Review of Systems
a practice workshop

Review of Systems: A Practice Workshop

How to Reduce Risk Related to Documentation

North Carolina Psychiatric Association
April 25, 2015

Donna L. Vanderpool, MBA, JD
Vice President, Risk Management
Professional Risk Management Services, Inc. (PRMS)

NORTH CAROLINA
Psychiatric
Association

CME Financial Disclosures

Ms. Vanderpool has no relevant financial relationships with any commercial interest.

Objectives

At the conclusion of this presentation, participants will be able to:

- Name three ways to reduce risk related to documentation of CPT coding.

Review of the Basics

Purposes and Uses of Medical Records

- **CLINICAL**
  - Patient history, treatment and continuity of care
  - Communication among healthcare professionals about the patient's care
  - Documentation of the standard of care provided
  - Research data – clinical outcomes, public health, etc.
  - Other
- **LEGAL**
  - Evidence in malpractice and other types of litigation
  - Evidence in administrative action by licensing board
  - Used in medical audits, peer review evaluations, etc.
  - Documentation of compliance with state licensing laws re: documentation/recordkeeping
  - Documentation of adherence to policies and procedures
  - Other
- **REIMBURSEMENT/BILLING**
  - Substantiates services rendered
  - Documents adherence to insurers' guidelines

Documentation

GOOD DOCUMENTATION HAS ALWAYS BEEN PART OF GOOD CLINICAL CARE

Documentation

Ideally, documentation should accomplish the following:

- It should substantiate clinical judgment and choices
- It should demonstrate the knowledge and skill exercised during treatment
- It should provide contemporaneous assessment of the patient's needs and behaviors
- It should document explanations of the treatment decisions, significant events, and revisions to the treatment plan
- Provide your most important defense in a medical malpractice lawsuit or an administrative action against your license

Take Away Point #1

Document your decision-making so you work can be understood by others (e.g., other providers, expert witnesses)

- What you did and why
- What you considered but rejected and why

Documentation

Risk Management Advice:

1. Documentation should be timely
2. Include a date for every entry
3. The patient's name should be on every page
4. Write or print legibly, if handwritten
5. Use only approved abbreviations
6. Document prudently
7. Correct the record appropriately

Documentation

Risk Management Advice (continued):

8. Document phone calls with and about patients
9. Document prescriptions and refills
10. Document when covering for a colleague
11. Document missed appointments
12. Documentation should be contemporaneous
13. DO NOT ALTER RECORDS

Documentation

The impact of altered records:

- They will be discovered
- Your credibility will be adversely affected
- It may be a criminal act
- It will compromise your professional liability insurance coverage

Documentation

Factors that provide evidence of the appropriate standard for documentation include:

- Statutes – federal and state
- Regulations – federal and state
- Case law
- Position papers, guidance documents, etc., from regulatory or administrative agencies (e.g., State Licen**ns**ing Board, CMS)
- Authoritative guidelines
- Position documents, policies, guidance documents of major professional organizations (e.g., AMA)
- Journal articles
- Medical staff bylaws
- Facility policies and procedures
- Standards of accreditation and quality assurance organizations

Documentation

From the NC Medical Board Position Statement on *Medical Record Documentation*:

Medical record should contain:

- An appropriate history and physical examination
- Results of ancillary studies
- Diagnoses
- Any plan for treatment

Documentation

From the NC Medical Board Position Statement on *Medical Record Documentation*:

The medical record is a chronological document that:

- Records pertinent facts about an individual's health and wellness;
- Enables the treating care provider to plan and evaluate treatments or interventions;
- Enhances communication between professionals, assuring the patient optimum continuity of care;
- Assists both patient and physician to communicate to third party participants
- Allows the physician to develop an ongoing quality assurance program
- Provides a legal document to verify the delivery of care; and
- Is available as a source of clinical data for research and education

Documentation

From the NC Medical Board Position Statement on *Medical Record Documentation*:

The following required elements should be present in all medical records:

- The record reflects the purpose of each patient encounter and appropriate information about the patient’s history and examination, and the care and treatment provided are described.
- The patient’s past medical history is easily identified and includes serious accidents, operations, significant illnesses and other appropriate information.
- Medication and other significant allergies, or a statement of their absence, are prominently noted in the record.
- When appropriate, informed consent obtained from the patient is clearly documented.
- All entries are dated.

Documentation

APA Practice Guideline for the Treatment of Patients With Suicidal Behaviors

From Part A (v); Table 9- General Risk Management and Documentation Considerations in the Assessment and Management of Patients at Risk of Suicide

… Careful and attentive documentation, including:

- Risk assessments
- Record of decision-making processes
- Descriptions of changes in treatment
- Record of communications with other clinicians
- Record of telephone calls from patients or family members
- Prescription log or copies of actual prescriptions
- Medical records of previous treatment, if available, particularly treatment related to past suicide attempts

No Documentation

- Sometimes the decision not to document is a considered one
  - But very risky

- Case law
  - Failure to document = inference that treatment fell below the standard of care

How To:

*** Keep Your Hard Earned Money,**

*** Keep Your Patients Safe, and**

*** Stay Out of Court**

Significance of EHRs

- Increased risk related to regulatory violations
  - Coding risk
  - Data protection risk – federal and state
- Increased risk related to patient safety
- Increased risk related to defense of malpractice allegations

Significance of EHRs

EHR vendors agree and admit:

EHRs were never designed to be printed

- Designed to be very fluid and self-correcting
- What one type of provider sees in the EHR may be very different from what other types of providers see
- Printed version doesn't always show everything

Risk Related to Regulatory Violations

Coding Risks

The False Claims Act (FCA)

Protects the Federal Government from being overcharged or sold substandard goods or services

- Imposes civil liability on any person who ***knowingly*** submits, or causes to be submitted, a false or fraudulent claim
  - "knowing" standard includes acting in deliberate ignorance or reckless disregard of the truth or falsity of the information related to the claim
    - Ex: billing Medicare for services not provided

The False Claims Act (FCA)

Protects the Federal Government from being overcharged or sold substandard goods or services

- Civil penalties:
  - Fines up to THREE times the amount of damages sustained by the Government as a result of the false claims
  - PLUS $11,000 per claim filed
- Criminal penalties:
  - Fines, imprisonment, or both

The False Claims Act (FCA)

Protects the Federal Government from being overcharged or sold substandard goods or services

- Covers items and services rendered to Medicare beneficiaries
- Many similar state laws apply to the provision of care under state-financed programs and to private-pay patients

The False Claims Act (FCA)

From CMS:

“**When you submit a claim for services performed for a Medicare patient, you are filing a bill with the Federal Government and certifying that you earned the payment requested and complied with billing requirements.** If you knew or should have known that the submitted claim was false, then the attempt to collect unearned money constitutes a violation. Examples of improper claims include:

- Billing for services that you did not actually render;
- Billing for services that were not medically necessary;
- Billing for services performed by an improperly supervised or unqualified employee;
- Billing for services of such low quality that they are virtually worthless…”

CMS, Avoiding Medicare Fraud & Abuse: A Roadmap for Physicians, 2014, http://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/avoiding_medicare_fanda_physicians_factsheet_905645.pdf

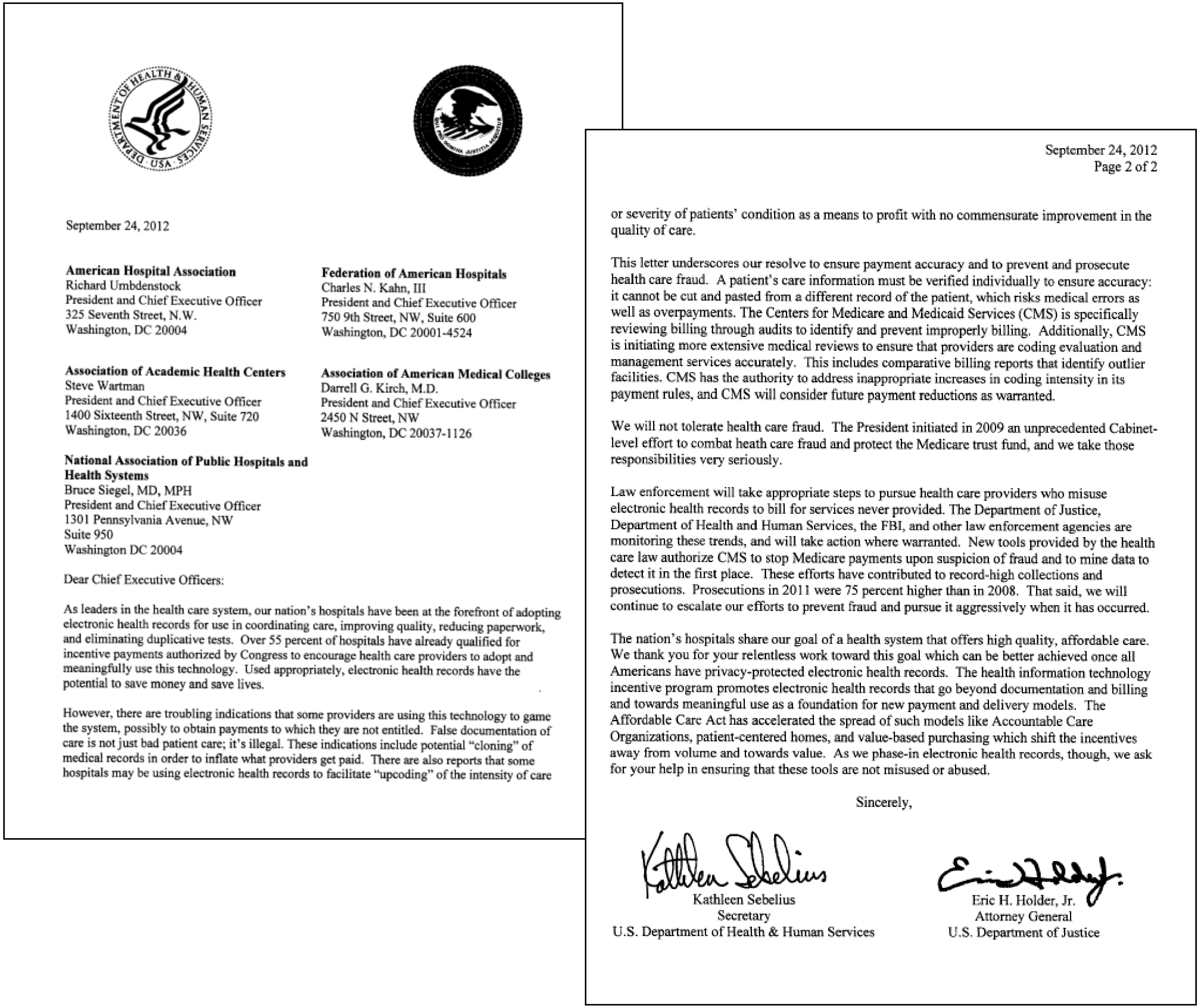
Increased Scrutiny

- NYT article from September 21, 2012: "Medicare Bills Rise as Records Turn Electronic"
- Use of EHRs is increasing
- Number of high level E/M services billed for is increasing
- These higher level services may be substantiated by EHR documentation
- But the validity of the documentation is being questioned by government and private payers

Take Away Point #2

Understand that the fact that the EHR can create documentation addressing the coding requirements for the highest code does not mean it is appropriate to bill the highest code

Medical necessity is the key to accurate coding, *even if a coding tool suggests a higher lever of service*



September 24, 2012

American Hospital Association
Richard Umbdenstock
President and Chief Executive Officer
325 Seventh Street, N.W.
Washington, DC 20004

Federation of American Hospitals
Charles N. Kahn, III
President and Chief Executive Officer
750 9th Street, NW, Suite 600
Washington, DC 20001-4524

Association of Academic Health Centers
Steve Wartman
President and Chief Executive Officer
1400 Sixteenth Street, NW, Suite 720
Washington, DC 20036

Association of American Medical Colleges
Darrell G. Kirch, M.D.
President and Chief Executive Officer
2450 N Street, NW
Washington, DC 20037-1126

National Association of Public Hospitals and Health Systems
Bruce Siegel, MD, MPH
President and Chief Executive Officer
1301 Pennsylvania Avenue, NW
Suite 950
Washington DC 20004

Dear Chief Executive Officers:

As leaders in the health care system, our nation's hospitals have been at the forefront of adopting electronic health records for use in coordinating care, improving quality, reducing paperwork, and eliminating duplicative tests. Over 55 percent of hospitals have already qualified for incentive payments authorized by Congress to encourage health care providers to adopt and meaningfully use this technology. Used appropriately, electronic health records have the potential to save money and save lives.

However, there are troubling indications that some providers are using this 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. These indications include potential "cloning" of medical records in order to inflate what providers get paid. There are also reports that some hospitals may be using electronic health records to facilitate "upcoding" of the intensity of care

September 24, 2012
Page 2 of 2

or severity of patients' condition as a means to profit with no commensurate improvement in the quality of care.

This letter underscores our resolve to ensure payment accuracy and to prevent and prosecute health care fraud. 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. The Centers for Medicare and Medicaid Services (CMS) is specifically reviewing billing through audits to identify and prevent improperly billing. Additionally, CMS is initiating more extensive medical reviews to ensure that providers are coding evaluation and management services accurately. This includes comparative billing reports that identify outlier facilities. CMS has the authority to address inappropriate increases in coding intensity in its payment rules, and CMS will consider future payment reductions as warranted.

We will not tolerate health care fraud. The President initiated in 2009 an unprecedented Cabinet-level effort to combat heath care fraud and protect the Medicare trust fund, and we take those responsibilities very seriously.

Law enforcement will take appropriate steps to pursue health care providers who misuse electronic health records to bill for services never provided. The Department of Justice, Department of Health and Human Services, the FBI, and other law enforcement agencies are monitoring these trends, and will take action where warranted. New tools provided by the health care law authorize CMS to stop Medicare payments upon suspicion of fraud and to mine data to detect it in the first place. These efforts have contributed to record-high collections and prosecutions. Prosecutions in 2011 were 75 percent higher than in 2008. That said, we will continue to escalate our efforts to prevent fraud and pursue it aggressively when it has occurred.

The nation's hospitals share our goal of a health system that offers high quality, affordable care. We thank you for your relentless work toward this goal which can be better achieved once all Americans have privacy-protected electronic health records. The health information technology incentive program promotes electronic health records that go beyond documentation and billing and towards meaningful use as a foundation for new payment and delivery models. The Affordable Care Act has accelerated the spread of such models like Accountable Care Organizations, patient-centered homes, and value-based purchasing which shift the incentives away from volume and towards value. As we phase-in electronic health records, though, we ask for your help in ensuring that these tools are not misused or abused.

Sincerely,

Kathleen Sebelius
Kathleen Sebelius
Secretary
U.S. Department of Health & Human Services

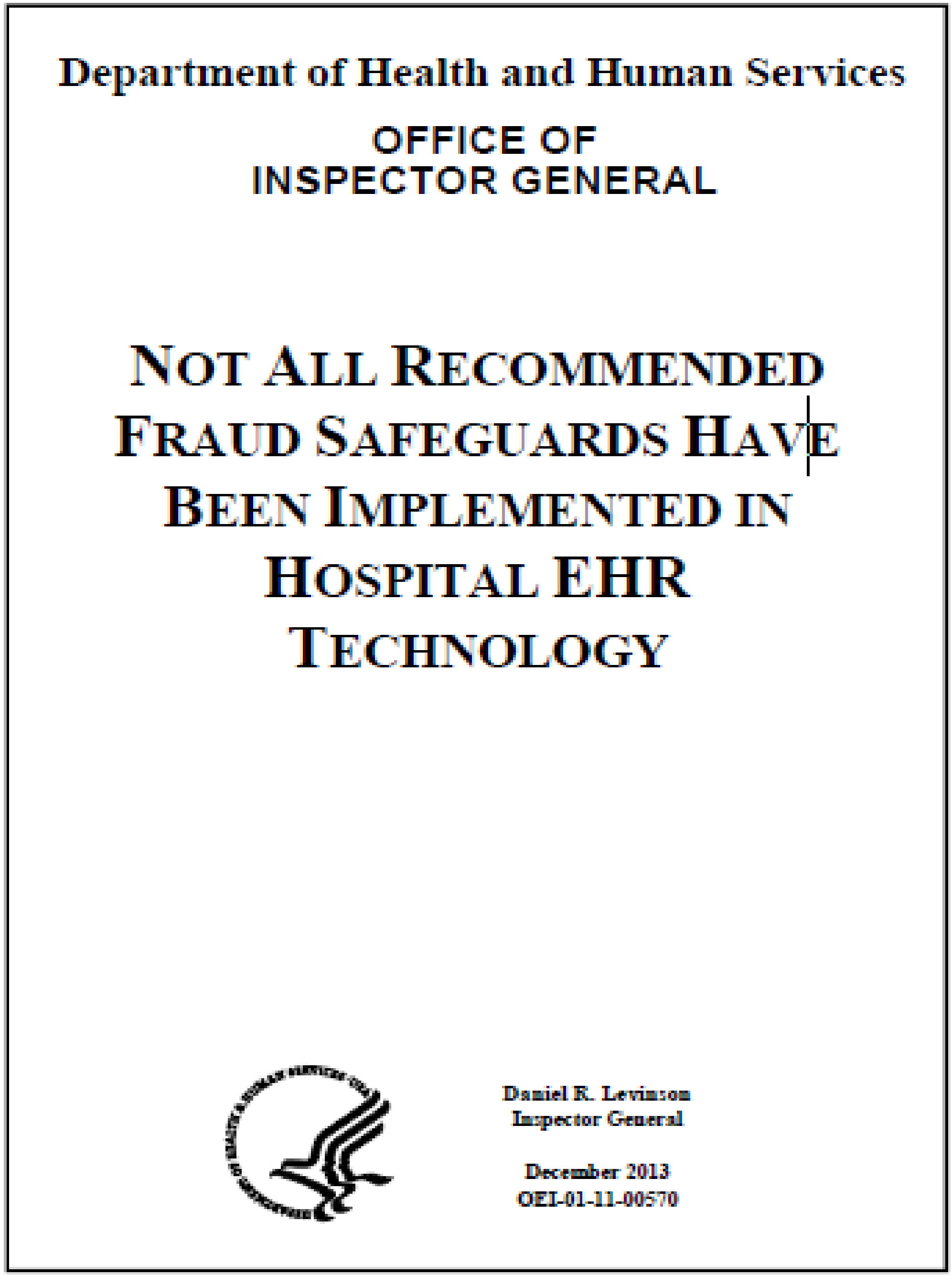
Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice

Increased Scrutiny

New York Times article on September 24, 2012:

"U.S. Warning to Hospitals on Medicare Bill Abuses"

- "…some providers are using this technology to game the system, possibly to obtain payments to which they are not entitled. False documentation of care is not just bad care; it's illegal."
- Cloning
  - "a patient's medical information 'must be verified individually to ensure accuracy; it cannot be cut and paste from a different record of the patient, which risks medical errors as well as overpayments"
- Upcoding
- "Regulators, including the Office of Inspector General for Health and Human Services, are concerned about the increase in billing for the most expensive evaluation services by hospitals, in the emergency room, and by doctors in their offices. Private insurers have also expressed concern about the higher level of billing."



Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology

Daniel R. Levinson
Inspector General

December 2013
OEI-01-11-00570

OIG Report (2013)

Two examples of EHR documentation practices that could be used to commit fraud:

Copy-Pasting (aka "cloning"):

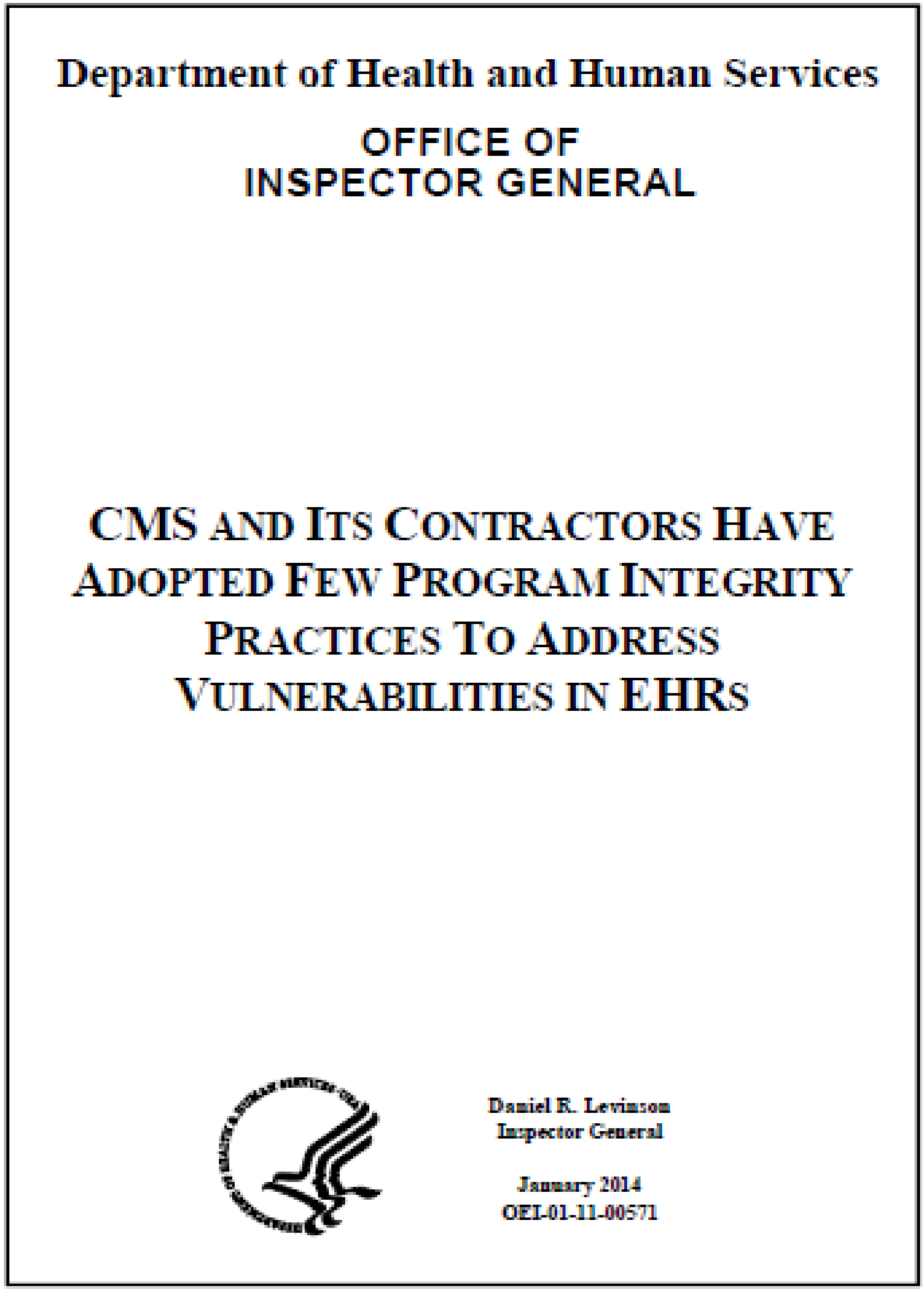
- Allows users to select information from one source and replicate it in another location
- When clinicians copy-paste information but fail to update it or ensure accuracy, inaccurate information may enter the medical record and inappropriate charges may be billed to patients and third party health care payers
- Inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims

OIG Report (2013)

Two examples of EHR documentation practices that could be used to commit fraud:

Over-documentation:

- Is the practice of inserting false or irrelevant documentation to create the appearance of support for billing higher level services
  - Some EHRs auto-populate fields when using templates
  - Other EHRs generate extensive documentation on the basis of a single click of a checkbox, which if not appropriately edited by the clinician, may be inaccurate
- Such features can produce information suggesting the clinician performed more comprehensive services than were actually rendered



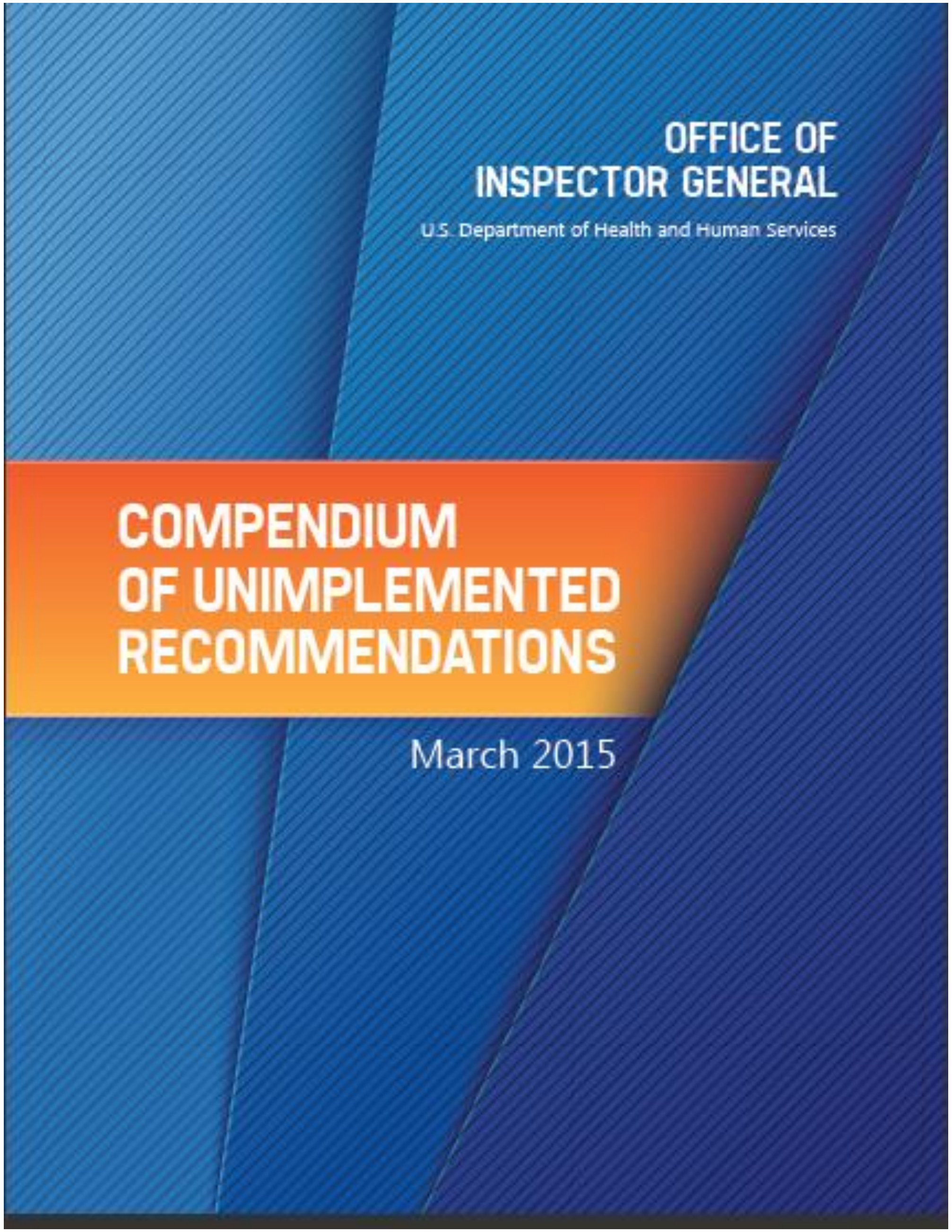
Department of Health and Human Services

OFFICE OF
INSPECTOR GENERAL

CMS AND ITS CONTRACTORS HAVE ADOPTED FEW PROGRAM INTEGRITY PRACTICES TO ADDRESS VULNERABILITIES IN EHRS

Daniel R. Levinson
Inspector General

January 2014
OEI-01-11-00571



OFFICE OF
INSPECTOR GENERAL

U.S. Department of Health and Human Services

COMPENDIUM OF UNIMPLEMENTED RECOMMENDATIONS

March 2015

Health Information Technology

Medicaid	■ Establish a deadline for when national T-MSIS data will be available. ■ Ensure that States submit required T-MSIS data. ■ Ensure that T-MSIS data are complete, accurate, and timely upon T-MSIS implementation.	CMS	**Expected Impact:** Improved program management	*Early Outcomes Show Limited Progress for the Transformed Medicaid Statistical Information System.* OEI-05-12-00610. **2013 SEP.**
Electronic Health Records	■ Audit logs should be operational whenever EHR technology is available for updates or viewing. ■ ONC and CMS should strengthen their collaborative efforts to develop a comprehensive plan to address fraud vulnerabilities in EHRs. ■ CMS should develop guidance on the use of the copy-paste feature in EHR technology.	CMS, ONC	**Expected Impact:** Improved program integrity	*Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology.* OEI-01-11-00570. **2013 DEC.**
	■ CMS should provide guidance to its contractors on detecting fraud associated with EHRs. ■ CMS should direct its contractors to use providers' audit logs.	CMS	**Expected Impact:** Improved program integrity	*CMS and Its Contractors Have Adopted Few Program Integrity Practices To Address Vulnerabilities in EHRs.* OEI-01-11-00571. **2014 JAN.**

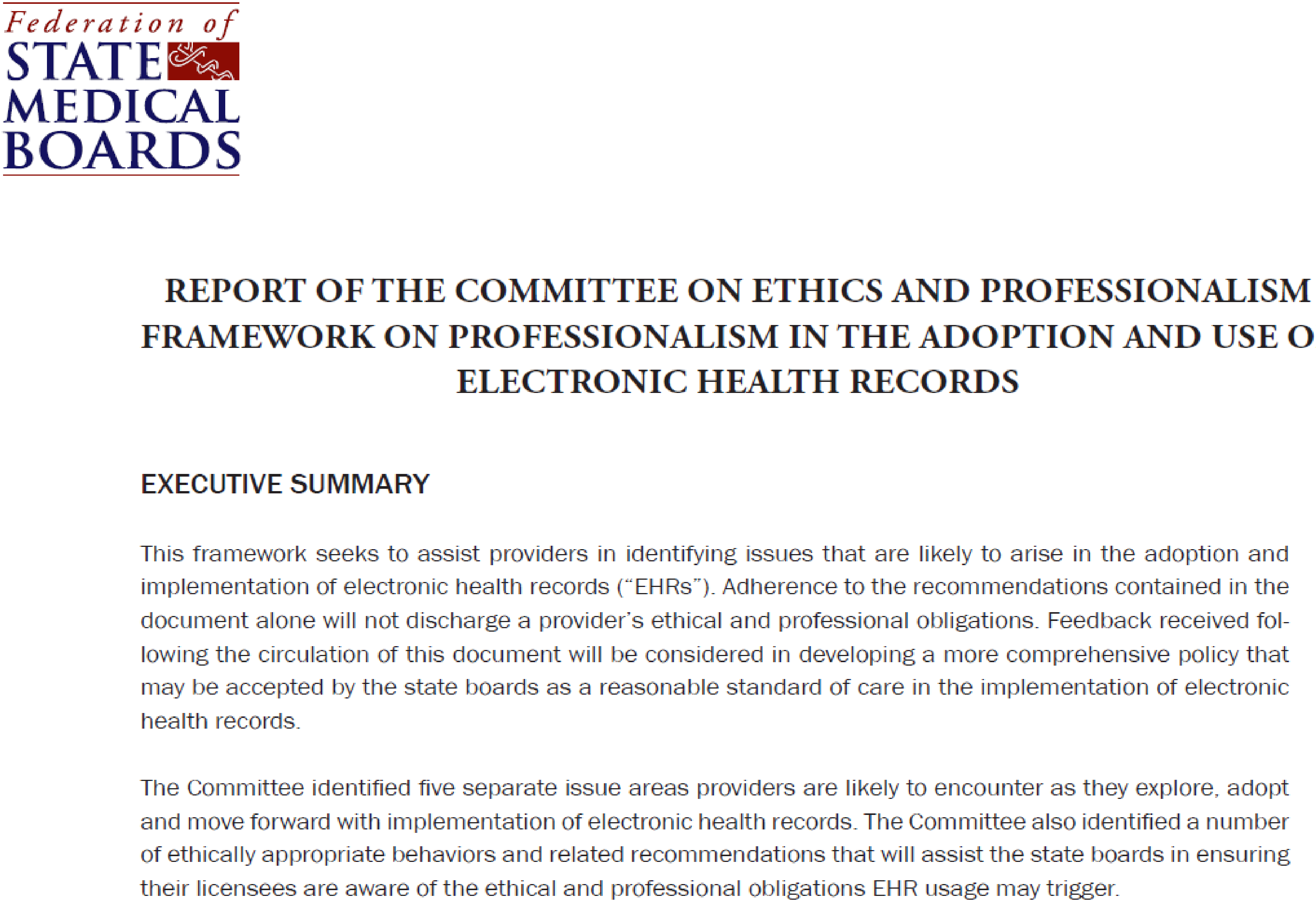
OIG Compendium of Unimplemented Recommendations, March 2015, http://oig.hhs.gov/reports-and publications/compendium/files/compendium2015.pdf

Documentation

From the NC Medical Board Position Statement on *Medical Record Documentation*:

The following additional elements reflect commonly accepted standards for medical record documentation:

1. Each page in the medical record contains the patient's name or ID number.
2. Personal biographical information such as home address, employer, marital status, and all telephone numbers, including home, work, and mobile phone numbers.
3. All entries in the medical record contain the author's identification. Author identification may be a handwritten signature, initials, or a unique electronic identifier.
4. All drug therapies are listed, including dosage instructions and, when appropriate, indications of refill limits. Prescriptions refilled by phone should be recorded.
5. Encounter notes should include appropriate arrangements and specified times for follow-up care.
6. All consultation, laboratory and imaging reports should be entered into the patent's record, reviewed, and the review documented by the practitioner who ordered them. Abnormal reports should be noted in the record, along with corresponding follow-up plans and actions taken…



Federation of
STATE
MEDICAL
BOARDS

REPORT OF THE COMMITTEE ON ETHICS AND PROFESSIONALISM FRAMEWORK ON PROFESSIONALISM IN THE ADOPTION AND USE OF ELECTRONIC HEALTH RECORDS

EXECUTIVE SUMMARY

This framework seeks to assist providers in identifying issues that are likely to arise in the adoption and implementation of electronic health records ("EHRs"). Adherence to the recommendations contained in the document alone will not discharge a provider's ethical and professional obligations. Feedback received following the circulation of this document will be considered in developing a more comprehensive policy that may be accepted by the state boards as a reasonable standard of care in the implementation of electronic health records.

The Committee identified five separate issue areas providers are likely to encounter as they explore, adopt and move forward with implementation of electronic health records. The Committee also identified a number of ethically appropriate behaviors and related recommendations that will assist the state boards in ensuring their licensees are aware of the ethical and professional obligations EHR usage may trigger.

http://www.fsmb.org/Media/Default/PDF/FSMB/Advocacy/ehr_framework_final_adopted.pdf
Accessed July 29,2014

Documentation “Short Cuts”

Other ways to automate documentation:

- Templates
- Pre-populated fields
- Default data
- Documenting by exception
- Etc.

Documentation

From the NC Medical Board Position Statement on *Medical Record Documentation*:

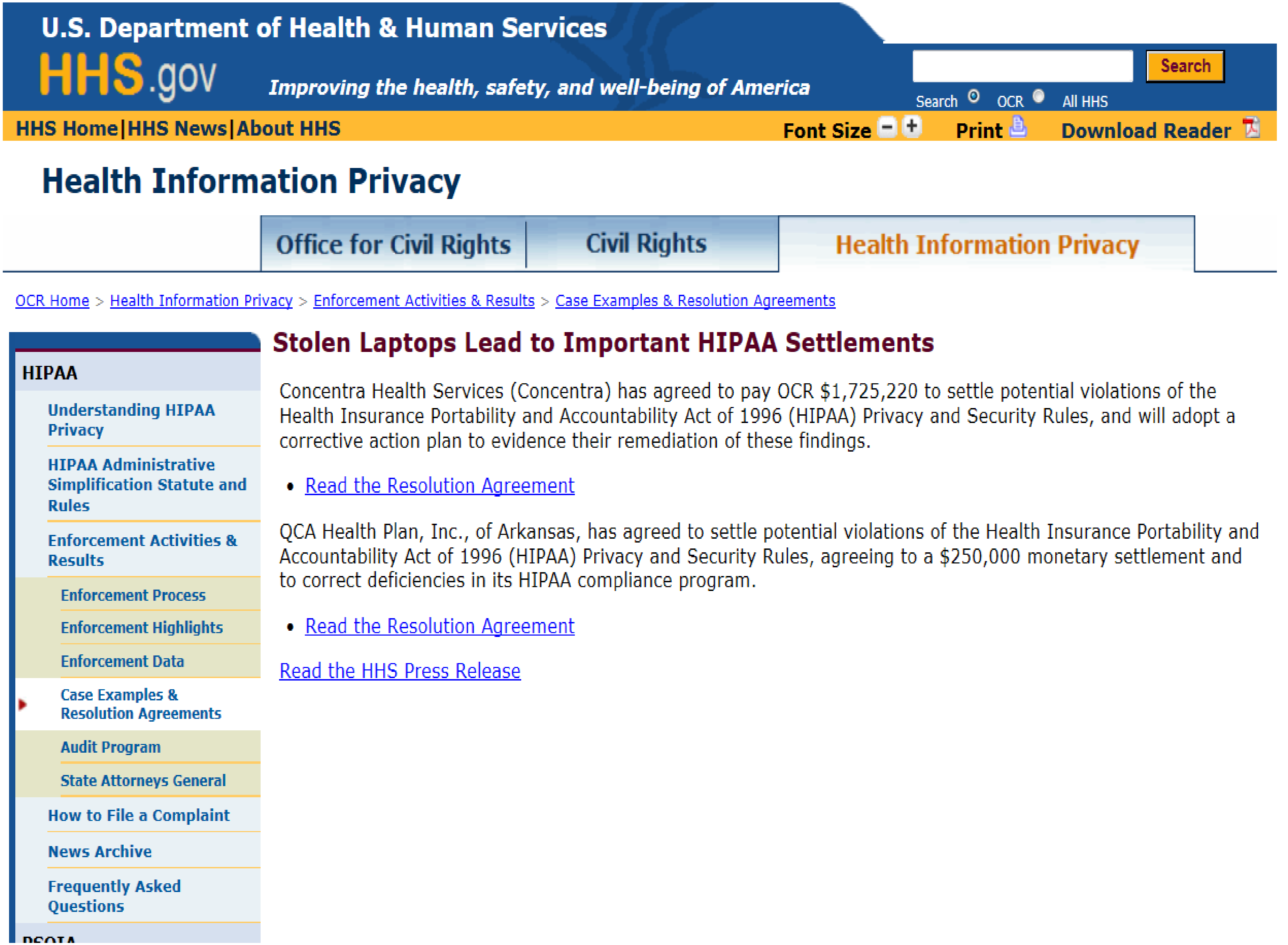
"The Board recognizes and encourages the trend towards the use of electronic medical records (EMR). However, the Board cautions against relying upon software that pre-populates particular fields in the EMR without updating those fields in order to create a medical record that accurately reflects the elements delineated in the Position Statement."

Documentation "Short Cuts"

Automated documentation:

- Automated entry ≠ documented
- Unable to distinguish between data entered by clinician and system-entered data
- Documentation must be specific to the patient and to the services provided
- Clinicians are responsible for the accuracy of documentation

Data Protection Risks


U.S. Department of Health & Human Services
HHS.gov
Improving the health, safety, and well-being of America
Search
Search ○ OCR ○ All HHS
HHS Home|HHS News|About HHS
Font Size − +
Print
Download Reader
Office for Civil Rights
Civil Rights
Health Information Privacy
HIPAA
Understanding HIPAA Privacy
HIPAA Administrative Simplification Statute and Rules
Enforcement Activities & Results
Enforcement Process
Enforcement Highlights
Enforcement Data
Case Examples & Resolution Agreements
Audit Program
State Attorneys General
How to File a Complaint
News Archive
Frequently Asked Questions
PSQIA

Health Information Privacy

OCR Home > Health Information Privacy > Enforcement Activities & Results > Case Examples & Resolution Agreements

Stolen Laptops Lead to Important HIPAA Settlements

Concentra Health Services (Concentra) has agreed to pay OCR $1,725,220 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, and will adopt a corrective action plan to evidence their remediation of these findings.

- Read the Resolution Agreement

QCA Health Plan, Inc., of Arkansas, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, agreeing to a $250,000 monetary settlement and to correct deficiencies in its HIPAA compliance program.

- Read the Resolution Agreement

Read the HHS Press Release

Protect Yourself | Protect Your Identity | Protect Your Business From ID Theft | Security Breach Information

SECURITY BREACH INFORMATION

Security Breach: Your Requirements

The Identity Theft Protection Act requires businesses and state and local government to notify people when there is a security breach involving their personal identifying information. More than 2,200 breaches that involved information about more than 6 million North Carolina consumers have been reported to the Attorney General's Office since 2005.

What is a Security Breach?

A “security breach” is defined as the unauthorized release of unencrypted or unredacted records or data containing personal information with corresponding names, such as a person’s first initial and last name. The acquisition of encrypted data only is a breach if a confidential process or key needed to unlock the data is also breached.

The authorized access of personal information by an employee or agent is not considered a security breach so long as the information is used for a lawful purpose.

Personal Information

Personal information includes: an individual’s Social Security number (SSN), employer taxpayer identification number (TIN), driver’s license or state identification number, passport number, checking/saving account number, credit/debit card number, PIN, digital signature, biometric data, fingerprints or any number that can be used to access his financial resources.

Get Help & Find Answers

Received a Security Breach Letter?

ID Theft Victim Kit

Take Action

Report a Security Breach

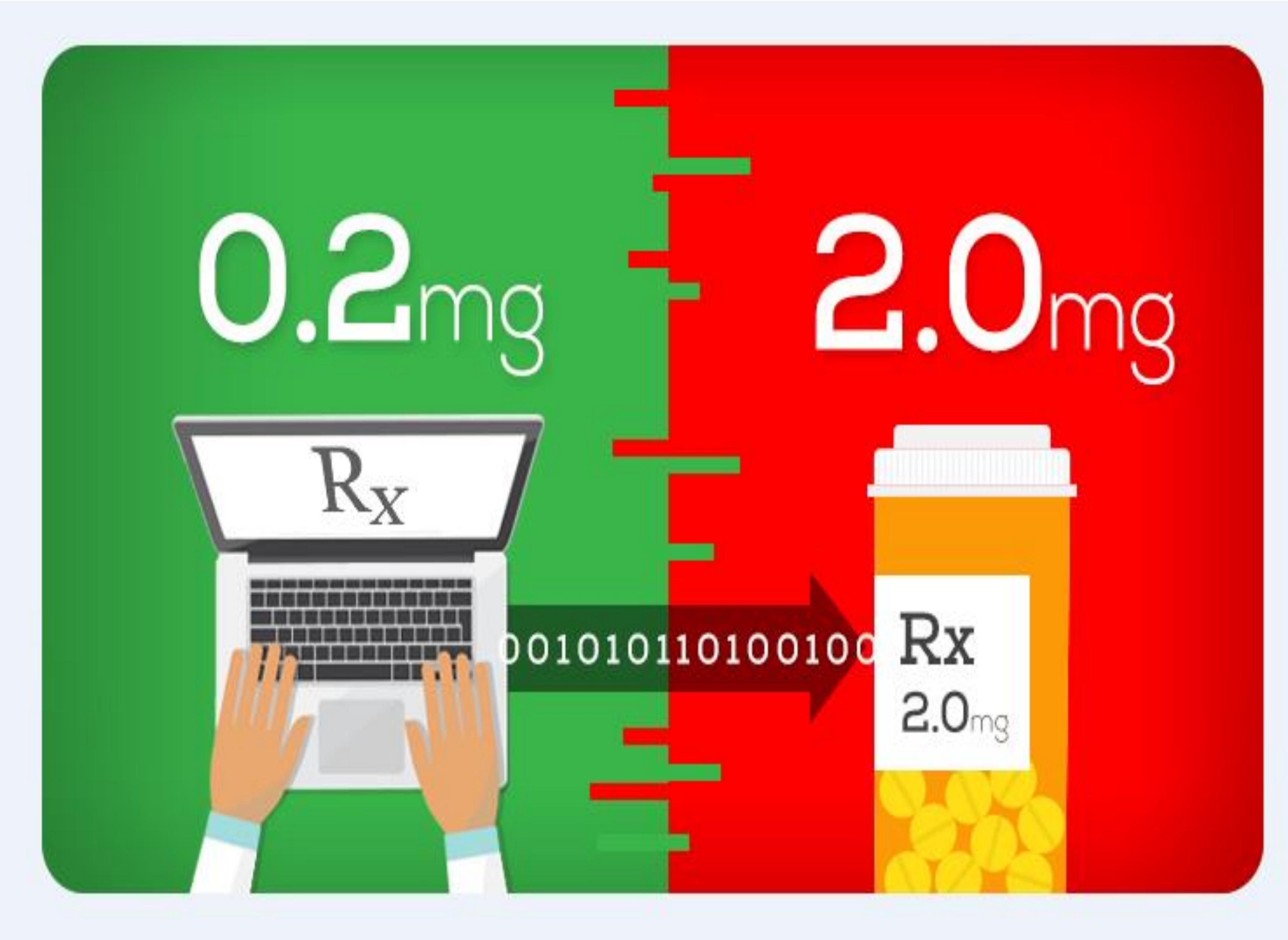
News and Events

Free shred-a-thons planned statewide this spring, AG Cooper says

Chapel Hill landlord ordered to pay $122,000 in refunds, penalties

Public invited to learn about new Western Regional Crime Lab

+more



0.2mg
2.0mg
Rx
0010101101001oo
Rx
2.0mg

Risk Related to Patient Safety

Sentinel Event Alert

A complimentary publication of The Joint Commission
Issue 54, March 31, 2015

Safe use of health information technology

Health information technology (health IT) is rapidly evolving and its use is growing, presenting new challenges to health care organizations. This alert builds upon *Sentinel Event Alert #42* on safely implementing health information and converging technologies (published in 2008) to take a broader look at health IT, particularly the socio-technical factors having an impact on its safe use. This alert's suggested actions center on safety culture, process improvement and leadership.

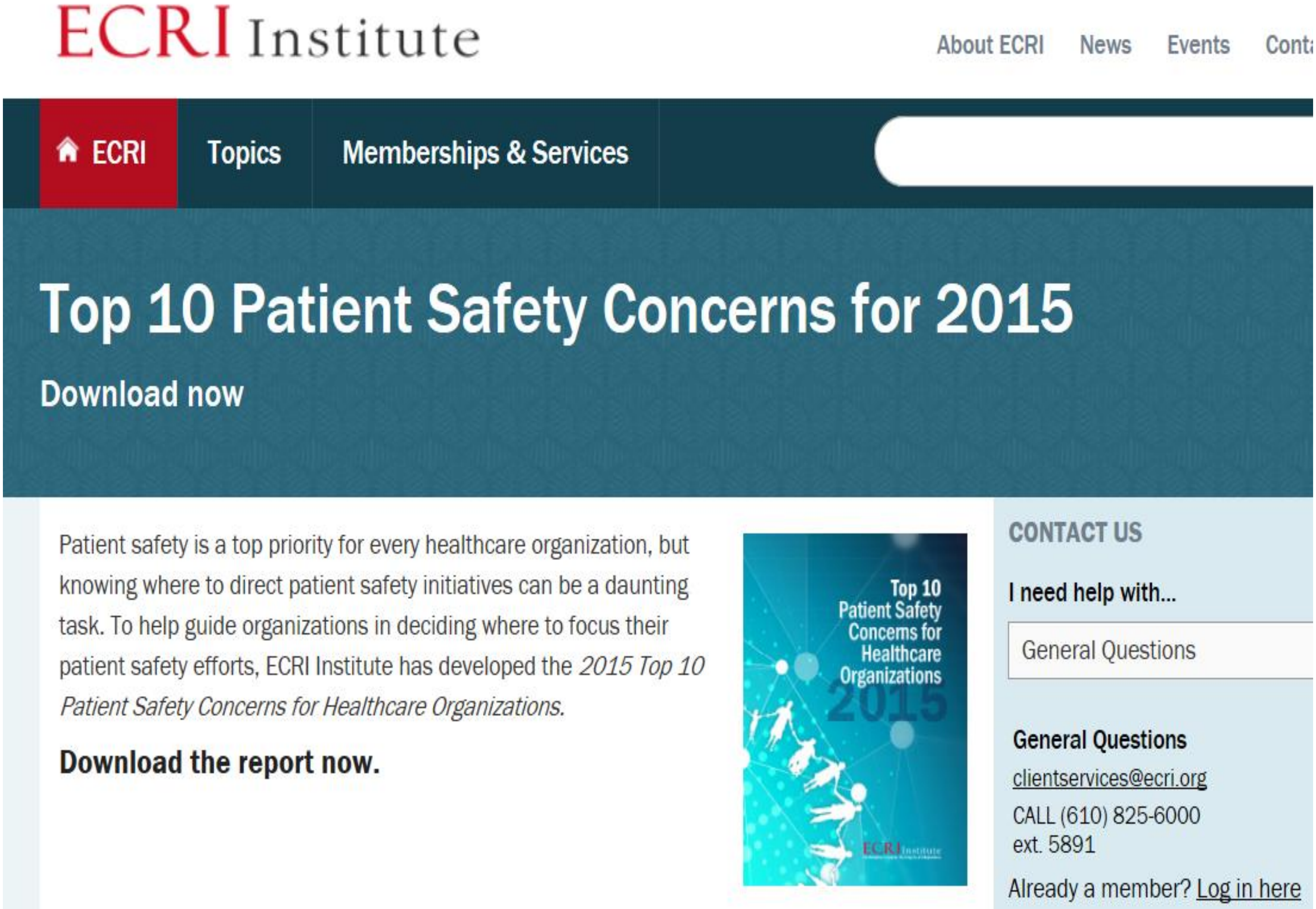
Incorrect or miscommunicated information entered into health IT systems may result in adverse events. In some cases, interfaces built into the technology contribute to the events. The following examples obtained from ECRI Institute[1] show a few ways adverse events may occur through the use of electronic health records (EHRs) and related technologies:

- A chest X-ray was ordered for the wrong patient when the wrong patient room number was accidentally clicked. The orderer noticed the error right away and promptly discontinued the order, but not in time for the X-ray technician to see that the order was withdrawn. The technician performed the test on the wrong patient.
- A drug was ordered as an intramuscular injection when it was supposed to be administered intravenously. The physician did not choose the appropriate delivery route from the drop-down menu.
- A nurse noted that a patient had a new order for acetaminophen. After speaking with the pharmacist, the nurse determined that the order was placed for the wrong patient. The pharmacist had two patient records open, was interrupted, and subsequently entered the order for the wrong patient.

Published for Joint Commission accredited organizations and interested health care professionals, *Sentinel Event Alert* identifies specific types of sentinel and adverse events and high risk conditions, describes their common underlying causes, and recommends steps to reduce risk and prevent future occurrences.

Accredited organizations should consider information in a *Sentinel Event Alert* when designing or redesigning processes and consider implementing relevant suggestions contained in the alert or reasonable alternatives.

Please route this issue to appropriate staff within your organization. *Sentinel Event Alert* may only be reproduced in its entirety and credited to The Joint Commission. To receive by email, or to view past issues, visit www.jointcommission.org.



Top 10 Patient Safety Concerns for 2015

Download now

Patient safety is a top priority for every healthcare organization, but knowing where to direct patient safety initiatives can be a daunting task. To help guide organizations in deciding where to focus their patient safety efforts, ECRI Institute has developed the *2015 Top 10 Patient Safety Concerns for Healthcare Organizations.*

Download the report now.

CONTACT US

I need help with...

General Questions

General Questions

clientservices@ecri.org

CALL (610) 825-6000
ext. 5891

Already a member? Log in here

EHRs and Patient Safety

Potential Problems

- “Box checking” may eliminate clinically necessary information from the narrative
- Copy and paste may perpetuate error
  - New information may be difficult to discern – it all looks the same
- Too much information may cause data to be missed

EHRs and Patient Safety

Potential Problems

- May be difficult to correct or amend record
  - Changes may not be adjacent to the old
- Templates may not actually reflect what occurred during treatment
  - A large number of identical notes will suggest provider wasn't thorough
  - If too detailed, may appear invalid

Risk Related to Malpractice

EHRs and Liability

Clinician Liability

- Expert witness
  - Relies, to a great degree, on clinical record
- Professional Judgment Rule
  - Courts will give great deference to treating provider IF there is something to base that deference on
    - Contemporaneous documentation
- Templates
  - All records look the same
  - Defendant provider loses credibility

EHRs and Liability

Clinician Liability

- Metadata
  - Keeps track of everything user does, and how long it takes to do it
  - Is discoverable
- Printed record
  - EHRs do not look the same on paper
  - EHRs may not contain all information in EHR

EHRs and Liability

Clinician Liability

- Physician time constraints and information overload
- Reliance on others' diagnosis and treatment decisions
- Input errors
- The challenges of decision support
- …

Source: E-Health Hazards: Provider Liability and Electronic Health Record Systems, Hoffman S. and Podgurski A., Berkeley Technology Law Journal 2009:24:4

EHRs and Liability

Clinician Liability

- Be very careful when documenting in the EHR
  - Take your time and see what actual documentation is created
- Review the entry before closing it
- "The chart you are documenting may be the one you will be called on to defend on the witness stand."

*Avoid the Dark Side of EHR Documentation***,** AAPC Coding Edge, Feb. 2011

Take Away Point #3

Consider taking the following steps related to EHR documentation:

- Ensure templates used are appropriate for the specific patient
- Disable the cut and paste function
  - If you allow this function, require author identification
- Do not allow pre-populated fields
- Do not allow auto population
- Include space for free-form text
- Periodically print out a record and review
  - Any technical glitches?
  - Would it pass a billing audit?
  - Would a subsequent treater or an expert witness understand what you did and why?