Texas Health Resources
Theragenics
VHA
Walgreens
Weight Watchers International
Workgroup for Electronic Data Interchange
ZS Associates

CONFIDENTIALITY COALITION

HIPAA
Introduction to the Privacy Rule

McDermott Will & Emery

Jennifer S. Geetter
Partner
McDermott Will & Emery LLP

For discussion purposes only. Does not constitute legal advice

CONFIDENTIALITY COALITION

HIPAA and HITECH

Act	Health Insurance Portability and Accountability Act of 1996	Health Information Technology for Economic and Clinical Health Act
Public Law Number	104-191	111-5 Title XIII of Div. A, Title IV of Div. B
Purpose	Improve the efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial information	Promote health information technology and improve privacy and security provisions of HIPAA
Key Privacy Provisions	• Addressed the privacy and security of patient records and other forms of Protected Health Information • Implemented through regulations in 45 C.F.R. Parts 160-164	• Added new audit provisions • Enhanced accountability for Business Associates • Required notification of affected individuals if a breach of unsecured Protected Health Information has occurred • Expanded enforcement to state attorneys general • Increased penalties

Who is Covered by HIPAA Regulations?

Health Care Providers

- That transmit information in connection with covered transactions
  - Health care claims
  - Health plan enrollment
  - Health plan eligibility
  - First report of injury
  - Coordination of benefits

Health Plans

- HMOs
- Health insurance companies
- Medicaid & Medicare
- Group health plans, i.e., employer-sponsored health plans
- Military and veterans health care programs

Health Care Clearinghouses

- Process or facilitate the processing of health information to/from nonstandard formats to/from standard formats
- Public or private entities that receive health information from others

Business Associates

- Perform certain functions or activities that involve the use or disclosure of PHI on behalf of the covered entity

Protected Health Information (PHI)

- Protected Health Information
  - Defined as individually identifiable health information that is transmitted by or maintained in any form or medium (oral, paper, electronic media)
  - Excludes educational records covered by FERPA, employment records held by a covered entity, and records of a person deceased for more than 50 years
- Individually Identifiable Health Information

Created or received by a health care provider, health plan, employer, or health care clearinghouse

AND

Relates to the individual's past, present, or future physical or mental health or condition; **or**

Relates to the provision of health care to an individual; **or**

Relates to past, present, or future payment for the provision of health care to the individual

AND

Identifies the individual, **or**

There is a reasonable basis to believe it could be used to identify the individual

Examples of Identifying Information

- Demographic information
  - Name
  - Residential Address
  - Phone #, fax # or an email address
- Identifying features or numbers
  - Social Security or Medicaid card numbers
  - Certificate or license numbers
  - License plate numbers
  - Device identifiers and serial numbers
  - Full-face photographic images, comparable images
  - Biometric identifiers, including finger and voice prints
- Dates directly related to an individual
  - Birth, marriage, death, admission, discharge, claim
- Exception: Persons deceased for more than 50 years

HIPAA Privacy Rule

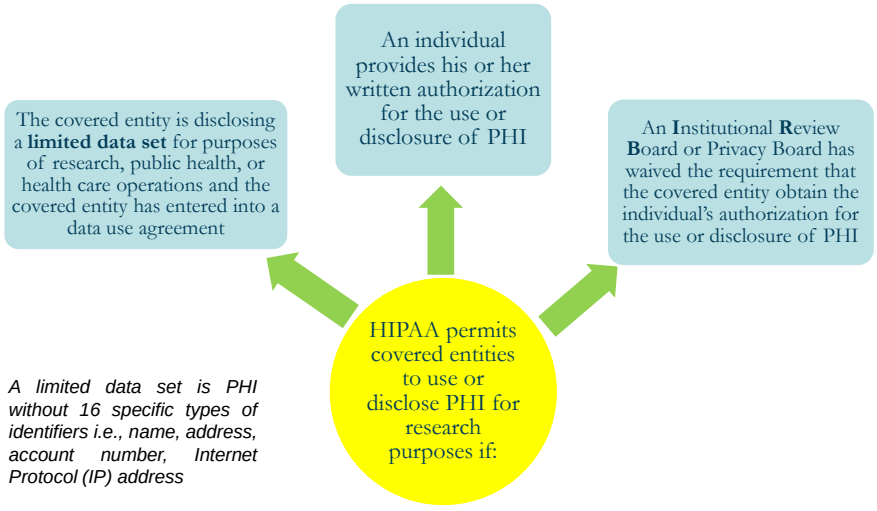
- Limits the use and disclosure of PHI by covered entities and business associates
- Use and disclosure require an individual's authorization or the opportunity to object unless:
  - Disclosure is to the individual
  - Use or disclosure is for treatment, payment, or health care operations
  - Use or disclosure is for one of the specified exceptions and in compliance with the specific rules for each exception:
    - uses and disclosures "required by law"
    - uses and disclosures to avert a serious threat to health or safety
    - uses and disclosures for notification purposes
    - disclosures for disaster relief purposes
    - disclosures for law enforcement purposes
    - uses and disclosures for public health activities
    - uses and disclosures for research purposes

Disclosures for Public Health Activities

HIPAA permits covered entities to use or disclose PHI for public health purposes:

- Public health authorities authorized by law to collect or receive PHI to perform public health activities
  - Preventing or controlling disease, injury, or disability
  - Public health surveillance, investigations, interventions
    - Foodborne illnesses, tuberculosis, HIV
  - Birth, death, and disease reporting
  - Reports of child abuse or neglect
- Food and Drug Administration
  - Adverse event reports related to drugs and medical devices
  - Reports that may lead to product recalls of other FDA-regulated products, such as food and dietary supplements

Disclosures for Research



A limited data set is PHI without 16 specific types of identifiers i.e., name, address, account number, Internet Protocol (IP) address

10

Accounting of Disclosures

- Individuals have the right to receive an accounting of disclosures of PHI made by a covered entity in the past 6 years
- HITECH required covered entities and business associates to account for disclosure of PHI for treatment, payment, and health care operations if the disclosures are made via an electronic health record
- HHS proposed rule to amend the accounting for disclosures provision is still pending

Exceptions:

- Disclosures to carry out treatment, payment, and health care operations
- Disclosures to the individual
- Disclosures incident to a use or disclosure otherwise permitted or required
- Disclosures pursuant to an authorization
- Disclosures for national security or intelligence purposes
- Disclosures as part of a limited data set
- Disclosures to correctional institutions or law enforcement officials
- Disclosures to persons involved in the individual's care or notification purposes

The Privacy Rule's Limited Reach

The Privacy Rule does not restrict uses and disclosures of:

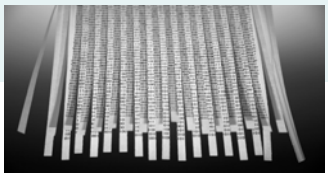
- Health and wellness mobile apps that are not created by covered entities or business associates (for example, most step and calorie counters)
- Consumer health information that is not PHI
- Employment records (sick leave, fitness for duty)
- Records of persons deceased for 50+ years
- Education records (Family Educational Rights and Privacy Act - FERPA)
- De-identified information
  - Does not identify an individual
  - No reasonable basis to believe that the information could be used to identify an individual from de-identified information

Breach Notification

- The breach rule applies to covered entities and business associates as of September 23, 2009
- A **breach** is the
  - acquisition, access, use, or disclosure of **unsecured** PHI
  - in a manner not permitted by the HIPAA Privacy Rule (i.e., unauthorized)
  - which compromises the security or privacy of PHI
- Required notifications may include:
  - Individuals
  - HHS Secretary
  - Media
  - State law enforcement or other state entities
    - Almost every state has its own data breach notification law

When is PHI Unsecured for Purposes of a Breach?

Unsecured PHI	Secured PHI
PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in a HHS guidance document • *i.e.*, PHI can be accessed by unauthorized persons	PHI meets the encryption or destruction standards in the HHS guidance document • Encryption for data in motion and at rest • Based on National Institute of Standards and Technology (NIST) publications • Cross-cut shredding



Breach Notification

- An acquisition, access, use, or disclosure of unsecured PHI in an unauthorized manner is presumed to be a breach
- The covered entity or business associate may demonstrate in a risk assessment that there is a low probability that the PHI has been compromised, based on four factors:
  1. Nature and extent of the PHI involved, including types of identifiers and likelihood of reidentification;
  2. Unauthorized person who used the PHI or to whom the disclosure was made;
  3. Whether the PHI was actually acquired or viewed; and
  4. Extent to which the risk to PHI has been mitigated

Major Omnibus Rule Provisions

- Mandated new provisions in Business Associate Agreements and made business associates directly liable for HIPAA/HITECH compliance
- Strengthened limits on the use and disclosure of PHI for marketing and fundraising purposes
- Expanded individual rights to receive electronic copies of PHI
- Allowed individuals to restrict disclosures to a health plan if they pay out of pocket, in full, for treatment
- Facilitated disclosures of proof of a child's immunization to schools
- Required revisions to a covered entity's Notice of Privacy Practices
- Compliance with the new rule was required by September 23, 2013 or September 22, 2014

How are HIPAA and HITECH Enforced?

- Enforced by HHS and the US Department of Justice
  - Individuals may face civil and/or criminal penalties for HIPAA violations
  - Covered entities and business associates may face large fines for HIPAA violations
    - Up to $1.5 million for all identical violations in a calendar year

- HITECH required HHS to perform periodic audits of covered entities and business associates
  - Any covered entity or business associate can be audited
  - Audits review compliance with the HIPAA Privacy, Security, and Breach rules
- HITECH permitted state Attorneys General to bring civil actions on behalf of state residents
- No federal private right of action for individuals

How is HIPAA Related to Other Laws?

- HIPAA preempts state laws that are contrary to HIPAA *unless*:
  - The HHS Secretary makes a determination that the law is necessary for certain purposes, such as the prevention of fraud and abuse;
  - The state law is more stringent than HIPAA's Privacy Rule;
  - The state law provides for the reporting of disease or injury, child abuse, birth, death, or the conduct of public health activities; or
  - The state law requires a health plan to report or provide access to information for audit, program monitoring, licensure, or other purposes

How is HIPAA Related to Other Laws? (continued)

- HIPAA does not overrule more restrictive federal law and needs to be understood in context with a number of other federal laws, including:
  - Federal Privacy Act of 1974
  - Genetic Information Nondiscrimination Act of 2008 (GINA)
  - Americans with Disabilities Act
  - Federal confidentiality laws and regulations for substance abuse patient records
  - Public Health Service Act, section 543 (42 U.S.C. § 290dd-2); 42 C.F.R. Part 2
- Proposals for the consumer privacy bill of rights incorporate HIPAA by reference

HIPAA Security Rule Basics

Sara Juster
Associate General Counsel & Privacy Officer
Surescripts, LLC

HIPAA's Three Key Properties

1) **Availability**: data or information is accessible & useable upon demand by an authorized person.
2) **Confidentiality**: data or information is not made available or disclosed to unauthorized persons or processes.
3) **Integrity**: data or information have not been altered or destroyed in an unauthorized manner.

Why is security key?

- Proper security helps ensure that PHI is not made available or disclosed to unauthorized persons or processes and that it has not been altered or destroyed in an unauthorized manner.
- This ultimately promotes use of electronic health information – an important goal of HIPAA.

Security Rule Requirements

- Covered Entities must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.
- Specifically, Covered Entities must:
  1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  3. Protect against reasonably anticipated, impermissible uses or disclosures; and
  4. Ensure compliance by their workforce.

Who is covered?

The HIPAA Security Rule, like all of the Administrative Simplification rules, applies to **health plans, health care clearinghouses,** and to any **health care provider** who **transmits health information** in **electronic form** in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA

"Security is not a one-time project but rather an on-going, dynamic process that will create new challenges as covered entities' organizations and technologies change."

CMS HIPAA Security Series

Flexible & Scalable

HIPAA Security Rule does **not** dictate measures to be taken but requires Covered Entities to consider:

- Size, complexity, and capabilities,
- Technical, hardware, and software infrastructure,
- Costs of security measures, and
- Likelihood and possible impact of potential risks to e-PHI

Required vs Addressable

- If an implementation specification is "**required**," the specification must be implemented.
- If implementation specification is "**addressable,"** Covered Entity must either:

  (a) implement the addressable implementation specifications;

  (b) implement one or more alternative security measures to accomplish the same purpose;

  (c) not implement either an addressable implementation specification or an alternative.

Security Risk Analysis

No specific format or process is required, but should include:

- Evaluation of likelihood and impact of potential risks to e-PHI;
- Implementation of appropriate security measures to address the risks identified in the risk analysis;
- Documentation of chosen security measures and, where required, the rationale for adopting those measures; and
- Maintenance of continuous, reasonable, and appropriate security protections

Administrative Safeguards

- **Security Management Process**: identify and analyze potential risks to e-PHI, & implement security measures to reduce risks and vulnerabilities to reasonable & appropriate level.
- **Security Personnel**: designate a security official responsible for developing and implementing security policies & procedures.
- **Information Access Management**: implement policies & procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

- **Workforce Training and Management**: provide for appropriate authorization and supervision of workforce members who work with e-PHI & train all workforce members regarding security policies & procedures, & apply appropriate sanctions against workforce members who violate policies & procedures.
- **Evaluation**: perform periodic assessment of how well its security policies & procedures meet the requirements of the Security Rule.

Physical Safeguards

- **Facility Access and Control**: limit physical access to its facilities while ensuring that authorized access is allowed.
- **Workstation and Device Security**: implement policies & procedures to specify proper use of and access to workstations and electronic media and have in place policies & procedures regarding the transfer, removal, disposal, & re-use of electronic media, to ensure appropriate protection of e-PHI

Technical Safeguards

- **Access Control**: technical policies and procedures that allow only authorized persons to access e-PHI
- **Audit Controls**: hardware, software, and/or procedural mechanisms to record & examine access & other activity in information systems that contain or use e-PHI
- **Integrity Controls**: policies and procedures to ensure e-PHI is not improperly altered or destroyed & electronic measures to confirm that e-PHI has not been improperly altered or destroyed
- **Transmission Security**: technical security measures that guard against unauthorized access to e-PHI being transmitted over an electronic network

Organizational Requirements

- **Covered Entity Responsibilities**: If Covered Entity knows of an activity or practice of a BA that constitutes a material breach or violation of BA's obligation, Covered Entity must take reasonable steps to cure the breach or end the violation.
- **Business Associate Contracts**. BA obligations were expanded under the HITECH Act; appropriate business associate contracts must be in place

How HIPAA Affects Healthcare Providers

blair w. barnhart-hinkle, Esq.
Director, Government Relations
Cleveland Clinic

Proposed Modifications

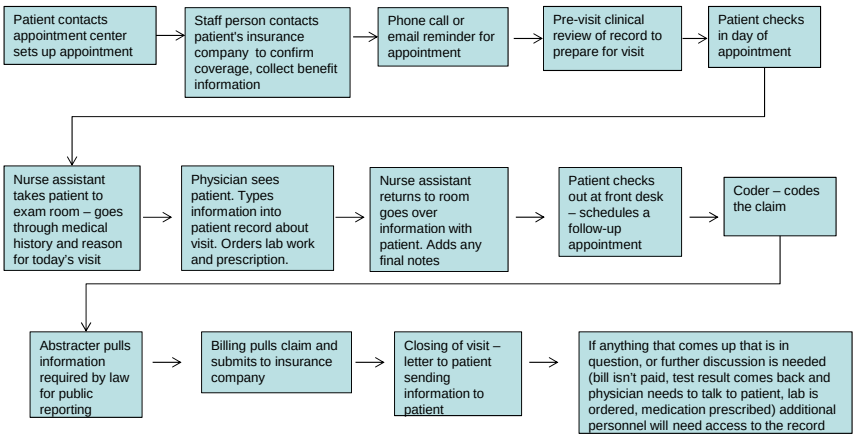
- Two proposals you may have heard about:
  - Require that healthcare organizations obtain consent prior to accessing the patient's medical record
  - Allow patients to restrict access to different portions of their record

Proposal 1
Prior Consent

- Why does this proposal harm patient care?
  - A minimum of 13 different caregivers need to access the patient record for a single outpatient visit to a doctor's office.
  - Nearly 200 caregivers may need to view and input information into a patient's record for an inpatient visit.
  - Asking the patient's permission for each of these views would unduly burden the patient and the healthcare system.

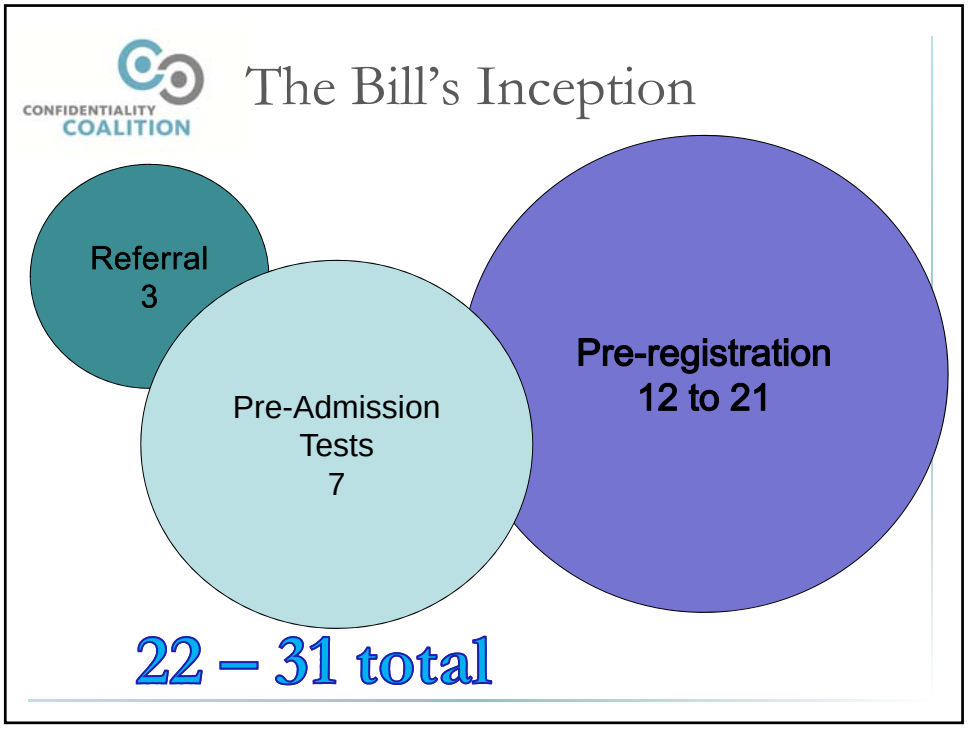
Sample Outpatient Visit

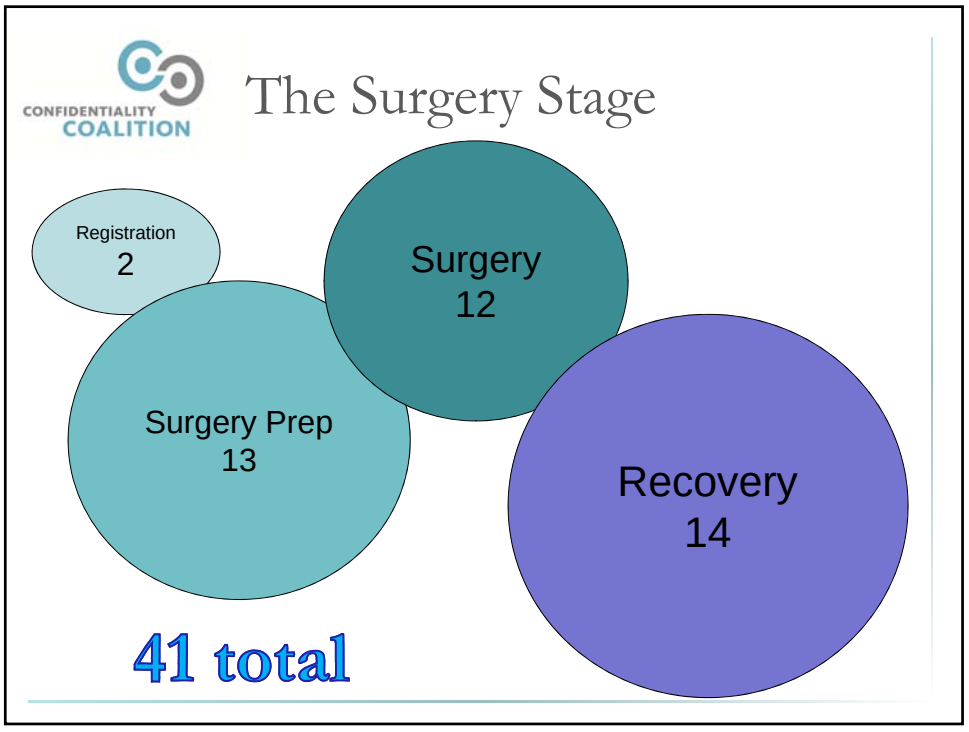
Patient record is accessed at each of the following points

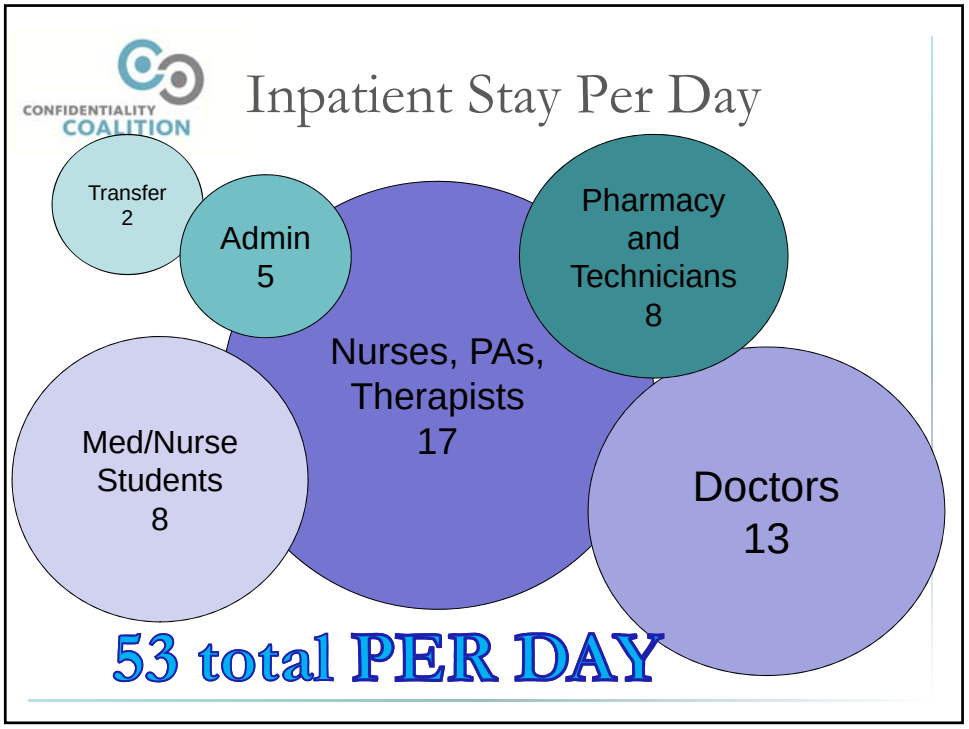


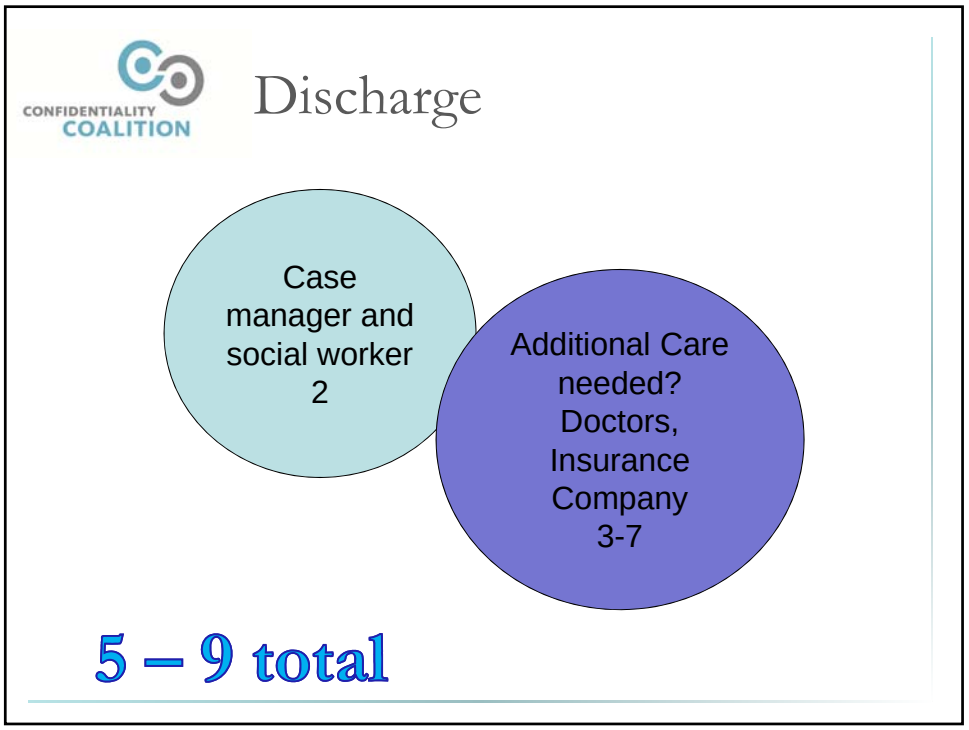
Inpatient Visit

- How many times is a patient's record touched on an average inpatient visit?

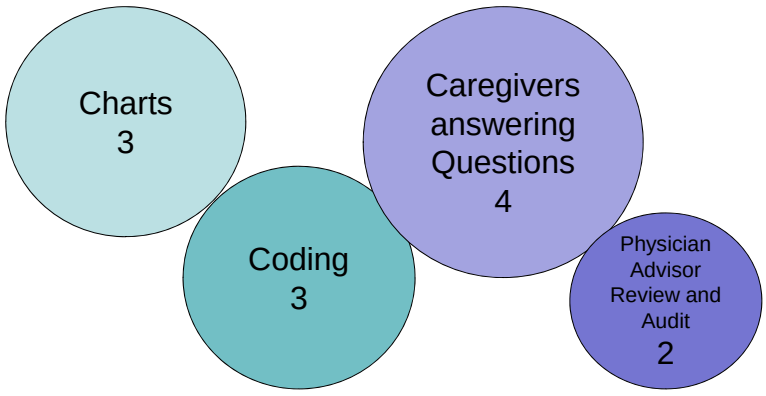

CONFIDENTIALITY COALITION
The Bill's Inception
Referral
3
Pre-Admission
Tests
7
Pre-registration
12 to 21
22 – 31 total


CONFIDENTIALITY COALITION
The Surgery Stage
Registration
2
Surgery
12
Surgery Prep
13
Recovery
14
41 total


CONFIDENTIALITY COALITION
Inpatient Stay Per Day
Transfer 2
Admin 5
Nurses, PAs, Therapists 17
Pharmacy and Technicians 8
Med/Nurse Students 8
Doctors 13
53 total PER DAY

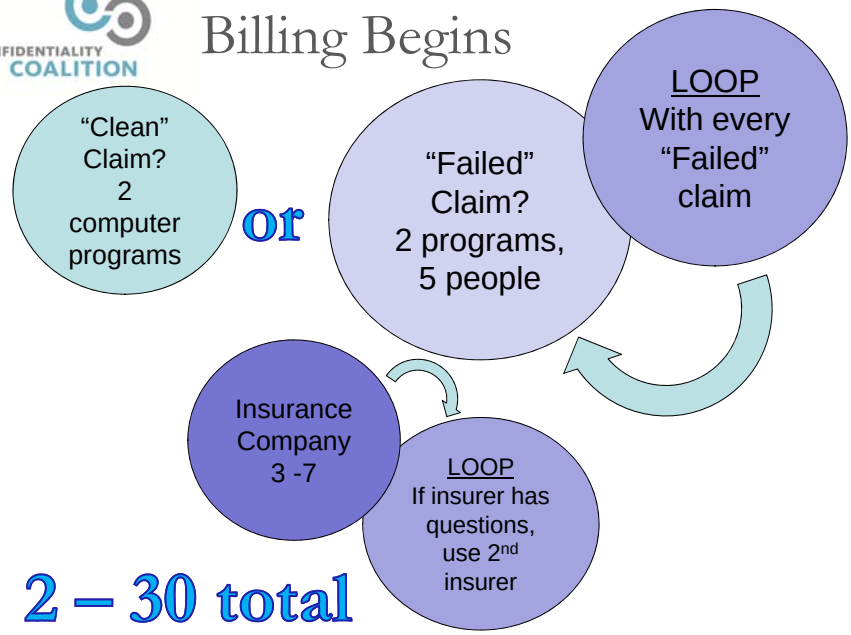

CONFIDENTIALITY COALITION
Discharge
Case manager and social worker 2
Additional Care needed? Doctors, Insurance Company 3-7
5 – 9 total

Compiling the Bill



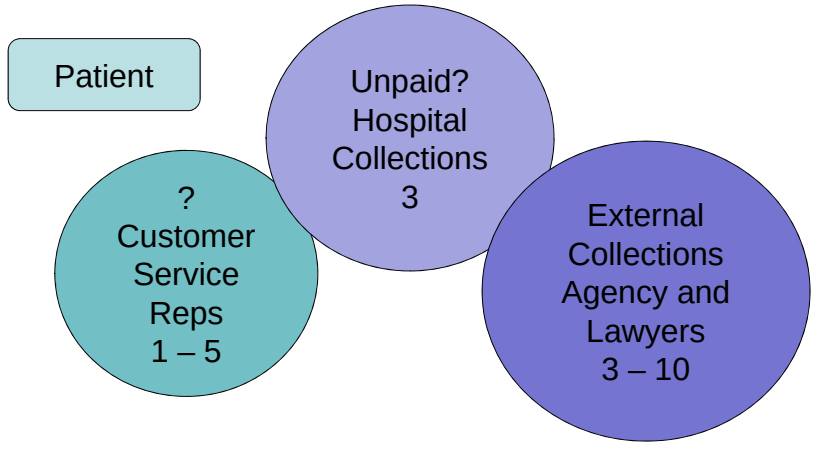
12 total

Billing Begins



2 – 30 total

Patient Receives Bill



1 – 18 total

Total EHR Views

194

Proposal 2
Access Restrictions

- How could restricting access to patient's records harm patient care?
  - Example #1: Mr. Jones doesn't want his primary care physician to know that he was admitted to the ED for an opioid overdose because the drugs were obtained illegally.
    - A week later, Mr. Jones goes to his physician complaining of insomnia.
    - The physician doesn't know that his patient is misusing drugs thus it could lead to
      - Misdiagnosis
      - Dangerous medication interaction

Proposal 2
Access Restrictions (cont'd)

- How could restricting access to patient's records harm patient care?
  - Example #2: Mrs. Jones doesn't want her OB/GYN to know that she has a history of alcoholism.
    - Mrs. Jones becomes pregnant
    - While the physician would likely have a conversation about alcohol consumption, it is unlikely that they would have a conversation about fetal alcohol syndrome or treatment options to try and protect the unborn child.

Questions?

Tina Olson Grande
Chair, Confidentiality Coalition
750 9th Street, NW, Suite 500
Washington, DC 20001
tgrande@hlc.org

www.confidentialitycoalition.org