CSHRM
CALIFORNIA SOCIETY for HEALTHCARE RISK MANAGEMENT

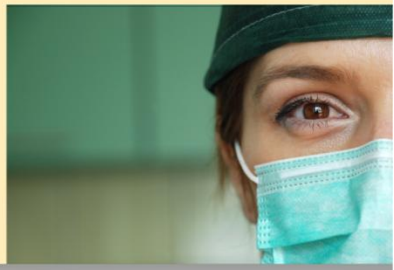
WOODRUFF SAWYER & COMPANY

Regulatory Risk Management Strategies and Coverage update





February 27, 2014



Insurance Services | Risk Management | Employee Benefits

Presented by:
Chad Follmer – WS&Co.
Felicia Sze – Hooper Lundy & Bookman
Lauri Floresca – WS&Co.

CA License 0329598
OR License 0100167994
AN ASSUREX GLOBAL & IBN PARTNER

www.wsandco.com

@WoodruffSawyer

www.linkedin.com/company/woodruff-sawyer-and-co

www.facebook.com/woodruffsawyer

The information contained herein is proprietary & confidential and not to be distributed without the consent of Woodruff-Sawyer & Co.

Table of Contents



- Program Overview – Chad Follmer
- Latest Regulatory Risk Developments for Healthcare Providers – Felicia Sze
- Regulatory Risk Management Strategies and Insurance Options – Chad Follmer & Lauri Floresca
  - Regulatory Liability & Billing E&O
  - Data Privacy & Cyber
    - *Wage & Hour*
    - *Responsible Corporate Officer*
    - *Antitrust*

Presenter

- Chad Follmer, Woodruff-Sawyer & Company, Healthcare Practice Leader
- Lauri Floresca, Woodruff-Sawyer & Company, E&O / Cyber Practice Leader
- Felicia Sze, Hooper Lundy & Bookman, Senior Counsel

Section: Introduction / Program Overview

Why Regulatory Risk?



- Intense pressure on Congress to identify fraud, waste and abuse in deficit reduction efforts
- Federal and state governments outsourcing oversight responsibilities (audits)
- All providers receiving government funds are at risk in the current environment
- Health Care fraud is estimated between $60B to $200B each year.
  - In 2012 DOJ secured $4.9B in settlements and judgments in civil fraud cases, of this $3B were recoveries from healthcare providers.
- The Government's ROI - for every dollar spent fighting fraud and abuse $8-15 is recovered.
  - Enforcement is a highly profitable business!
- Data Privacy - In 2012 healthcare represented 34.5% of all data breaches
  - 63% of healthcare providers said they had a cyber attack in the past year
  - the average cost of that attack was $2.7 million. * *Ponemon Survey*
- Regulatory risk ranked as THE most important concern for over 50% of healthcare executives

Section: Regulatory Risk Update
Felicia Sze, Hooper Lundy & Bookman

California Society of Healthcare Risk Management

California Society of Healthcare Risk Management | February 27, 2014

Presented by:

Felicia Y. Sze | Partner | (415) 875-8503 | fsze@health-law.com

HLB

HOOPER, LUNDY & BOOKMAN, PC

HEALTH CARE LAWYERS

| Los Angeles | San Francisco | San Diego | Washington D.C. |

TOPICS

- OIG Work Plan Highlights
- Two-Midnight Rule
- 60-day Reporting and Refund Rule
- False Claims Act Update

2014 OIG WORK PLAN

- Released January 31, 2014
- Available for download at: https://oig.hhs.gov/reports-and-publications/workplan/index.asp#current

2014 OIG Work Plan Selected Focus Areas

- New inpatient admission criteria
  - Assess impact of new inpatient admission criteria on hospital billing, Medicare payments, and beneficiary payments
  - Analyze how billing varied among hospitals in FY 2014
- Medicare costs associated with defective medical devices
  - Identify the costs resulting from additional utilization of medical services associated with defective medical devices and determine the impact on the Medicare Trust Fund

2014 OIG Work Plan
Selected Focus Areas

- Analysis of salaries included in hospital cost reports
- Provider-based status
  - Impact on Medicare billing
  - Comparison of provider-based and free-standing clinics
    - Determine the difference in payments for similar procedures at similar locations
    - Assess the financial impact for Medicare of hospitals claiming provider-based status

2014 OIG Work Plan Selected Focus Areas

- Outpatient evaluation and management services billed at the new-patient rate
  - Review Medicare outpatient payments made to hospitals for E/M clinic visits billed at the new-patient rate to determine whether they were appropriate
- Nationwide review of cardiac catheterization and heart biopsies
  - Review Medicare payments for right heart catheterizations (RHC) and heart biopsies billed during the same operative session and determine if hospitals complied with Medicare billing requirements

2014 OIG Work Plan Selected Focus Areas

- Payments for patients diagnosed with kwashiorkor
  - Evaluate whether the diagnosis is adequately supported by medical record documentation (protein deficiency confusion)
- Outpatient dental services
- Bone marrow or stem cell transplants
- Direct and Indirect medical education payments
- Oversight of hospital privileging
  - Review how hospitals assess medical staff candidates prior to granting initial privileges, including verification of credentials and review of the National Practitioner Databank

2014 OIG Work Plan Selected Focus Areas

- Meaningful Use Audits
  - 234,065 organizations – 3,781 hospitals and 229,684 physicians and other professionals - have received EHR incentive payments totaling nearly $12.7 billion
  - OIG Work Plan focus on both Medicare and Medicaid incentives
  - Target areas
    - Stage 1 (Data Capture)
      - Core Area 14 – security risk analysis (performed before reporting period ends; need an action plan with measurable goals, deadlines, and proof of progress on action plan)
    - Stage 2 (Integration to Clinical Process)
      - Audits will be coming
      - Core Area 14 – encryption/security of data stored or at rest

2014 OIG Work Plan Selected Focus Areas

- Systems and Information Security
  - OCR oversight of CE's compliance with the HIPAA privacy rule
  - OCR oversight of CE's compliance with HITECH breach notification rule

Two-Midnight Rule

Background

Practitioner decision to admit patient as inpatient or for outpatient observation.

- Inpatient Admission:
  - Used a 24-hour benchmark period
  - Practitioner considers a number of factors, such as medical history, current medical needs, severity of signs and symptoms, and prediction of something adverse occurring to patient. Severity of illness and intensity of service needed!

Background (cont.)

Observation Services:

- Clinically appropriate services including ongoing short term treatment, assessment and reassessment before a decision may be made as to whether the patient requires further treatment as an inpatient or discharge
- Typically, decision to admit as inpatient or discharge can be made in less than 24 hours
- Rare and exceptional cases where reasonable and necessary observation services go longer than 48 hours

Patient admissions are not covered/non-covered solely on the basis of the length of time the patient spends in the hospital.

The "Two-Midnight" Rule

Finalized in the 2014 IPPS Final Rule

- Issued August 2013; effective October 1, 2013
- May also apply to Medicare Part C, depending on contract language

Key provisions:

- Use of a time-based standard to justify an inpatient admit – the "Two-Midnight" presumption
- Practitioner order and certification
- Documentation guidelines
- Inpatient admission guidance

The "Two-Midnight" Rule cont.

Medicare review contractors to apply two presumptions when reviewing hospital claims:

First presumption:

- Inpatient admissions are reasonable and necessary for beneficiaries who require more than one Medicare utilization day, defined as crossing two midnights of medically necessary inpatient hospital services
- *Exception*: Finding that the hospital is delaying necessary care to meet the two-midnight rule

The "Two Midnight" Rule (cont.)

Second Presumption: hospital services spanning less than two midnights considered outpatient, paid as Part B service, unless:

- The medical record contains clear documentation supporting the physician's order and expectation that the beneficiary would require care beyond two midnights
- Examples:
  - Patient improves more rapidly than physician's reasonable, documented expectation
  - Patient signs out against medical advice

The "Two-Midnight" Rule — Exceptions

- Services are designated by CMS as "inpatient only"
- Patient death or transfer occurs before second midnight threshold
- "Rare and Unusual Circumstances" when second night stay is not expected, but is appropriate for inpatient admission. CMS to provide further guidance on this exception

Physician Order

- For Part A payment, need practitioner order indicating admission as an inpatient e.g., “admit to inpatient”
- May still be considered valid order if “inpatient” not specified in record “provided that the intent to admit as an inpatient is clear and consistent with the remainder of the record” (e.g., admit to ICU)
- Orders that specify a typically outpatient or other limited service will not be treated as meeting inpatient admission requirements (e.g., admit to ED; observation, recovery, outpatient surgery)
- If order is ambiguous, CMS recommends that the hospital obtain and document clarification prior to billing

Physician Certification

- No specific procedures or forms required for statement
- The certification will be evaluated in relation to the evidence in the medical record. The certification does not document medical necessity
- The physician must certify prior to discharge (except outliers):
  - That the services were provided in compliance with Medicare admission requirements
  - The reasons for the inpatient medical treatment,
  - The estimated patient stay in the hospital and
  - Plans for post-hospital care, if appropriate.

Documentation Guidelines

- Physician admission and progress notes must support the physician's order for inpatient admission
- Medicare review contractors will evaluate:
  - Physician order
  - Documentation supporting order with expectation of care spanning at least two midnights, such as:
    - Medical history and comorbidities
    - Severity of signs and symptoms
    - Current medical needs
    - Risk of an adverse event
- Documentation supports medically necessary inpatient admission

Inpatient Admission Guidance

- Practitioner should order admission if expectation is that patient's stay will exceed two-midnights benchmark, or if an inpatient-only specified procedure
- Starting point for time-based instruction:
  - If physician makes the decision to admit after the patient arrives at the hospital and begins receiving services (e.g., observation, treatments in the ED, or routine recovery following outpatient surgery)
    - **May consider** the time spent as an outpatient before the formal inpatient order when determining if the expectation of a stay lasting at least two midnights is reasonable and appropriate
    - However, the time the beneficiary spends as an outpatient is not considered inpatient time

Enforcement Moratorium

- CMS issued several enforcement moratoria
- First, instructed RACs not to review 0 or 1 midnight stays which occur between 10/1/13 and 12/31/13, then extended to 3/31/14, now extended to 9/30/14
- For inpatient stays less than two midnights after 10/1/13:
  - MACs directed to conduct a limited sample of 10-25 cases for pre-payment review for a 90-day period. If inpatient is not supported, the hospital will be instructed to bill those services as outpatient Part B
  - CMS did not prohibit post-payment review

Sixty-Day Rule

ACA 60-Day Rule Provisions

- Affordable Care Act Section 6402(a) (42 U.S.C. § 1320a-7k(d))
  - If a person has received an **overpayment**, the person shall:

    (A) **report and return** the overpayment to the Secretary, the State, an intermediary, a carrier, or a contractor, as appropriate, at the correct address; and

    (B) notify the Secretary, State, intermediary, carrier, or contractor to whom the overpayment was returned in writing of the reason for the overpayment

ACA 60-Day Rule Provisions

- An overpayment must be reported and returned by the later of:
  - (A) the date which is 60 days after the date on which the overpayment **was identified**; or
  - (B) the date any corresponding cost report is due, if applicable
- Any overpayment retained after the deadline is **obligation** for purposes of the Federal Civil False Claims Act

FCA Exposure

31 §3729(a)(1)(G)

- "Any person who … **knowingly conceals or knowingly and improperly avoids or decreases** an **obligation** to pay or transmit money or property to the Government..."
- Knowing and "improper" failure to timely report and refund can lead to FCA liability
  - Treble damages
  - $5500 to $11,000 per claim penalty
  - *Qui tam* lawsuit possible
- Knowing: actual knowledge, reckless disregard, or deliberate ignorance

Civil Monetary Penalty Exposure

Civil Monetary Penalty and Exclusion liability added by the ACA

- For knowing of an overpayment and failing to timely return and report such overpayment
- Penalty: $10,000 for each item or service and an assessment of not more than three times the amount claimed
- “Requires[s] no proof of specific intent to defraud”

Proposed Medicare Rules

- **Parts A and B Rule**: On February 16, 2012, CMS published proposed regulations regarding the obligation to report and return Medicare Parts A and B overpayments (77 Fed. Reg. 9179)

- **Parts C and D Rule**: On January 10, 2014, CMS published proposed regulations regarding the obligation to report and return Medicare Parts C and D overpayments. Rule focuses on MA and Part D plans

- Neither rule has been finalized
- No guidance yet re: Medicaid

Overpayment And Reconciliation

- "Overpayment" means any funds that a person receives or retains under title XVIII or XIX to which the person, after applicable reconciliation, is not entitled under such title"
- CMS's view is reconciliation is limited to cost report reconciliation for items typically reconciled in cost reports
  - Two exceptions in proposed rule — occurs upon final reconciliation
    - Provider receives updated SSI ratio data
    - Outlier reconciliation

CMS Examples of "Overpayments" Proposed Rule

- Medicare payments for non-covered services
- Medicare payments in excess of the allowable amount for an identified covered service
- Errors and non-reimbursable expenditures in cost reports
- Duplicate payments
- Receipt of Medicare payment when another payor is primary

Overpayment Examples

- Our experience is that overpayments are usually related to:
  - Improper coding
  - Inadequate documentation to support level or type of service billed
  - Inadequate documentation of medical necessity

"Identify An Overpayment" Proposed Rule

- A person has "identified" an overpayment if he or she has actual knowledge of the existence of the overpayment or acts in reckless disregard or deliberate ignorance of the overpayment
- Indicates if not sure, but have some facts that would lead a reasonable person to look further, should look further

Proposed Medicare (A and B) Rule – Examples of "Identified"

- Provider receives an anonymous compliance hotline complaint about a potential overpayment and fails to make a reasonable inquiry
- Provider reviews billing or payment records and learns that it incorrectly coded certain services, resulting in increased reimbursement
- Provider learns that a patient death occurred prior to the service date on a submitted claim

Proposed Medicare (A and B) Rule – Examples of "Identified"

- Provider learns that services were provided by an unlicensed or excluded individual
- A provider performs an internal audit and discovers that overpayments exist
- A provider is informed by a government agency of an audit that discovered a potential overpayment, and the provider fails to make a reasonable inquiry
- Duty to make reasonable inquiry
- "All deliberate speed"

How Far Back?

- How far to go back for purposes of calculating the amount of an overpayment?
- Can you put a "stake in the ground"
- Effect of administrative finality
  - CMS regs allow claims reopening for four years from payment for "good cause"
  - Effect of extension of the time period from three years to five years over which the "without fault" provisions in 42 U.S.C. §1395gg(b) apply (§638 of the American Taxpayer Relief Act of 2012)
- Ten-year look back period proposed in 2012 (Parts A & B)
- Six-year look back period proposed in 2014 (Parts C & D)

Steps When You Suspect an Overpayment

- Move with deliberate speed to determine if there are overpayments
- Once determined there are overpayments, act reasonably to quantify overpayments
- Identify potential universe of claims
- If overpayments are identified in a sample, 60 days would start for the sample right away
- Less certain when 60 days start for the remainder of the potential universe of claims
- Calendar 60-day deadline when you determine the start date

Steps When You Suspect an Overpayment (cont.)

- Consider engaging counsel to determine whether there is an overpayment (privilege considerations)
- Consider working with a consultant or auditor to identify affected claims
- If necessary, define a sampling methodology (note, the government may carefully review any sampling methodology)
- Suspend billing for potentially affected claims during review and/or take corrective action before billing

To Whom to Report and Refund?

- The MAC where only an innocent or negligent overpayment and not false claims or criminal level of intent
- CMS using the Stark self-disclosure protocol for Stark issues
- DHCS Third-Party Liability and Recovery
- The OIG using the self-disclosure protocol where there is a false claims or criminal level of intent
- The US or CA DOJ?

What to Report?

- Obligation is to report and repay
- Report is a description of the overpayment and identifying the claims or other matters involved
- Suggest report anything needed to make it not misleading, such as how far back you went and why
- Use MAC forms and process, or create own that includes the same information
- Include corrective action plan
- If sampling used, describe methodology

Managed Care

- Proposed 60-day Rule on Parts C and D creates inference that there is not a 60-day obligation under Medicare and perhaps Medicaid managed care
- May be an obligation under the managed care contracts
- May be time limits and reconciliation provisions in the contracts
- Unclear whether there is an obligation under the FCA to refund apart from 60-day rule

FCA UPDATE

Qui Tam (FCA) Update

- Federal and State False Claims Actions continue to be primary enforcement tool and source of revenue of government – Billions collected from defendants
- 2009 FCA amendments make it easier for whistleblowers to maintain actions

Updates

- Failure to timely return identified overpayments
- Services which are related to kickbacks now equal false claims
- Worthless services can give rise to liability

Limitations

- Violations of Conditions of Participation do not equal worthless services
- Malpractice or negligence claims do not equal worthless services
- Substandard care or occasional lapses do not equal worthless services

Evidence

- Worthless services require the relator to show that the services have no value – equivalent to no services at all
- A long term pattern of appalling conditions may be basis for worthless services

Examples

- Liability has been found where there are dangerously low staffing levels, jobs being performed by unqualified staff, non-sterile instruments used, food shortages bordering on starvation, poor sanitary conditions, etc.

Relators

- Relators' rights can still be limited in cases where the allegations have been previously disclosed and relator is not original source of the allegations
- Relators may be limited to the steps they can take to obtain and disclose records and other information

Section: Regulatory Risk and Billing E&O Overview



Basic Elements for Effective Compliance

- Implement written policies, procedures and standards of conduct
- Designate a compliance officer and compliance committee
- Conducting effective training and education
- Develop effective lines of communication
- Enforce standards through well-publicized disciplinary guidelines
- Conduct internal monitoring and auditing
- Respond promptly to detected offenses and develop a corrective action plan

Potential Regulatory Risk Coverages found in other policies:

- Directors & Officers – regulatory sublimit
- Professional Liability Policies – can contain specific sub-limits for coverage
- Information Privacy and Security Policies / Cyber – Will discuss at length
- Captive Policies – Opportunity for broader coverage

Broad Regulatory Risk / Billing E&O Coverage



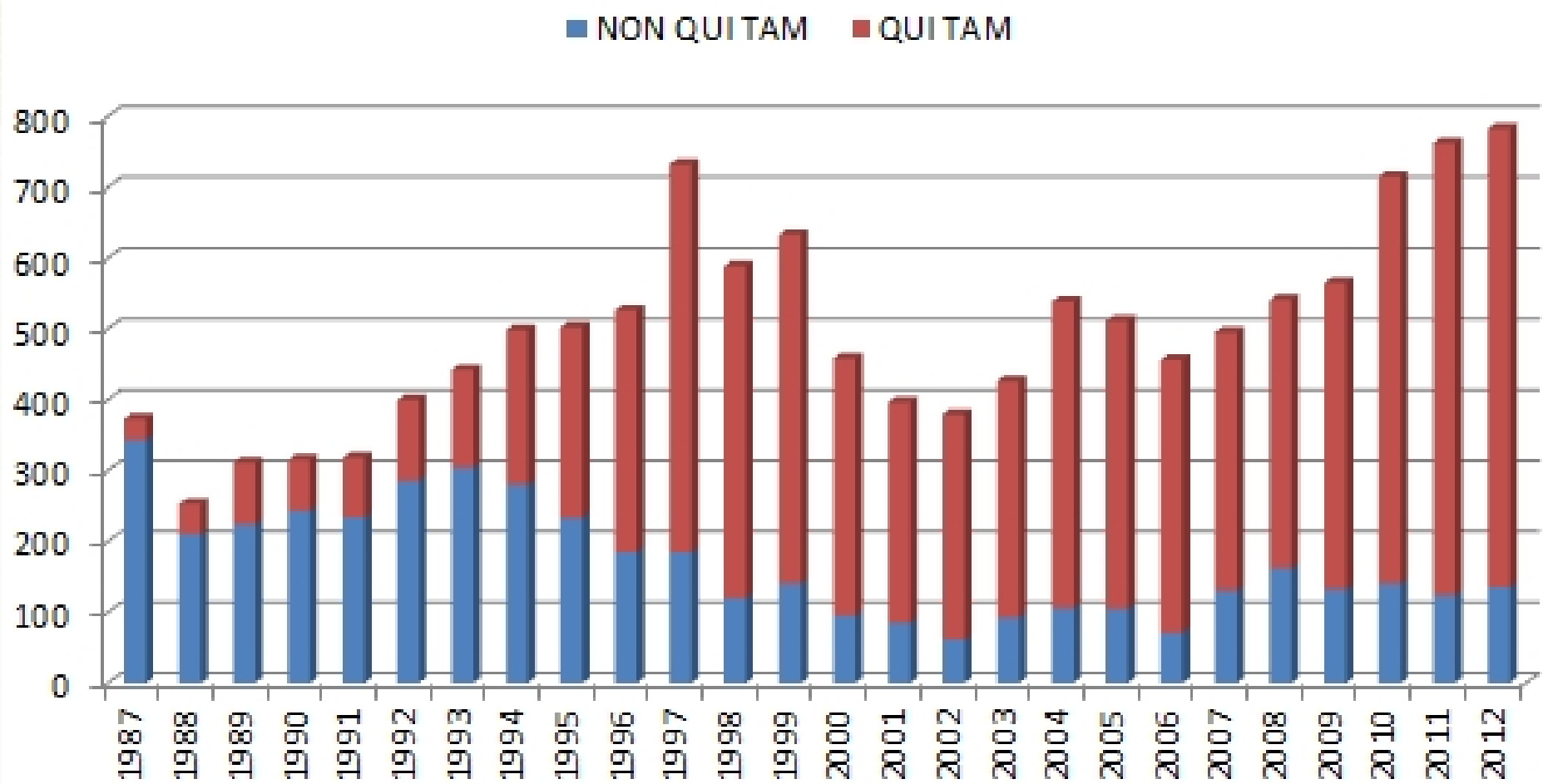
Claim Triggers

- ***False claims audits and investigations (Qui Tam/Whistleblower)***
- Recovery Audit Contractor audits (RAC)
- Zone Program Integrity Contractors audits (ZPIC)
- Search warrants/subpoenas
- Voluntary disclosure to a government entity

Who's Watching?

- Whistleblowers
- DOJ/US Attorney Offices
- HHS - Office of Inspector General (OIG)
- Medicare and Medicaid Contractors – RAC, ZPIC, MAC, MIC
- Health Care Fraud Prevention and Enforcement Action Team (HEAT)
- Commercial Payors
- Competition
- Press

New False Claim Matters



Examples of violations



- Quality of care
- Billing for services not rendered
- Medically unnecessary level of service
- Stark Law & Anti-kickback statute violation
- Medicare payments in excess of the allowable amount for an identified covered service.
- Errors and non-reimbursable expenditures in cost reports (reverse False Claims)
- Duplicate payments
- Receipt of Medicare payment when another payor had the primary responsibility for payments.

Claim Examples – Show me the money!



Organization	Damages	Allegations
Florida-based sleep diagnostic company	$15.3M settlement	False claims misrepresenting technician credentials
Urgent Care Chain	$10M settlement	Unnecessary allergy, virus and respiratory testing -upcoding
Florida health system	$26M settlement	Miscoding outpatient service claims as more expensive inpatient services. – whistleblower – State & Federal FCA
Largest healthcare system in Utah	$25.5M settlement	Violated FCA by engaging improper financial relationship with referring physicians
South Carolina hospital	$39M verdict	Improper patient referrals
Rhode Island Health System	$2.6M in disgorgement and $2.7M in damages	Doctors billed Medicare and Medicaid for unnecessary overnight hospital stays
Medical Center in Iowa	$406K settlement	The OIG alleged that they employed an individual that it knew or should have known was excluded
Texas dialysis provider	$7.3M settlement	Billing for phantom services in violation of FCA by charging for more of a drug than actually administered. Whistleblower received $1.3M
Medical Center in KY	Ongoing investigation	Alleged that the medical center completed 28% more heart stents than any other hospital in the area



Coverage Overview

- Responds to actions brought by or on behalf of governmental entities for Medicare / Medicaid billing errors and omissions and actions brought by commercial payers.
- Provides for defense reimbursement
- Provides for external forensic audit expenses
- Provides for civil fines and penalties (where insurable by law)
- Primary Limits up to $10M ($1M - $3M more common)
- Excess Available
- Coinsurance 10% - 40%
- Optional retroactive buy back coverage for up to 3 years

Section: Cyber Liability Overview

Who Has Cyber Liability?



The (new) old adage is that there are two types of companies: Those that have had a security breach, and those that *don't know* they've had a breach. The 2013 Ponemon study reported that more than 55% of the 1200 small businesses in their study reported having a data breach.

- **All companies now face exposure to cyber liability:**
  - Costs and liability arising from a breach of customer data, including PHI, credit cards, address, SSN, and even login credentials such as email address and password
  - Employee PII and PHI
  - Loss of profits due to a network outage or security failure
- **As the definition of PII expands, a broader range of companies are now targets:**
  - Retailers (brick and mortar AND online)
  - Healthcare providers
  - Financial industry, including new payment technologies
  - Social media and other content aggregators
  - Gaming and entertainment companies
  - Cloud/SaaS providers

Breaches in the News – All Industries



— Target (December 2013)
Malware discovered on Target's point-of-sale systems allowed hackers access to 70M+ credit and debit cards during the busiest shopping period of the year. Target later reported that the breach involved both CVV data and "strongly encrypted" PIN numbers as well as customer names, addresses, and emails. Nearly 50 class-action lawsuits were filed in the weeks after the security breach became public.

— Horizon BCBS (NJ) (November 2013)
Two unencrypted laptops stolen from BCBS's NJ offices, potentially exposing 840K members' info. Credit monitoring offered to those members whose SSN may be at risk. Class action filed in Feb. 2014

— Adobe (Oct 2013)
Hackers broke into Adobe's network and stole source code for an undetermined number of software titles, including its Cold Fusion Web application platform, and possibly its Acrobat family of products. The company said hackers also accessed nearly 3M customer credit card records, and stole login data for an undetermined number of Adobe user accounts.

— South Carolina Department of Revenue (Oct 2012)
On Oct. 26, officials disclosed a massive data breach at the Department of Revenue, which exposed at least 3.6M SSNs and information for 650K businesses, with losses totaling $15M.

— Global Payments (March 2012)
Hackers breached the security of one of the largest payment processors servicing Visa and MasterCard transactions for merchants, resulting in $94M in post breach costs.

— Zappos Breach (January 2012)
Zappos notified their 24M customers that their security was breached and may have potentially exposed their name, email address, billing/ shipping addresses and the cryptographically scrambled version of their Zappos account password. Full credit card numbers were not compromised. Numerous class action suits have been filed against them.

— Accretive Health (2011)
The healthcare billing services vendor faced an FTC inquiry in 2013 over a lost laptop incident in 2011. The laptop contained data on 23,500 patients. In its settlement with the FTC, Accretive agreed to pay $2.5M in restitution for patients and agreed to stop doing business in Minnesota for 2 years.

— CitiGroup (May 2011)
Hackers obtained personal data on approximately 1% of Citibank's 21M users. 3,400+ customers were affected with losses totaling $2.7M.

— Sony (April 2011)
Hackers accessed personal data for more than 100M users of Sony's online games. 55+ suits filed in the US along with investigations by state & federal regulators. In 2013, Sony was fined £250K (US $395K) by the UK Information Commissioner's Office for allowing UK gamer details to be exposed online.

Breaches in the News – Healthcare Specific



- February 2014 - St. Joseph Health System reports that as many as **405,000 records** may have been compromised (Second largest ever)
- June 2013 – *Bon Secours – 5,000 patients due to* ***breach of electronic records***
- June 2013 – *University of Florida Pediatric Clinic – 5,682 patients and parents due to* ***insider leaking information to criminals***
- February 2013 – *Sonoma Valley Hospital – 1,350 patients due* ***to internet exposure of unsecured section of website. (sometimes called "Google Search"-breaches)***
- January , 2013 – *Lucile Packard Children's Hospital – 57,000 patients –* ***stolen laptop from physician's car***
- January 2013 – *New York Hospital – 9,887 patients due to* ***Hurricane Sandy and structural damage to facility and unauthorized individuals on premise***

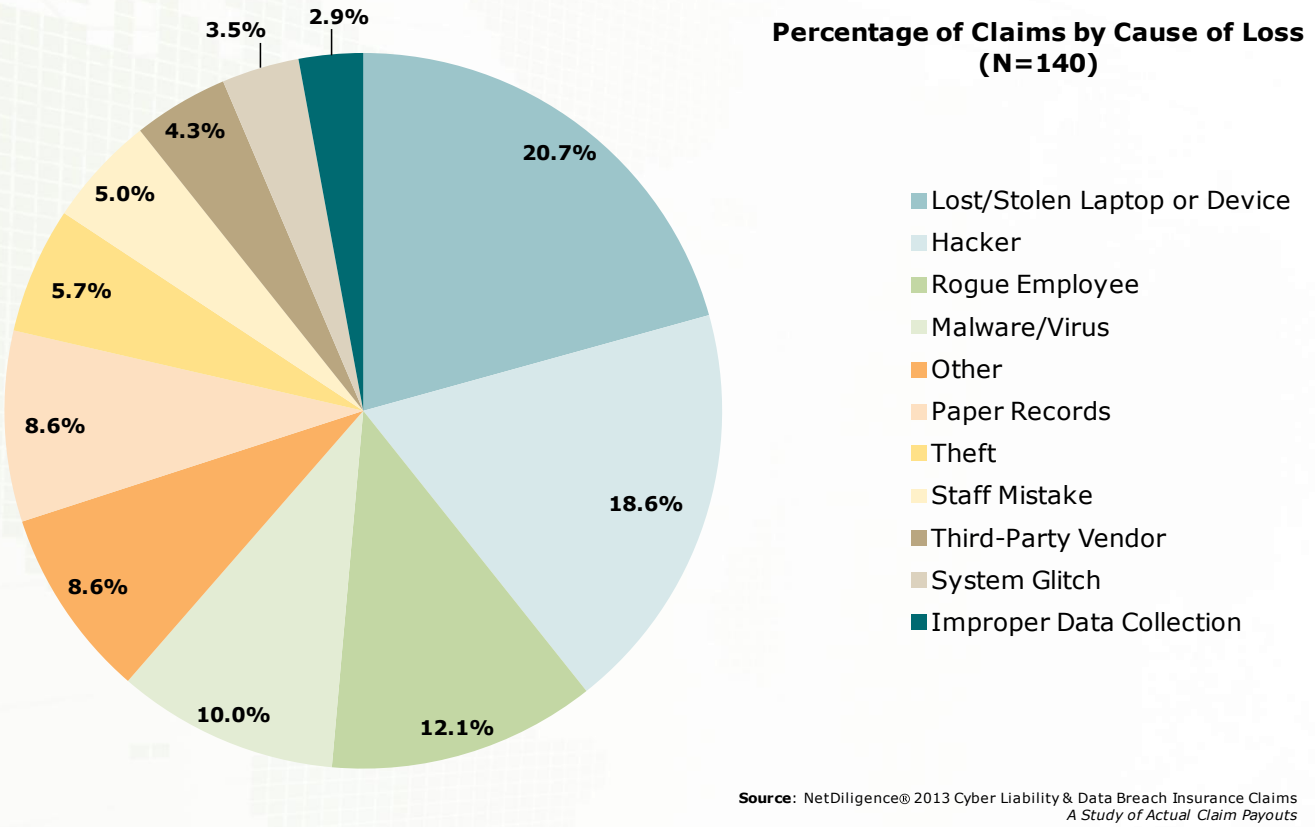
Breaches in the News – Healthcare Litigation & Fines



- February 2014 – Triple S Management Corp., San Juan Puerto Rico - **$6.8M Fine. (Federal HIPAA capped at $1.5M, but also State & Regional)**
- January, 2013 – ***FTC Settles with CBR Systems (Blood Bank) for Failure to Protect Data – 20 year consent decree***
- January, 2013 – *Goldthwait Associates, Pathology Group pay $140,000 to settle claims that* ***patients' PHI was disposed of improperly***
- January, 2013 – ***Hospice of North Idaho fined $50,000 by OCR for a 441 person breach***
- May, 2013 – *Idaho State University – $400,000 settlement involving 17,500 patients for* ***violating HIPAA Security Rule***
- June, 2013 – *Shasta Regional Medical Center fined $275,000 for* ***CEO and CMO discussing with media on medical services of a patient***
- August, 2013 – *Woman awarded $1.44M against Walgreens due to* ***pharmacist sharing prescription history***

Cause of Loss

"Lost/stolen laptops and devices accounted for 20.7% of events, but those incidents resulted in less than 1% of records exposed."



Source: NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims
A Study of Actual Claim Payouts

"Hackers accounted for fewer than 18.6% of reported incidents, but were responsible for 97.6% of the records exposed."

Why you need Cyber Liability Insurance



Property Insurance
Excludes "data" as property.

General Liability (including Product Liability)
Excludes damage to intangible property, such as data, and either excludes or limits coverage for many exposures common to companies conducting business in an E-World.

Errors and Omissions (E&O)
Limited to "traditional" professional exposures and financial loss due to failure of a product/service to perform as designed.

First-party v. Third-party Coverage



Network Security

First-Party*

- Loss of Profits & Extra Expenses
- Data Replacement
- Cyber Extortion
- Crisis Management
  - Public Relations
  - Forensic
  - Legal

Third-Party

- Customer Suits
- Other Third-Party Suits

*May be subject to sub-limits

Privacy

First-Party*

- Notification Costs
- Credit Monitoring
- Crisis Management
  - Public Relations
  - Forensic
  - Legal
  - Call Center

Third-Party

- Consumer Suits
- Regulatory*
  - Defense
  - Fines & Penalties
- Charges Levied by Credit Card Issuers
- PCI-DSS Fines*

*May be subject to sub-limits

Cyber is a Board-Level Concern



- **In October 2011, the SEC published guidance for companies that suggested issuers should consider**
  - the "probability of cyber incidents occurring"
  - "the quantitative and qualitative magnitude of those risks"
  - the SEC also noted that appropriate disclosure may include a "description of relevant insurance coverage."

Significant Data Breaches Can Lead to D&O Issues

Company	Cyber Event	D&O Matter	Status
ChoicePoint	February 2005: Breach at data warehouser exposed PII of over 500,000 consumers	Class Action filed March 04, 2005	Settled for $10M in July 2008
TJX Companies	2006-2007: Hackers obtained card data and other PII of more than 45 million customers from all TJX stores in North America, cost a reported $171M	Separate Books & Records and Derivative lawsuits (breach of fiduciary duty) filed March 2007	Settled July 2010 for therapeutics and a $595K plaintiffs fee award
Heartland Payment Systems	January 2009: Breach of 130M cards at payment processor cost a reported $140M	Class Action filed March 6, 2009	Dismissed December 2009
Target	December 2013: Massive breach of Target's POS system involving more than 70 million credit and debit cards; total costs expected to exceed $1 billion	Derivative lawsuit (breach of fiduciary duty) filed January 29, 2014	Pending

Sample Large-Scale Breaches Cost Estimates

	Target	Horizon BCBS (NJ)	Zappos
Total Cost	**$592,463,000**	**$9,323,500**	**$39,527,000**
Cost per record	**$14.81**	**$11.10**	**$1.65**
Breach Parameters			
Number of Records	40,000,000	840,000	24,000,000
Centralized Data?	Yes	Yes	Yes
Actual Fraud Expected?	Yes	No	No
Offer Credit Monitoring/ID Theft?	Yes	Yes	No
Type of Records	Credit Card	PHI	PII
Class Action Lawsuits Filed	Yes	Yes	Yes
Breach Investigation			
Forensic	$5,614,000	$188,000	$4,820,000
Data breach legal guidance	$10,000	$10,000	$10,000
sub-total	$5,624,000	$198,000	$4,830,000
Breach Response Cost			
Notification letter	$40,000,000	$840,000	$0
Credit/Identity Monitoring	$98,000,000	$2,940,000	$0
PR/Call center	$3,014,000	$83,000	$20,000
sub-total	$141,014,000	$3,863,000	$20,000
Legal Liablity /Regulatory			
Defense Damages	$140,000,000	$262,500	$33,652,000
Regulatory Fines	$1,025,000	$5,000,000 †	$1,025,000
PCI Assessment/Card Re-issuance	$304,800,000	$0	$0
sub-total	$445,825,000	$5,262,500	$34,677,000

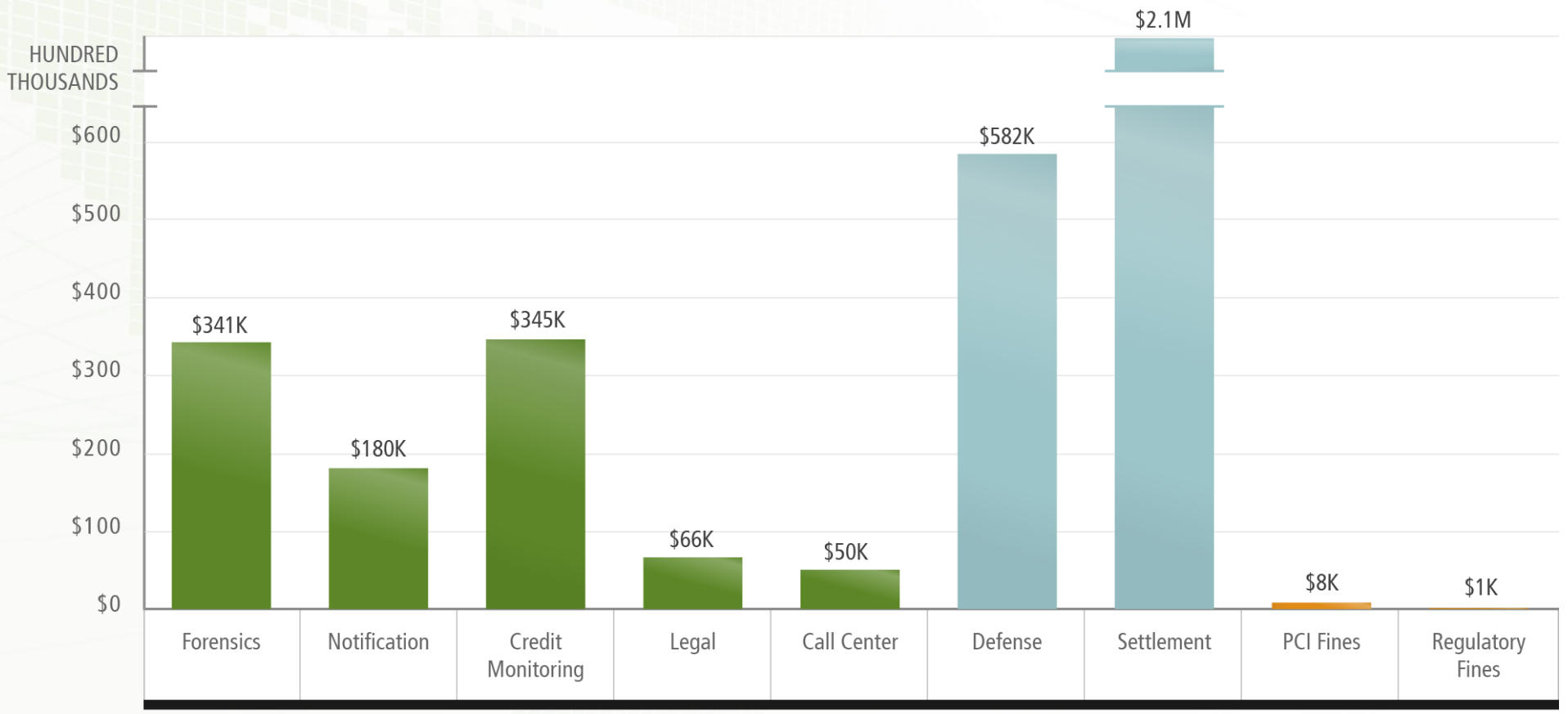
*PCI costs above may include "chargebacks" and/or card brand settlements

**Estimates based on Travelers/NetDiligence Data Breach Cost Calculator with broker modifications to reflect specific Breach Event profile.

† Capped at maximum known HHS/OCR fine/penalty recorded for HIPPA ($4.3M Cignet 2011), although projected loss is higher in this model.

Lower Average Costs of Breach

Average Cost Per Event by Cost Type (Average Total Cost: $3.7M)



NOTE: DATA IS BASED ON 135 BREACH EVENTS.
SOURCE: NETDILIGENCE®, "CYBER LIABILITY & DATA BREACH INSURANCE CLAIMS," PRELIMINARY DRAFT JUNE 2012

Cyber Limit Decision Factors



Selecting Cyber/E&O Limits requires a multi-step assessment:

- **Contract Requirements:** The traditional driver for determining E&O limits
  - *Key Considerations: Larger customers and larger contracts will often result in higher E&O limit demands; ensure sub-limits are reasonable*

- **Network Security Assessment:** Estimate potential expenses and lost profits associated with a security incident that brings your network or website down
  - *Key Considerations: Profitability, continuing expenses, waiting periods, contingent exposures (security incident or outage involving outside vendors)*

- **Data Breach Loss Exposure:** Utilize breach calculators to estimate potential first- and third-party costs
  - *Key Considerations: Number and type of individual customer records at risk, location of data, use of outside vendors (payment processors, cloud providers)*

What about peer data?

No two risks are the same. The variety of exposures and complexity of factors that go into choosing E&O limits, makes peer data an overly simplistic metric. Woodruff Sawyer provides peer data to add a broad perspective on trends.

Section: Other Regulator Liability Coverages

WOODRUFF SAWYER & COMPANY

Wage & Hour Liability



- **Wage & Hour** (the alleged employer misclassification of individuals as exempt employees or independent contractors) is a big target because of the reduced payroll taxes from independent contractors versus employees.

  Exacerbating Factors:

  - ACA – Must provide Healthcare for employees or pay a fine
  - Increases in Minimum Wage – Increased incentive to misclassify
  - American with Disabilities Amendments Act – Need proper documentation for essential job function

- **Responsible Corporate Officer** - Federal regulators pursuing *corporate executives* for violations RCO doctrine.
  - Corporate officers may be held criminally liable under the FDCA, Medicare/Medicaid, or other programs regardless of whether the corporate officer had actual participation in or even knowledge of the wrongdoing.
  - Neither intent nor negligence is required for a criminal conviction.
  - Penalties include fines, imprisonment, and debarment/exclusion from working with federal or state health care programs, including Medicare and Medicaid.

Section: Q&A

Woodruff-Sawyer & Co.

Corporate Office
50 California Street
Floor 12
San Francisco, CA 94111

Southern California
2 Park Plaza
Suite 500
Irvine, CA 92614

North Bay, CA
88 Rowland Way
Suite 180
Novato, CA 94945

Sacramento, CA
2295 Gateway Oaks Drive
Suite 230
Sacramento, CA 95833

South Bay, CA
2105 S. Bascom Avenue
Suite 149
Campbell, CA 95008

Pleasanton, CA
6700 Koll Center Parkway
Suite 240
Pleasanton, CA 94566

Portland, OR
1001 SW 5th Avenue
Suite 1000
Portland, OR 97204

CA License 0329598
OR License 0100167994

AN ASSUREX GLOBAL & IBN PARTNER

www.wsandco.com