LTC Facilities
Big or Small,
Exposures for All
LTC FACILITIES: BIG OR SMALL, EXPOSURES FOR ALL

MODERATOR:
Melissa J. Perez, Esq., BSN, Of Counsel, Troutman Sanders LLP

PANELISTS:
Chuck Colburn, Vice President, CNA
Kasie Leigh Cousino, Director of Claims, Chelsea Rhone, LLC
Kim Martin, JD, Senior Vice President Risk Management & Chief Compliance Officer, Kindred Healthcare
Matthew Prewitt, Area Vice President, RPS Healthcare
A Conference Call in Real Life: Tripp and Tyler
Long Term Care Trends – National Level

- Claim Loss Rates
- Frequency
- Severity
Problematic Jurisdictions
Problematic Jurisdictions

• Typical Offenders
  – Kentucky, West Virginia, Georgia, Tennessee, and Florida

• Tort Reform
  – Is it unraveling?
    • Florida’s cap on non-economic damages in wrongful death held unconstitutional (March 13, 2014)
    • California’s $250,000 cap on non-economic damages under MICRA is at risk

• Recent seven-figure verdicts
• Market Response
Consolidation in Industry

Compliance Costs – Affordable Care Act (“ACA”)

• Fewer Independent Operators

• Now Operators tend to own 5-7 facilities

• Litigation Implications

Hospitals/LTC Facilities

• Acquisitions?

• Looping in of LTC facilities by hospitals because of higher reimbursements

• Facilities with Electronic Health Records more likely to get referrals
False Claims Act
Federal False Claims Act

Long term care providers may face civil FCA claims and criminal prosecution for billing for the provision of substandard care.

**Elements:**

1. Defendant made a claim, or made a statement in order to get the government to pay money on a claim;
2. The claim or statement was false or fraudulent; and
3. Defendant knew that the claim or statement was false or fraudulent.

FCA, 31 U.S.C. § 3729 *et seq*. The Act defines “knowingly” as either: (1) possessing actual knowledge; (2) acting in deliberate ignorance of falsity; or (3) acting in reckless disregard of falsity. 31 U.S.C. § 3729(b).
State False Claims Acts

- Many states have enacted False Claims Acts with *qui tam* provisions.
- States with qualifying FCAs, approved by the Office of Inspector General ("OIG"), receive a 10% increase of any fraudulent payments recovered under that state’s statutes. 42 U.S.C. § 1396h(a).
- **States Approved By the OIG**: California, Colorado, Connecticut, Delaware, Hawaii, Illinois, Iowa, Massachusetts, Minnesota, Montana, Rhode Island, Tennessee, Texas, and Washington
Courts Have Recognized Two Theories Supporting FCA Claims As They Relate To Billing Substandard Care

(1) False Certification
   (a) Express False Certification
   (b) Implied False Certification

(2) Providing Worthless Services
Potential For Liability

• The Justice Department ("DOJ") secured $4.9 billion in settlements and judgments in civil cases for fiscal year 2012, where recoveries for health care fraud exceeded $3 billion.
  See http://www.justice.gov/opa/pr/2012/December/12-ag-1439.html

• The DOJ secured $3.8 billion in fiscal year 2013, with recoveries for health care fraud reaching $2.6 billion.

• In February 2013, the OIG issued a report titled “Skilled Nursing Facilities Often Fail to Meet Care Planning and Discharge Requirements,” highlighting deficient care.
  – Inadequate level of care overpayments in 2009 amounted to approximately $4.5 billion in Medicare payments.
    See https://oig.hhs.gov/oei/reports/oei-02-09-00201.pdf
Potential For Liability

Substantial Incentive to Settle

• Each violation is subject to a civil penalty of “not less than $5,000 and not more than $10,000… plus 3 times the amount of damages which the Government sustains because of that person.” 31 U.S.C. § 3729(a)(1)(G)
  – On April 22, 2013, Ensign Group Inc., the parent of an operator of nursing facilities, announced a tentative agreement to pay the DOJ $48 million to settle FCA allegations of overbilling for care provided in California. Arose out of two whistleblower qui tam lawsuits filed in California.

Awards to Qui Tam Plaintiffs: Incentives for Whistleblowers to Bring Suit

• If the Government intervenes: “at least 15 percent but not more than 25 percent of the proceeds of the action or settlement.” 31 U.S.C. § 3730(d)(1)
• If the Government does not intervene: “not less than 25 percent and not more than 30 percent of the proceeds.” 31 U.S.C. § 3730(d)(2)
Coverage Implications For FCA Claims

Professional Liability and CGL Policies
• FCA claims are **likely not covered** under either CGL policies or Professional Liability policies.

Employment Practices Liability Policies
• EPL policies provide coverage for wrongful acts, which may include claims of wrongful dismissal, discharge or termination and claims involving allegations of retaliation.
• EPL policies typically define the scope of retaliatory acts to include any act alleged to be in response to the filing of any claim under the FCA.

*Note: CGL policies usually contain broad “employment-related practices” exclusions.*
Insurance Products Available

• **Specialized Endorsements Available For Defense Costs**

• **Healthcare Regulatory Liability Policies**
  – **Specifically Provide Coverage For Regulatory Violations, Including:**
    • False Claims Act Allegations (Government or *Qui Tam* Initiated)
      – Also Triggered By False Claims Audits and Investigations
    • Medicare and Medicaid Billing Investigations
  – **Provides Coverage For:**
    • Defense Reimbursement
    • External Forensic Audit Expenses
    • Civil Fines and Penalties (In Certain Contexts)
  – **Claims Made And Reported Policy**
Cyber Liability & HIPAA in Long Term Care Industry
Data Breach HIPAA/HITECH Compliance

**HIPAA and 2009 HITECH Act**

**Covered entities** and their **business associates** are required to comply with notice requirements in the event of a breach of unsecured Protected Health Information ("PHI"). See 45 CFR §§ 164.400-414.

- **Breach** - impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information
- **Unsecured PHI** - not secured through the use of technology or methodologies to render the data unusable, unreadable, or indecipherable to unauthorized persons

*Note: Some states (e.g., California, Missouri, North Dakota and Texas) have also enacted state specific data breach notification statutes.*
Privacy Risks in the Healthcare Sector

• Types of information stored:
  – Protected Health Information (PHI)
  – Personally Identifiable, Non-Public Information (PII)
  – Financial information
  – Other types of data

• Lack of institutional controls
  – Personal mobile devices
  – Failure or ineffective use of security software

• Demand for portability of EHRs
Black Market Value of Medical Records

Medical Records sell for $50 compared to a social security number ($3) and a credit card number ($1.50). Source: Digital Health Conference Panel, NYC 12/1/2011.

- **Why?**
  - PHI = data rich
  - Unable to cancel

- **Uses**
  - Fraudulent insurance claims
  - Medical treatments
  - Prescription drugs
  - Resale to black market
Nursing Home Vulnerabilities

• Human error or failure to follow online procedures
• Lost or stolen laptops, equipment or mobile devices
• Stolen or hacked passwords
• External hackers (including 3rd party equipment)
• Disgruntled employees
• Employee conspiracy involving identity theft
• Viruses, worms
Data Breach in Healthcare Sector
By the Numbers

- 7,095,145 patient health records breached in 2013
- 137% increase in # of patient records breached in 2012 – 2013
- 83% of records breached in 2013 resulted from theft
- 22% of breach incidents in 2013 resulted from unauthorized access
- 35% of incidents were linked to an unencrypted laptop or other portable electronic device

Source: Redspin Breach Report – Protected Health Information – February 2014
Real, Recent Breaches

• St. Anthony’s nursing home suffered a 2,600-patient data breach on July 29, 2013 when a laptop computer and flash drive with PHI were stolen from a doctor’s car.  

• Caledonia Home Health and Hospice reported a data breach that involved a work Netbook containing PHI, which was stolen from an employee’s home on July 20, 2013.  

• Laptop connected to EEG machine detached and stolen from St. Vincent Hospital. PHI of more than 1000 patients breached…”  
2/20/14 www.indianapublicmedia.org

• “Hackers swipe health data of 405,000; access servers from a Texas healthcare system, representing one of the largest healthcare breaches on record, per HHS.”  
2/5/14 http://www.healthcareitnews.com

• “6,777 patient names, addresses, medical diagnosis information and some social security numbers on a desktop computer thrown away by mistake.”  
1/13/14 www.scmagazine.com
Risk Prevention

System Controls, Policies & Procedures
- Network environment
- Wireless capabilities / access
- Mobile devices, media, laptops / encryption
- User access
- Physical security
- Penetration testing
Breach Notification Requirements

Notice Requirements (Can Be Costly)

- Data breaches **affecting more than 500 individuals** must be reported in no case later than 60 days following the discovery of the breach to the Department of Health and Human Services, major media outlets, and those affected by the breach.
  - The DHHS Secretary must also post a list of covered entities that have reported breaches affecting more than 500 individuals.
- Data breaches **affecting fewer than 500 individuals** must be reported to the Department of Health and Human Services on an annual basis and to those affected by the breach without unreasonable delay, and in no case later than 60 days following the discovery of the breach.
- Business associates responsible for the breach must notify the appropriate covered entity, which must in turn, follow the notice requirements.
Specific Exclusions in Traditional Policies for Privacy Breach

- **General Liability**
  - Exclusions for copyright, trademark, etc.
  - Exclusions for social media
  - Limitation on privacy injury

- **Property** – Exclusion for Electronic Data & Cost to Re-create

- **Business Interruption** coverage will not respond to outages by computer viruses or hackers

- **Medical Professional** Liability
  - Must be qualifying “Medical Incident”
  - Often carry exclusion for privacy breach

- **Commercial Crime** coverage has limitations
Solutions Available in Insurance Marketplace

• Many Professional & General Liability Policies include Cyber sub-limit
  – Limit is not sufficient for the exposure
  – Limited coverage terms & conditions

• Stand-alone Cyber Policies
  – Regulatory coverage available as well
Typical Barriers to Purchasing

• **Cost**
  – Many operators are not able to afford
  – Reimbursements from Medicare / Medicaid are down

• **Misunderstanding Risk or Coverage**

• **Overconfidence in IT security**
Impact of Social Media

- Patients/Families/Employees take Frustrations Out by Posting on Internet
  - Larger companies can scrub internet
  - Smaller companies or independent operators

- Nanny Cameras
- Employee Smart Phones
- Can lead to HIPAA/HITECH Liability
- Trends/Emerging Exposures
Managing Risk Through Effective Communication - Apology & Disclosure
The Case for Apology

• First and foremost, without any equivocation, you apologize because it is the right thing to do
• Mistakes happen, but it is how we respond to those mistakes that will help define the outcome
• Known Benefits of a Disclosure Program
  – Improves employee and patient satisfaction
  – Healing on all sides after an error
    – Disclosure is not just about the patient, it’s about the employee, too.
  – Promotes trust through transparency
  – Facilitates appropriate closure of issue
  – Improves safety
  – Improves care
  – Improves communication
What Patients Consider Important

• Timely disclosure of the error
• Truth and transparency
• Clear explanation of what happened and why
• Explanation of how the consequences of the adverse events will be addressed (medical treatment, etc.)
• Assurance that steps have been/will be taken to prevent the error from happening again
• Emotional support including an apology
Why Is It So Hard to Do Something Your Mother Has Taught You to Do Since You Were a Toddler?

• Traditional approach is conservative; we are usually reluctant to apologize or admit error
• Therefore, it is a skill set that must be learned
• Fear of the patient or family response
• Lack of support & agreement among all caregivers
Structure of a Successful Disclosure Program

• **Time**
  – The sooner the better. Delay breeds mistrust

• **Initial Disclosure**
  – Keep Promises
  – Disclose only what you know to be true. You can’t un-ring the bell.

• **Investigation**
  – Specify times that you will follow up
  – Investigations don’t have to be complete for periodic updates

• **Disclosure/Apology**

• **Resolution**
  – Provide the opportunity for closure
Total Interventions (n=3,989)

- Family Interventions Converted to Claim (n=498) - 12%
- Family Interventions Not Converted to Claim (n=3,491) - 88%
Impact of Apology and Disclosure on Paid Claims (Kindred)

Average Closed With Payment Claim By Risk Management Code – 1FAM vs All Other Codes (In $000’s)

Continuing Operations – Nursing Centers

**RM Category and Code**
1FAM - Family Intervention
2NO - Aware of Issue - No RM Involvement
3FOL - Aware of Issue - Followed Up with Facility
4ATT - Attempted Family Contact - No Family Intervention
5UN - Unaware of Issue
6X - No RMS Coverage
State Directors of Risk Management

- Variety of backgrounds
  - RN’s, JD’s, RN JD’s, Physical Therapy, Operations, Dietary, Quality Professionals, Regulatory
- Most have had no previous Risk Management experience
- Have the ability to connect the dots
- High “EQ”
- Ability to relate to individuals with diverse backgrounds
- Work within a dynamic organization
  - Operations, Human Resources, Legal, Clinical Services, Administration
Kindred Nursing Center PL Data

Average Closed With Payment (CWP) Claim ($000)

- ADR & RM (n=96): $103
- RM Only (n=76): $83
- ADR Only (n=106): $105
- Neither (n=154): $116
LTC Staffing Requirements: Private Right of Actions
Private Right Of Action For Residents

• Many states have established a private right of action for residents of nursing facilities for violating statutes governing nursing facilities or rights of residents guaranteed under such statues. See 1-10 Long-Term Care Advocacy § 10.16 (Matthew Bender & Co. 2013).

• Courts in these states may recognize the failure to adhere to staffing ratios as a cognizable cause of action.
  – California recognizes a private right of action through Health & Safety Code Section 1430(b).
California’s NHPPD Requirement

• **NHPPD (Nursing Hours Per Patient Day)** -number of hours of nursing care provided by staffed nurses at a facility, compared to the number of patients at that facility during a 24-hour period.

• **Relevant Sections of the California Health & Safety Code Forming The Basis The Private Right of Action**
  – Section 1430(b) provides a private right of action for the violation of rights established by federal or state law or regulation.
  – Section 1599.1(a) requires facilities to “employ an adequate number of qualified personnel to carry out all the functions of the facility.”
  – Section 1276.5 provides that the minimum number of actual nursing hours per patient day must be at least **3.2 hours**.
California’s NHPPD Requirement

Significant Litigation
• In 2010, a jury issued a $677 million verdict in Lavender v. Skilled Healthcare Group, Inc. (Cal. Super Ct., Humboldt County); Plaintiffs alleged the failure to meet minimum staffing requirements, including the failure to meet the 3.2 NHPPD standard; ultimately settled for a fraction of the jury verdict.
• Subsequent litigation has narrowed recoverable damages; only a matter of time before Plaintiffs’ bar pursue alternative grounds

Standing
• Limited to current or former residents of skilled nursing facilities; successors-in-interest may also bring suit.
• Resident must have resided in the facility when the facility was staffed below the 3.2 standard

Remedies
• Statutory Damages
• Injunction
• Statutory Attorneys’ Fees

Additional Claims
• Unfair Competition Law
• Consumer Legal Remedies Act
Alarm-Free Facilities
Alarm-Free Nursing Homes Have Better Outcomes

- Masspro Case Study showed 32% reduction in falls for 1st quarter after implementation (Q4 2005)
  - at Jewish Rehabilitation Center for the North Shore

- Alarms do not prevent falls; they alert staff to a falling resident

- Alarms have negative consequences
  - Startle residents
  - Decrease overall mobility
  - Require staff time to respond, reset and document without solving why the resident was moving
  - From “Rethinking the Use of Position Change Alarms” by Joanne Rader, Barbara Frank, Cathie Brady; January 4, 2007
Surveyors are Resistant to Change

• Pushback from the state surveyors as alarms have become *de facto* standard


• Many states are supporting pilot programs
  – Minnesota Dept of Human Services Performance grant to Empira
  – Montana Fall 2012 presentation to their surveyors
Effect of this Trend on Litigation

• Defending Falls vs. Defending Injury
• What are the FacilityProtocols?
• Care planning still provides the roadmap to the defense standard of care argument