Openness and Exactness – Mitigating Fraud Vulnerabilities in the Age of EHRs and ICD-10

Bill Fox, Senior Director Market Planning Healthcare
LexisNexis Risk Solutions

Jim Sheehan, Chief Integrity Officer/Exec. Dep. Comm.
New York City Human Resources Administration

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.
Learning Objectives

- Describe opportunities for fraud, waste and abuse inherent in the industry move to electronic exchange of health information and the more complex coding of ICD-10.
- Discuss the implications of failing to take steps to mitigate the risk of fraud, waste and abuse in the ICD-10 and electronic exchange environment.
- Identify strategies for avoiding fraud, waste and abuse in the ICD-10 and electronic exchange environment.
Future Shock

A personal perception of too much change in too short a period of time.

Alvin Toffler
As quoted in New Scientist 03/19/1994
ICD-10  Health Insurance Exchanges
PHRs  Experiencing Future
Health Information Shock
Exchange  EHRs
Health Care Reform
ACOs
This sea change has the potential to create even more fraud, waste and abuse if not properly managed

- Change is no longer perceived as an option but a “must do.”
- Escalating costs are pushing the health care system to make rapid and sweeping changes
- In the drive to get things done, quality and risk mitigation may be become unintentional casualties.
Challenges Facing the Health Care Industry
Health Care Fraud

misstatement of facts – either knowingly or through unreasonable ignorance – that leads to unfair profit through medical coverage
Health care’s emerging electronic environment, coupled with the complexity of the ICD-10 coding system creates unprecedented opportunity for fraud and abuse.

- Potential coding issues related to ICD-10
- Unauthorized users may gain access to PHI through HIEs
- E-visit environment vulnerable to fraudsters who may assume someone else’s identity to gain access to services
- Fraudulent PHI can be spread across the health care continuum with lightening speed through EMRs and electronic health information exchange
Provider Health Care Fraud – Just “a few bad Docs”?

The American Society of Business and Behavioral Sciences estimates that 80% of health care fraud is committed by hospitals, clinics and medical professions\(^1\)

- According to an April 2000 article published in the *MS Journal of the American Medical Association*\(^2\):
  - 39% of providers surveyed admitted they sometimes exaggerate a patient's symptoms, report symptoms the patient did not have, or change the diagnosis so the patient's insurance company will pay the claim
- Monetary harm estimated to be between $50B and $250B per year – at least

---


Example of Provider Health Care Fraud – Is this happening in your organization?

- Billing for services not performed
- Billing for duplicate times for one service performed
- Falsifying a diagnosis
- Misrepresenting procedures (billing for a covered service when a non-covered service was performed)
- Upcoding – billing for a more costly service than was performed
- Accepting kickbacks for patient referrals
- Waiving co-pays or deductible amounts and overbilling insurance plan
Medical Identity Theft — Scope of the Problem

- According to World Privacy Forum, stolen medical information has 50 times more street value than a stolen social security number
  - Street cost for stolen social security number is $1.00
  - Street cost for stolen medical identity information is $50.00
- On average, criminals use information from medical records to commit fraud for 320 days as opposed to 81 days of misuse of information from other types of identity theft\(^1\)
- Accounts for approximately 3% of all identity crimes and is 10 times more expensive than financial identity theft
  - Average payout for financial identity theft is $2,000
  - Average payout for medical identity theft is $20,000
- According to NHCAA, 3% of all health care costs ($60 billion) is the result of fraud; of that 1% ($600 million) is attributed to medical identity theft

Medical Identity Theft – The Risks Are Increasing

- Between 2010 and 2011, the number of health care breaches increased by 32%¹
- Fraud resulting from exposure of health data has risen from 3% in 2008 to 7% in 2009, a 112% increase (Javelin Strategy and Research)²
- Nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of $28.6 billion. (Ponemon Institute)³
- As the use of EMRs, HIEs and HIX increase, victims of medical identity theft are at increased risk of receiving the wrong medical treatment or having their health insurance benefits exhausted

And the problem isn’t just thieves...

In a recent Ponemon Institute survey:\n\- 26% of those surveyed admitted they had shared their medical credentials with a family member  
\- 44% who shared their medical identity did it more than once  
\- 78% believed healthcare providers ensure the privacy of their health care records - but if 26% of those surveyed are successfully sharing their credentials with a family member, what does that say about how well medical information is being protected???

The Inherent Risks of Improved Technology
ICD-10 creates increased risks for providers
Key Date:  October 1, 2013

- The United States will begin official use of ICD-10 on October 1, 2013, using Clinical Modification ICD-10-CM for diagnosis coding and Procedure Coding System ICD-10-PCS for inpatient hospital procedure coding. All HIPAA "covered entities" must make the change.
- ICD-10 is much bigger with almost twice the categories of ICD-9.
- ICD-10 uses alphanumeric categories instead of numeric only.
- ICD-10 changed chapters, categories, titles and regrouped conditions.
- Like learning a new language, or converting to the metric system
ICD-10 Challenges for Providers

- Potential for double billing if two systems (ICD-9 and ICD-10) remain in use during transition period
- Could create unintentional FCA violation
- Shortage of experienced coding professionals
- Shortage already exists today
- Coders near retirement age may elect to retire rather than learn new system
- General Equivalency Mappings (GEMs) do not provide a definitive map from ICD-9 to ICD-10
- Only about 5% of all ICD-9 codes will map accurately 1:1 with ICD-10 codes
- One ICD-9 code often translates to several ICD-10 codes
- There may be multiple translations for a source system code, all of which are equally plausible
- ICD-10 conversions require manual review because of the significant differences in language and structure between ICD-9 and ICD-10
Transition Issues

- CMS on General Equivalence Mapping (GEM)
  - “There is no simple “crosswalk from I-9 to PCS” in the GEM files. A mapping that forces a simple correspondence—each I-9 code mapped only once—from the smaller, less detailed I-9 to PCS (a code set of entirely different design and scope) defeats the purpose of upgrading to PCS.”

- “. . .converting historical ICD-9 codes to ICD-10 is nearly impossible, since ICD-9 codes are translated to many ICD-10 codes and may require clusters of codes for accurate translations. “. . . in crosswalking from ICD-9 to ICD-10 only about 5% of codes will map completely accurately.

Transition Issues

- Edit system logic for payers
- Default system logic and drop-downs for provider systems
- Payment denials/pends in payment systems
- Payer policy documents:
  - “One of the following ICD-9-CM diagnosis codes must be billed with Halaven:
    - 174.0 through 175.9 (malignant neoplasm of the breast)”
- National Coverage determinations
- Local coverage decisions
- Pharmacy coverage policies
- Laboratory/Device/DME
- CMS/ State audit issues and articulated policies
- DRG/case mix severity measures
- Predictive modeling for psych, sex offenders
“Clinicians will have to provide much more detailed documentation to ensure correct coding using ICD-10-CM/PCS; failure to do so will likely result in increased workload for case managers and health record professionals, potentially delaying reimbursements and discharge planning for post-acute care, even after a “successful” conversion to the new ICD-10-CM/PCS coding system.”

Coming wave of change: ICD-10
J Pathol Inform. 2010
1: 28 Kim and Beckwith
“For most physicians, coding is viewed as a “necessary evil.” Codes are not generally considered a way of documenting or communicating the patient’s condition, but more so as a task to ensure payment...coding tasks and responsibilities are typically assigned to office staff who identify necessary codes..used in preparing and submitting health insurance claims...the operational disconnect between the code and the physician result in ‘suboptimal’ coding quality.”

Joseph Nicols, MD
Medical Group Strategy Council
The Advisory Board Company
March 2011
The complexity of the audit world

- Existing state audit agencies and contractors – NY OMIG, NJ Controller, Pa. DPW, UMass
- HHS-OIG
- Law enforcement agencies with audit authority (Medicaid Fraud Control Units, US Attorney Offices)
- Medicaid Integrity Contractors (2008)
- Medicaid RACs (2011-12)
The complexity of the audit world

How are audit entities accountable?

- MIC (Medicaid Integrity Contractors)-reimbursed on a fee for service basis by CMS-keep the customer (CMS) satisfied
- RAC –reimbursed on a % of recoveries basis by state Medicaid-maximize recoveries consistent with state rules
- Medicaid Fraud Control Units-responsive to the agenda of the elected Attorney General who supervises them
- State program integrity agencies within Medicaid-deal with elected state officials, often supervised by State Medicaid Director-but must also comply with CMS regulatory requirements of Medicaid Integrity Program
- CMS Medicaid Program Integrity-subject to 2006 Deficit Reduction Act requirements and Congressional oversight (including GAO)
- Department of Justice-HEAT initiative, whistleblower enforcement
Medicare ~10% error rate using ICD-9 coding

- HHS’ “analysis showed most Medicare fee-for-service improper payments were for medically unnecessary durable medical equipment and inpatient hospital services.”
- “For Medicare Advantage, HHS reported that the majority of the improper payment estimate resulted from insufficient documentation to support the diagnoses submitted by private health plans for payment”

What will happen during first year of ICD-10 coding?

- The 2012 target error rates are 6.2% for Medicare fee-for-service and 13.2% for Medicare Advantage
- The 2013 target error rates are 5.8% for fee-for-service and 12.9 for Medicare Advantage.
- Targets for FY 2014, beginning 10/1/13? Not yet set-what will be effect of transition?
Predictive Modeling and ICD-10

- “Small Business Jobs Act of 2010 requires CMS to use predictive modeling and other analytic techniques—both to identify and to prevent improper payments under the Medicare fee-for-service program.”
- “According to CMS, as of July 1, 2011, initial predictive modeling has been used on claims prior to payment to identify their level of risk for being improper and to focus investigative efforts.”
- How to build predictive models without historic data?
- Predictive modeling opportunities during period of transition and adaptation
- Epidemiology model
Health care fraud and abuse enforcement

- GAO and CONGRESS to CMS:
  - You must measure and report improper payments
  - You must use contractors to recover improper payments
  - You must measure and report on ROI (return on investment) from your contractors’ recovery efforts

- New CMS reviews:
  - “Predictive modeling technology (is being applied) to Medicare fee-for-service claims nationwide July 1, 2011. All claims across the country are now being screened before they are paid. The ones with the highest risk scores will receive immediate attention and additional review by our analysts through our new rapid response strategy.”

  Dr. Peter Budetti, Director, CMS Center for Program Integrity
Electronic Health Information Exchange creates increased risks for everyone.
EMR Challenges
- Demographic data entry errors (e.g. age, blood type, allergies) are quickly perpetuated throughout the health care continuum as records are shared between providers and facilities
- Fraudulent PHI may be entered into an individual’s medical record if someone else successfully assumes their identity to access care

HIE Challenges
- Master Patient Index (MPI) struggles with accuracy of record linking and providing common identifiers across regions and nationally to ensure that the right information is being attached to the right individual
- While much attention has been paid to patient authorization, very little has been said about the need to verify the identity and confirm the status of the provider requesting medical records; failure to include a mechanism to authenticate and verify a provider’s identity and credentials at the time information is exchanged opens the door for fraud
The High Cost of Ignoring the Risks
2011 Coding and Billing Case

- 2007 – SSM St. Charles audited Dr. Goldstein
  - Found records “scant and illegible”
  - Considered firing, but sent him to coding education classes

- 2009 – SSM St. Charles routine peer review identifies continued coding and record support issues
  - Reported to compliance officer, who reported to DOJ

- SSM St. Charles
  - Repaid $870,000 to federal and state governments
  - No CIA; No monitor
  - Commendation by US Attorney’s Office

- Dr. Goldstein
  - Criminal conviction
  - Repaid $870,000
  - Prison time
Lessons from Dr. Goldstein case

- What routine monitoring do you undertake of coding and billing?
- What actions do you take when physicians’ records do not support coding and billing?
- What records do you make of findings?
- What records do you make of corrective actions?
- What do you do to monitor current actions of non-compliant physicians?
There can be a legal, financial, and relationship cost to the health care organization

- Federal fines and potential prison time on health care organizations who violate privacy and security laws, depending on how egregious the violation is viewed as being
  - $50,000/1 year in prison
  - $100,000/5 years in prison
  - $250,000/10 years in prison

- Civil monetary penalties tiered at
  - $100 - $25,000
  - $1,000 - $100,000
  - $10,000 - $250,000
  - $50,000 - $1,500,000
Fraud and Abuse Provisions of ACA:

- Suspend payments to a provider or supplier where a credible allegation of fraud exists;
- Place a temporary moratorium on enrollment for those categories of providers demonstrating a high risk for fraudulent or abusive claims practices. Payers will be on the lookout for trends that may indicate healthcare fraud, including using advanced predictive modeling software, such as that used to detect credit card fraud. The program can temporarily stop enrollment for a category of high-risk providers; and
- Terminate providers from state Medicaid programs when previously terminated by Medicare or another state Medicaid program; also authorizes CMS to terminate providers and suppliers from Medicare when separately terminated by a state Medicaid program.
Mitigating the Risks
Transition to ICD-10

- Review existing practice management billing software to ensure its ability to successfully transition to ICD-10
- Train clinical and administrative staff on new code sets, technological changes and fraud, waste and abuse regulations and reporting
- Review Third Party agreements to ensure any vendors involved in your billing processes will be compliant with ICD-10 requirements
- Ensure clinical documentation procedures reflect the increased level of detail required by ICD-10
- Contract with an outside entity to audit 6-12 months of claims submitted by your organization to identify any activity that might be considered fraudulent; take immediate corrective action where necessary
- Augment your provider credentialing/hiring processes with a provider screening service that will identify the level of risk associated with any professional individuals you may be considering hiring for your practice/group
EMR/HIE/e-Visits

- Implement identity management tools into all business processes involving patients, other providers and vendors
  - Use photo ID, knowledge-based authentication, bio-metrics, or a combination of these to confirm that the patient presenting themselves for care is who they say they are
  - Incorporate knowledge-based authentication or other forms of identity management into all forms of electronic communications to be sure the person on the other side of the screen is who they claim to be
  - Require and verify that business partners have identity management tools in place for the transactions you engage in with them
Components of an effective Identity Management tool

<table>
<thead>
<tr>
<th>Establish the Identity</th>
<th>Manage the Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resolve</strong></td>
<td><strong>Alert</strong></td>
</tr>
<tr>
<td>“What information do we need?”</td>
<td>“Should I change your privileges?”</td>
</tr>
<tr>
<td>“What information do we have about you?”</td>
<td></td>
</tr>
</tbody>
</table>

- **Resolve**
  - Transaction Origination Data Capture
  - Identity Capture and Validation
  - IP Geolocation / Device Fingerprint
  - Data Enrichment and Hygiene

- **Verify**
  - Core Identity
  - Professional Identity
  - Configurable Identity Verification Checks and Scoring
  - Business Credential Verification
  - “Is this a real identity?”

- **Authenticate**
  - Dynamic Knowledge-Based Authentication
  - Out-of-band Authentication
  - Biometric Authentication
  - “Are you this identity?”

- **Evaluate**
  - Internal Policy/Rule Evaluations
  - Compliance Evaluations
  - Eligibility
  - Credit & Financial Assessments
  - Manual Review/Remediation
  - “Can you have what you requested?” or “Should I do business with you?”

- **Approval**
  - Identify changes in key criteria
  - Age, Name, Address, SSN
  - Derogatory Data
  - Changes in Principals/Owners or Business Credentials

- **Components**
  - What information do we need?
  - What information do we have about you?
  - Is this a real identity?
  - Are you this identity?
  - Should I change your privileges?

- **Eligibility**
  - Credit & Financial Assessments
  - Manual Review/Remediation

- **Identify**
  - Changes in key criteria

- **Alert**
  - Should I change your privileges?

- **Resolve**
  - Transaction Origination Data Capture
  - Identity Capture and Validation
  - IP Geolocation / Device Fingerprint
  - Data Enrichment and Hygiene

- **Verify**
  - Core Identity
  - Professional Identity
  - Configurable Identity Verification Checks and Scoring
  - Business Credential Verification
  - “Is this a real identity?”

- **Authenticate**
  - Dynamic Knowledge-Based Authentication
  - Out-of-band Authentication
  - Biometric Authentication
  - “Are you this identity?”

- **Evaluate**
  - Internal Policy/Rule Evaluations
  - Compliance Evaluations
  - Eligibility
  - Credit & Financial Assessments
  - Manual Review/Remediation
  - “Can you have what you requested?” or “Should I do business with you?”

- **Approval**
  - Identify changes in key criteria
  - Age, Name, Address, SSN
  - Derogatory Data
  - Changes in Principals/Owners or Business Credentials

- **Alert**
  - Should I change your privileges?”
IDENTITY-RELIANT TRANSACTIONS

All subsequent transactions build on initial identity proofing and authentication

Relationship establishment
- Does this identity exist?
- Does the data exist?
- Does it belong together?
- Is this identity yours?
- Is this identity associated with valid, current credentials?
- Which rights & privileges are you entitled to?

Transaction
- Are you the owner of the proven identity?
- Are your credentials still valid?
- Are you qualified to access this particular transactional service?

High-risk/value transaction
- Are you the owner of the proven identity? (↑ invoke higher level of assurance)
- Is this identity linked to any suspicious entities or displaying suspicious behavior patterns?
- Are your credentials still valid?
- Are you qualified to access this particular transactional service?

Transaction
- Are you the owner of the proven identity?
- Are your credentials still valid?
- Are you qualified to access this particular transactional service?
Comprehensive Identity Management: *Identity Proofing and User Authentication*

When sharing data, proper user authentication of providers and members is essential to protect the privacy of individuals and the integrity of the health information exchange (HIE).

- User registration and account setup
- User credentialing
- User authentication login
- Credential reset
- Audited access

- Physician
- Patient
- Health care provider
- Insurance provider
- Public health personnel
- Government personnel
Case Study: Major National Pharmacy Chain

Goals
• Prevent Fraudulent activities
• Protect PHI in the online pharmacy environment

Approach
• Implement identity authentication solution
  ➢ Establish ownership of the presented identity profile
  ➢ Determine whether individual presenting the identity owns the identity

Result:
• 97% of customers agreed to complete the quiz (3% opt-out rate)
• No PHI breach related to portal security

Impact:
• Operational Efficiency/Overhead Cost Savings
  ➢ Customers no longer required to call customer service to verify their identity; reduction in number of calls led to a 33% reduction in call staff
• Increased customer satisfaction
  ➢ Customers able to access prescription history immediately upon logging in; previously this required additional contact with the Client’s customer service staff to verify identity
  ➢ Customers need less information to process their request (e.g. previously they could not fill or renew a prescription without the prescription number – part of the identity verification process)
Provider Screening – it pays to know.
Do you know which providers in your network are practicing with an expired license? Whether or not they’ve been previously convicted of a felony? Or if they’ve been disbarred from participating in other programs or networks because of previous fraudulent activity?

An effective provider screening tool:
• Identifies potentially fraudulent providers and businesses enrolled or attempting to enroll in health-related programs
• Takes a proactive approach to uncovering derogatory attributes linked to providers, reducing a payer’s exposure to fraud before it affects the organization’s bottom line
Risk mitigation begins with knowing your providers

- Screen all currently enrolled fee-for-service providers
- Implement robust provider validation and evaluation upon enrollment
- Assign dynamic risk scores and track provider files between enrollment periods for pertinent activity; alerts generated when changes occur
- Extend enrollment and screening standards to include managed care organizations
## Sample Input/Outputs for Provider Screening

<table>
<thead>
<tr>
<th><strong>Input Data</strong></th>
<th><strong>Output Data</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>NPI</td>
</tr>
<tr>
<td>Last Name</td>
<td>Sanctions, Exclusion Lists, Disciplinary Actions</td>
</tr>
<tr>
<td>SSN</td>
<td>Deceased Information</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>License Information</td>
</tr>
<tr>
<td>Business Name</td>
<td>DEA controlled substance information</td>
</tr>
<tr>
<td>Business Street Address</td>
<td>Criminal Convictions</td>
</tr>
<tr>
<td>City</td>
<td>Sexual Offenses</td>
</tr>
<tr>
<td>State</td>
<td>Corporate Affiliations</td>
</tr>
<tr>
<td>Zip Code</td>
<td>Liens/Judgments/Bankruptcies</td>
</tr>
<tr>
<td>Work Phone</td>
<td></td>
</tr>
<tr>
<td>Tax ID</td>
<td></td>
</tr>
<tr>
<td>License Number</td>
<td></td>
</tr>
</tbody>
</table>
Case Study: Major National Health Insurance Carrier

Goals
• Develop statistics on individuals and businesses who are currently providing services to <customer> and its beneficiaries
• Identify risk of fraud, waste or abuse within <customer> Provider file (Date)

Input Statistics
• 404,532 Providers currently providing services to <customer> programs
  – 351,623 Individuals (87%)
  – 52,906 Businesses (13%)

Approach
• Analyze full Provider list across all social services programs
**Test:** Identify Providers who may be Deceased or are Registered Sex Offenders

**Result:**
- 117 Providers were flagged as Sex Offenders
  - 54 whose victims were minors
- 2,982 <state> providers were flagged as Deceased

**Examples:**
- <SUBJECT>was convicted of Sexual Abuse of Children in January, 2004
- <SUBJECT>reportedly died in city, state in April, 1971
Test: Identify Providers who may have Federal Exclusions or State Sanctions

Result:

- 415 Providers with Sanctions and no reinstatement <date listed>
  - 32 Providers with fraud and abuse related sanctions resulting in a loss of license and no reinstatement date listed
- 141 Providers flagged with GSA Exclusions, preventing them from receiving federal money

Examples:
- <SUBJECT> has a 1999 Sanction for Felony Medicaid Fraud
- <SUBJECT> was convicted of 1st degree murder in <state> in 2003
Questions?
Contact Information:
Bill Fox, JD, MA
Senior Director Health Care
LexisNexis Risk Solutions
Bill.fox@lexisnexis.com
856-325-9627

Jim Sheehan
Chief Integrity Officer/
Executive Deputy Commissioner
NYC Human Resources Administration
sheehanj@hra.nyc.gov
(212) 274-5600

Linked In Group: LexisNexis Health Care Solutions
Twitter: LexisHealthCare