CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Medical Legal Summit
June 3, 2015 in Chicago, IL

The Affordable Care Act's Impact on Liability Insurance: Coverage, Cost and New Exposures

I. Nuts and Bolts of the Affordable Care Act ("ACA")

A. Goal: new approaches to improve performance and reduce cost

1. The ACA and its implementing regulations have created a new environment for health care providers and insurers, with a complex series of incentives and penalties designed to improve performance (i.e., see more patients with fewer medical providers) and reduce cost (i.e., shifting healthcare provision away from doctors and hospitals). This section discusses key aspects of this new world and the primary carrots and sticks that will drive compliance.

    a) Tighter control on Medicare fee schedules

    b) Penalties for certain Hospital readmissions

    c) Formation of Accountable Care Organizations (ACO's)

    d) Penalties for health plans with high expense ratios – goal to directs premium dollars towards patient care

    e) Creation of an Innovation Center to test, evaluate, and expand different payment structures that increase efficiency

    f) Greater focus on generic drug use

    g) Bundled payment system for inpatient hospital and post discharge services

    h) Pay for performance payment system: emphasis on prevention and quality

    i) Comparative Effectiveness Research

B. Key Provisions of the ACA

1. The ACA is 974 pages of legislation supported by 10,000 pages of final and proposed regulations. Within this mass of words, key

provisions of the law are relevant to the insurance industry. This section will discuss the individual and employer mandates, expansion of Medicaid, and the insurance exchanges.

2. Provisions to provide health coverage to current uninsured population-services- intended to have universal risk pool by including uninsured young and healthy pool
    a) Individual Mandate provision
    b) Employer Mandate provision
    c) Expansion of Medicaid eligibility
3. Creation of public insurance exchanges and other new entities
    a) Accountable Care Organizations
    b) Consumer Operated & Oriented Plans "COOPS"-directed by their customers and are designed to offer individuals and small businesses more affordable, consumer-friendly and high quality health insurance options.
    c) Narrow or "Skinny" Networks-limited network of health care providers, cost effective

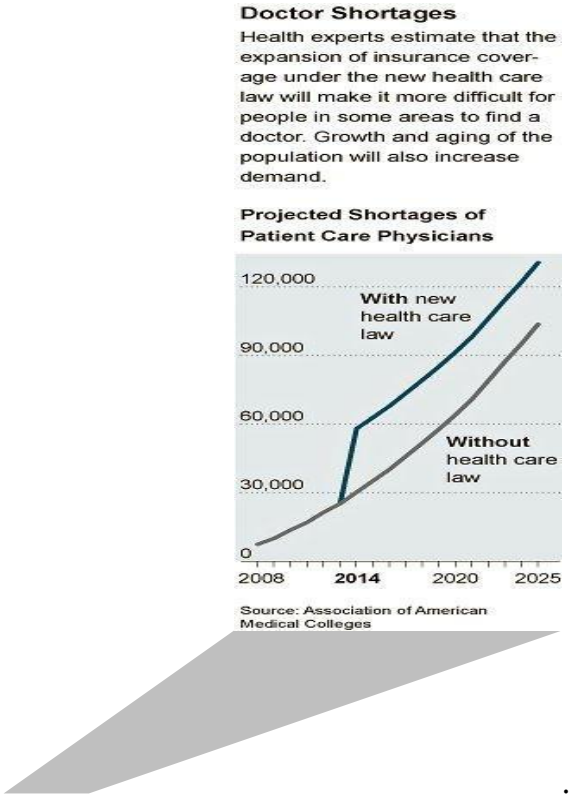
C. Shifting relationships in the ACA on insurers and healthcare providers

1. The ACA shifts longstanding aspects of the patient/doctor/insurer relationship. It alters the scope and accountability of healthcare providers, it shifts incentives for patients and providers, it shifts the standard of care, and it shifts the scope of regulatory compliance.
2. Provisions will affect health plans, and both patients and providers with potential for:
    a) Shift in scope of practice and "accountability" for providers
    b) Shift in compensation/employment related to quality outcomes
    c) Shift in incentives for patients and providers
    d) Shift in standard of care, whether real or perceived.
    e) Increase in audits and regulatory compliance expansion
    f) Decreases in reimbursement
    g) Increase in penalties

II. Top 5 Specific Impacts of the ACA

A. Supply & Demand

1. The ACA increases the number of potential patients and it increases the number of required touch points between the patient and the healthcare system all while there is a critical shortage of primary care physicians.
2. Inability of the system to keep up with demand.
    a) Under the ACA, increased responsibilities of the primary care physician.
    b) New federal budget proposes spending $5.23B over the next decade to foster increase in primary care doctors.
    c) The Balanced Budget Act of 1997 imposed caps on hospital residency positions for training new doctors. Over the past 17 years, a few hospitals have established residency programs for primary care docs with low single digit increases. Meanwhile US population has risen by 50 million or 20%. Of the new doctors, a small percentage enters primary care – the vast majority focus on more lucrative specializations.



.

B. Expanded Scope of Practice

1. The ACA increases the use of primary care physicians, physician assistants and nurse practitioners and requires the use of retail medicine.
2. How will the rendering of care change?
    a) Delegation of services to mid-level and ancillary providers due to shortage
        (1) "Physicians can delegate a task, but they cannot delegate liability"
        (2) Tug of war between Physicians and Mid-Levels
        (3) Scope of practice laws and regulations vary by state law and define what may or may not be provided by a professional licensed in the state
    b) PPACA appropriated $50M for Nurse Managed Health Centers-provide primary care and wellness services to underserved & vulnerable populations.
    c) Retail Medicine (Walmart)

C. Expands the use of technology

1. The ACA requires the transition to electronic medical records and Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act Omnibus Rule ("HIPAA/HITECH") sets a technologically standard for securing those medical records from accidental or malicious disclosure. The ACA also requires the use of telemedicine. Healthcare providers now must medically savvy and technology savvy, which creates personnel challenges.
2. Data compliance standards (HIPAA, HITECH and Gramm-Leach-Bliley Act) and the implementation of Electronic Health Records (EHR) requirements of the Affordable Care Act (ACA) require medical practices and healthcare organizations to utilize electronic data, but also ensure that the data is secure and methods are in place to report and recover any lost or stolen information.
    a) According to the PPACA, all health care providers must have electronic medical records (EMR) by 2015 or face penalties.

b) HIPAA/HITECH extends regulations to Business Associates- i.e., anyone who receives, creates, maintain and transmit PHI on behalf of covered entities (healthcare providers or insurers).

c) *See* **Appendix A** for detailed HIPAA/HITECH data breach information.

3. Healthcare Data-accounts for 43% of major data breaches according to the Identity Theft Resource Center.

    a) US Dept. of Health & Human Services database of major breach reports (those affecting >500 people) has tracked 944 incidents affecting personal information of from about 30M people. The majority of those records are tied to theft (17.4M) data loss (7.2M) hacking (3.6M) and unauthorized access (1.9M).

4. Have recent court decisions created a private cause of action under HIPAA?

    a) In this case, a pharmacist breached one of her most sacred duties by viewing the prescription records of a customer and divulging the information she learned from those records to the client's ex-boyfriend. A jury heard extensive evidence during a four-day trial and ultimately found that the pharmacist and her employer are liable for the damages sustained by the customer as a result of the breach and awarded plaintiff $1.8m.

    b) In another case, defendant was responsible for placing personal medical information on a database accessible to the public. Trial court denied class certification and found plaintiff had no standing and suffered no injury or economic loss. Order reversed because Plaintiff has a legal interest in having their medical information kept confidential. When a medical provider violates this interest, it is an invasion of that interest sufficient to satisfy standing. Class certification order reversed because all of the class members were in exactly the same position, and, because no injury (other than invasion of privacy interest) was alleged, there are no varying injury allegations outside of the common injury to the class' privacy interest.

5. The Accountable Care Organizations are based on shared financial savings that involves disclosing personal health information (PHI) – protected by HIPAA to various entities.

a) It requires sharing of information internally- as such information is being shared electronically with members who have different systems. This increases the risk of data loss

(1) i.e. private physician sends EMR to Hospital, ACO, pharmacy etc.

b) IRS agreed to share tax data with CMS for verification of household size & income to verify eligibility for health insurance.

D. Increased Audits and regulatory scrutiny

1. The ACA and its relationship to HIPPA/HITECH create a regulatory scheme that permits unannounced federal regulatory compliance audits and a system of fines and penalties.
2. Fraud & Abuse-The ACA allows CMS to conduct background checks, site visits and other enhanced oversight to weed out fraudulent providers. It created the following new requirements:
    a) Withholding payments-to any Medicare or Medicaid provider if credible allegations of fraud has been made and an investigation is pending
    b) PPACA expands the CMS "integrated data repository" to incorporate data and give the DOJ and OIG clearer right to access CMS claim and payment databases.
3. Stark Law is a federal law that limits physician self-referrals to any Medicare entity that they have a financial interest. The law changes:
    a) limits whole hospital exception;
    b) increased transparency requirements for physician ownership in ancillary services-need to notify patients of interest/options; and
    c) self-reporting protocol of actual/potential violations.
4. Corporate Practice of medicine is restricted.
    a) Physician actions and ethics should not be influenced by corporate entities.
    b) They have absolute control over medical decisions.
5. Anti-kickback statutes are intent based statute with civil and criminal liabilities and are triggered whenever someone knowingly and willingly gives remuneration to induce an action.

6. The ACA addresses antitrust issues too.
    a) FTC and DOJ will review mergers and acquisitions to avoid collusion of competitors and monopolistic behavior.
    b) There is no statute of limitations on challenges to completed transactions.
    c) ACO's may not have ERISA protection.
    d) ACO's do not have antitrust immunity either.
        (1) St Luke's which was the largest area hospital system - acquired the Saltzer Group medical practice as part of their plan to reward high quality work, stabilize insurance rates and allow access to medical care for indigent patients. The Saltzer Group was located across the street from the "other" area hospital – St Alphonsus – between St. Lukes and Saltzer, they included 80% of the primary care physicians in the area.
        (2) The FTC sued St Luke's for violating Section 7 of the Clayton Act anti-trust law, which prohibits mergers that lessen competition. The Judge determined the acquisition violated the law & ordered the acquisition "unwound" – The Court found the acquisition gave St. Luke's a large enough foothold that it could influence insurance premiums & the cost of patient care.
        (3) Shared savings programs.
        (4) Less likely to raise competitive concerns if institutional providers participate non-exclusively and if their combined market share is up to 30%. Otherwise, they could:
            (a) block commercial payers that incentivize patients to choose certain providers;
            (b) tying ACO services to the sale of other services – i.e. health insurers requiring ACO to contract with all of providers services;
            (c) contracting exclusively with non-primary care physicians – only primary care MDs can be exclusive; and

(d) share sensitive price data among ACO members.

E. Quality metrics & Cost Containment

1. The ACA transforms the standard of care to include regulatory accountability with the competing goal of setting financial incentives to provide quality care at reduced costs.
2. Will the quality outcome oriented focus create new causes of actions for facilities and hospitals with resulting increased frequency and severity of claims?
    a) The GAO looked at the possibility that the ACA could create new avenues for medical liability – specifically whether the ACA guidelines could be used as standards for medical practice. Although the GAO did not feel this was likely but left it up to the Courts to decide.
    b) Safe Harbor Statutes: enacted to prevent the ACA guidelines from being turned into standards for medical practice.
        (1) Georgia HB 499 – based on the AMA Model Act – prevents the use of the ACAs guidelines on healthcare quality measures, payment adjustments, hospital value based purchasing & value based modifiers – as "standards of care " in connection with medical malpractice claims.
    c) Value based payment models: hospitals are rewarded based on performance – failure to qualify for incentive payments (improved care & safety) can be viewed as negligence.
        (1) The two-midnight rule for Medicare beneficiaries means inpatient stays must last at least "2 midnights" to be considered reasonable and necessary. If the admission is shorter, it must be billed as outpatient treatment. This may increase cases of premature discharge.

III. State of the Market

A. The ACA has altered the insurance market and litigation environment

1. Assessing risk and exposure in the ACA environment is more challenging.

a) *Medical Professional Lines*: supply and demand issues including shortage of primary care physicians; the expanding scope of practice and the use of nurse practitioners, physician's assistants; and retail medicine, electronic health records, and telemedicine all expand the scope of healthcare liability claims – including into untested waters like the intersection of telemedicine and the standard of care.

b) *Workers Compensation and Auto PIP: possible* lower WC costs as claimants rely on private insurance to cover co-morbidities that are not related to the injury, which should decrease cost shifting.

c) *D&O and E&O* claims: antitrust issues associated with consolidation.

d) *Fiduciary*: The effect of the ACA on ERISA requirements and potential civil and equitable claims by health plan participants to enforce coverage requirements and information sharing.

2. Competitive
3. Market shift –significant entity consolidation, physicians joining Hospital programs
4. Decrease in premium
5. Tort reforms continue to be under attack
6. Softer terms and conditions-e.g. Batch wording -concerns about a different kind of severity.

    a) Longevity-increase in aged population increased need for care.

    b) Sweeping changes in Technology.

B. Five ACA standards that could give plaintiffs an advantage in litigation.

1. The ACA has altered settlement strategy in litigation
2. Physicians say a first-of-its-kind bill passed in Georgia will protect doctors from being exposed to increased liability associated with new federal health system reform standards. Supporters argue that without such a safe harbor, more than a dozen provisions of the Affordable Care Act could be used by plaintiffs for establishing civil tort liability in medical cases, including:

a) Adult health quality measures: The federal government is authorized to develop a core set of health care quality measures to be reported for adult Medicare beneficiaries.

b) Hospital readmissions reduction program: To decrease Medicare hospital costs, excessive 30-day readmissions of certain patients will mean lower payment rates.

c) Hospital-acquired conditions initiative: Facilities will be prohibited from receiving additional Medicare payment for treating certain hospital-acquired conditions.

d) Medicare shared savings program: Hospitals and physicians that coordinate care successfully for patients will share in some of the cost savings to the federal government that result — and might be penalized for failing to restrain costs.

e) Value-based payment modifier: Medicare payments to certain physician group practices will be modified based on how well they meet certain quality measures.

Appendix A

The purpose of this Appendix is to demonstrate how the ACA and the Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act Omnibus Rule ("HIPAA/HITECH") relate. This information is a summary of the data breach aspect of HIPAA/HITECH. It is not a comprehensive treatment of the data breach aspect, nor does it address other interrelated areas of HIPAA/HITECH like the enforcement or security provisions or how those provisions link to the ACA. You ***must*** seek additional guidance to ensure that your organization is complying with the ACA and with HIPAA/HITECH.

Electronic copies of the final rule published on January 25, 2013 can be found at the Government Printing Office website at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

The Department of Health and Human Services' Office for Civil Rights (OCR), the entity that has oversight and enforcement for HIPAA/HITECH, has indicated that significant new guidance and additional regulations will be published only on its website at: http://www.hhs.gov/ocr/privacy/.

The principal compliance obligations under HIPAA/HITECH include: (a) restricting access to protected health information (PHI) to only those employees who must use the PHI to achieve a legitimate healthcare or business function; (b) ensuring that employees with access to PHI use and disclose it only as permitted under the HIPAA Privacy Rule; (c) **implementing the physical, technical and administrative safeguards described in the HIPAA Security Rule for electronic PHI**; (d) notifying individuals, the state, and HHS when a security breach occurs; (e) refraining from disclosing PHI to third-party service providers, known in HIPAA parlance as "business associates," until the business associate signs a contract (or "business associate agreement"), which contains certain language required by the Privacy Rule; (f) notifying the appropriate person or entity of your privacy practices; (g) establishing policies and procedures to administer patient rights for data access and data restrictions under HIPAA; and (h) amending your agreements to comply with HIPAA/HITECH.

The Final Rule establishes **a new and lower standard for determining whether an entity is required to notify individuals of a security breach involving their PHI**. Under the old standard, notification was required only if an unauthorized use or disclosure of unencrypted PHI "posed a significant risk of financial, reputational or other harm" to the individual. *See* Interim Final HIPAA Breach Notification Rule, 45 C.F.R. § 164.402.

Under the revised standard, *any* **unauthorized use or disclosure of unencrypted PHI triggers a security breach notification obligation** *unless* **the organization can prove "a low probability that the [PHI] has been compromised based on a risk assessment."** *See* Final HIPAA Breach Notification Rule, 78 Fed.Reg. 5566, 5695 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 164.402).

The Final Rule does not define the word "compromise."

The referenced risk assessment **must consider at least the following four factors**:

1. **the nature and extent of the [PHI] involved**, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the [PHI] or to whom the disclosure was made;
3. **whether the [PHI] was actually acquired or viewed**; and
4. the extent to which the risk to the [PHI] has been mitigated." *Id.*

Other factors may also be considered where necessary. *Id.*

The first factor requires organizations **to evaluate the nature and the extent of the PHI involved**, including the types of identifiers and the likelihood of re-identification of the information. To assess this factor, **entities should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature.**

The second factor requires organizations to consider the unauthorized person who impermissibly used the PHI and to whom the impermissible disclosure was made. **Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information** (i.e., professional obligations, non-disclosure agreements, etc.).

The third factor requires organizations **to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.**

The final factor requires organizations to consider **the extent to which the risk to the PHI has been mitigated**.

Covered entities and business associates **should attempt to mitigate the risks to the PHI** following any impermissible use or disclosure, **such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed**, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

The organization's analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor discussed above. Other factors may also be considered where necessary. In the future, OCR will issue additional guidance to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.

If an organization determines that notice is not required, **it must document its risk assessment supporting that conclusion**. If that decision is questioned by the HHS or by a state attorney general (they are also authorized to enforce HIPAA) in an investigation, **the organization carries the burden of proving a low probability of compromise**. *Id.* at 5641, 5646.

To justify a decision *not* to provide notice, an organization must establish a low probability that an unauthorized recipient (or a potential unauthorized recipient in the case where PHI is lost) misused, or may misuse, the information. In addition, in light of the first risk assessment factor, the regulators likely will take the position that the more sensitive the PHI received by the unauthorized recipient, the lower the likelihood of misuse will need to be in order to justify *not* providing notification.

Organizations likely will be required to provide security breach notification more frequently under the Final Rule.

Impermissible uses and disclosures of PHI most commonly involve the following:

1. email attachments containing PHI that are sent to the wrong recipient;
2. email sent to the correct recipient but with an attachment containing PHI not intended for that recipient;
3. the loss or theft of a portable electronic storage device containing unencrypted PHI;
4. letters or explanations of benefits (EOBs) sent to the wrong person;
5. letters or EOBs with PHI either printed on the envelope or viewable through a clear envelope window; and
6. websites that, because of a technical error permit, viewing of one individual's PHI by others.

In most of these situations, especially those involving dozens, hundreds, or thousands of individuals (which often is the case), **it will be infeasible or overly burdensome to gather the facts necessary to *prove* what each unauthorized recipient did with, or might have done with, the errant PHI**. Consequently, it will be difficult to *prove* to the satisfaction of regulators "a low probability that the [PHI] has been compromised" because the organization likely will not have adequate documentation to support that conclusion.

The increased likelihood of a duty to notify translates into an increased risk of enforcement. HHS' record to date demonstrates a pattern of "breach-driven enforcement." Most publicized settlements with a covered entity originated when the organization notified HHS of a security breach.

The reason for this pattern is obvious: **under the HIPAA Breach Notification Rule, organizations are required to notify HHS of a security breach, effectively putting a target on their back**. *See* Interim Final HIPAA Breach Notification Rule, 45 C.F.R. § 164.408.

In light of the above, organizations should take steps to reduce the risk that the most common, impermissible uses and disclosures of PHI will occur and also should be prepared to respond rapidly to those incidents to establish, when possible, a low probability that the PHI will be compromised.

1. Organizations should encrypt email containing PHI, where feasible, because an impermissible disclosure of encrypted PHI does not trigger a notification obligation.
2. Employees who work with PHI should receive additional training and periodic reminders on steps that can reduce the risk of a mis-addressed email or the creation of attachments containing PHI not intended for the email's recipient.
3. Organizations can implement a clearance procedure before any communication containing the unencrypted PHI of more than a small number of people is emailed or mailed or can consider implementing data loss prevention (DLP) software.
4. Organizations also can implement policies that generally prohibit storage of unencrypted PHI on portable electronic media.
5. Organizations should carefully vet the security procedures of printers and other service providers responsible for mailing communications containing PHI.

To complement these measures, organizations should develop a plan of action that will permit them to document that erroneous recipients of unencrypted PHI never actually viewed the PHI.

1. A corporate IT Department can recall email sent internally or delete it from corporate inboxes before the email is opened.
2. If actual receipt of the misdirected PHI cannot be prevented, the organization may be able to call or email unauthorized recipients to confirm that they destroyed the PHI before reading it or promptly after realizing the communication containing the PHI was not intended for

them. Given human nature, as soon as you contact someone and tell them "they have a different person's PHI" the first thing most people **will do is look at the data**. **It's the "don't think about elephants" rule**. So this option may be a double-edged sword.

By documenting these steps, the organization could credibly prove "a low probability that the [PHI] was compromised," justifying a decision not to provide notice.

Finally, **organizations are encouraged to take advantage of the safe harbor provision of the Breach Notification Rule by encrypting limited data sets and other PHI pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742)**. If PHI is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information