AMERICAN BANKRUPTCY INSTITUTE

2017 Winter Leadership Conference

How Health Care Technology Changes Will Impact Your Practice

Hosted by the Health Care, Real Estate, and Technology and Intellectual Property Committees

J. Patrick Darby, Moderator
HealthSouth Corp.; Birmingham, Ala.

Michael R. Lane
Hammond Hanlon Camp LLC; Chicago

Johnny J. Lee
Grant Thornton LLP; New York

Samuel R. Maizel
Dentons US LLP; Los Angeles

CONCURRENT SESSION

2017

American Bankruptcy Institute

Health Care
Real Estate
Technology & IP
Committees

Winter Leadership Conference 2017

Patrick Darby
HealthSouth
Birmingham, AL

Michael Lane
Hammon Hanlon Camp
Chicago, IL

Johnny J. Lee
Grant Thornton
New York, NY

Sam Maizel
Dentons US LLC
Los Angeles, CA

Today's Agenda:

I. Electronic Health Record System (EHR) Implementation
II. Security Challenges Facing Healthcare
III. EHR Drawbacks
IV. Legal Considerations of Shift to EHR

EHR System Implementation

High Transition Costs to Electronic System

Large Implementation Cases

Henry Ford Health System	Budget of $353 million for an EPIC EHR system implementation. Budget was roughly 2/3 for Epic process and 1/3 other implementation costs, including data warehouse. Detroit, Michigan based health system that employees 30,000 people and 1,200 physicians. The system operates 6 hospitals (~2,600 beds) and a number of smaller facilities
Lahey Health	$160 million Epic EHR and patient portal implementation project. Later partially blamed for layoffs made at the system. Three hospital (~350 bed) Burlington, Massachusetts based system. The system also has a number of smaller outpatient facilities
Mayo Clinic	Estimated implementation of an Epic EHR system at over $1 billion

Estimated Cost on a Per-Provider Basis

Cost	In Office			SaaS		
	Upfront Cost	Yearly Cost	5 Year TCO	Upfront Cost	Yearly Cost	5 Year TCO
Estimated Average Cost	$33,000	$4,000	$48,000	$26,000	$8,000	$58,000

Sources: Becker's Healthcare (2016); US Department of Health and Human Services (2017)

Meaningful Use (MU) Subsidies

Subsidies Have Driven Implementation

Meaningful Use Phases

Phase 1	Promotes basic EHR adoption and data gathering
Phase 2	Emphasizes care coordination and exchange of patient information
Phase 3	Improves healthcare outcomes

Medicaid EHR Incentive Program

- Program runs from 2011 to 2021
- Maximum incentive amount is $63,750 (across six year time horizon)
- First year benefit of $21,500 with subsequent five year benefit of $8,500 per annum
- No Medicaid payment reduction for opting out
- In first year, providers can receive an incentive payment for adopting, implementing, or upgrading a certified EHR
- In all remaining years, providers will meet meaningful use guidelines, just like in the Medicare program

Strong EHR Uptake

- The percentage of office-based physicians using EHR systems has increased to 87% (2015) from 22% (2009)
- The Center for Medicare and Medicaid Services (CMS) has paid out over $37.2 billion to 533,000 providers
  - Total value of ~$70,000 per provider
  - Includes both initial costs and annual supporting incentives
- Meaningful use has been a rolling process of stricter EHR standards
  - EHR vendors must be "certified" for the healthcare provider to qualify for the subsidy
  - Phase 3 requirements have been introduced as voluntary in 2017 and will become mandatory in 2018
  - Only enroll in MU program once – comply with stricter requirements going forward – Vendors do much of upgrading and complying (software)

Medicare EHR Incentive Program

- Program ran from 2011 to 2016
- Maximum incentive amount was $44,000 (across five year time horizon)
- Payment reductions began in 2015 for providers who were eligible but chose not to participate
- In the first year and all remaining years providers must demonstrate meaningful use of certified EHR technology to get incentive payments
- Run by Centers for Medicare and Medicaid Services

Sources: Center for Disease Control (2015); Center for Medicare and Medicaid Services (2012; 2017)

Today's Agenda:

I. Electronic Health Record System (EHR) Implementation
II. Security Challenges Facing Healthcare
III. EHR Drawbacks
IV. Legal Considerations of Shift to EHR

Security Challenges Facing Healthcare

Cost of a Breach is Higher in Healthcare

$6.2 Billion Annually is Spent due to Breaches

Data Breach Costs		
Hospitals reporting a breach (last 2 years)		90%
Forensics cost	$	610
Breach notification cost		560
Legal defense cost		880
Post-breach clean-up costs		440
Average HIPAA settlement fine		1,100
Total Direct Cost	**$**	**3,590**
Estimated lost brand value	$	500
Estimated lost revenue		3,700
Indirect Cost	**$**	**4,200**
Total Cost of Data Breach	**$**	**7,790**

(000s)

Average of One Breach per Day in Industry

Data Breach Occurrences	
Total # breaches (2016)	450
Patient records lost (million)	27
% of breaches caused by insiders	43%
% of breaches caused by hacking / malware	27%
Average days to discover breach	238
Average days to discover if insider	607
Average days to report breach to HHS**	344

**Healthcare firms are required to report to HHS within 60 days

Sources: Becker's Healthcare (2017)

Healthcare Cybersecurity Efforts

Cybersecurity Investment Can Save Millions in the Future

Cybersecurity Budgeting

% of Total Budget Spent on Cybersecurity	% of Firms
0%	10%
Between 1% and 2%	36%
Between 3% and 6%	29%
Between 7% and 10%	15%
More than 10%	10%

Existing Defense Infrastructure

Cyber Defense Capabilities	% of Firms
On-premise web application firewall	61%
Distributed denial of service protection	42%
Content delivery network	21%
Cloud web application firewall	21%
None of the above	23%

Cybersecurity Budgets

Amount Spent on Cybersecurity	% of Firms
Less than $500,000	46.2%
Between $500,001 and $1 million	8.6%
Between $1 million and $5 million	5.4%
Between $5 million and $10 million	2.2%
More than $10 million	4.3%

Planned Defense Infrastructure

Cyber Defense Investment Plans	% of Firms
On-premise web application firewall	16.5%
Distributed denial of service protection	13.2%
Content delivery network	9.9%
Cloud web application firewall	6.6%

Sources: Healthcare Information and Management Systems Society (2017); Becker's Healthcare (2017)

Need for Cyber Certifications

Health Industry Vendors are Certified at a Lower Rate than Other Industries

Lack of Certification in Industry

- Health industry vendors less likely to make an investment in a cybersecurity certification than other industries vulnerable to cyberattacks
  - Only 26% of health IT, medical device, and outsourced service businesses maintain a security certification
  - Limited consistency in certification across industry for those that do have one
- Certain companies have begun to require that its vendors are certified in order to be engaged and handle its data. [discuss blues HiTrust requirement?]

Primary Healthcare Certification Vendors

Cyber Certification Types	% of Firms
Attestation Engagements No. 16	24%
PCI	23%
International Organization for Standardization 27001	19%
Service Organization Controls 1	18%

Sources: Becker's Healthcare (2017)

EHR Technology Challenges

Going Electronic Brings a New Set of Challenges

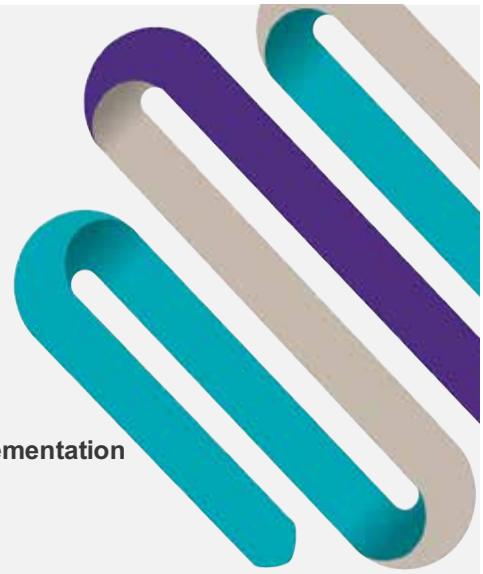
Significant Investment Required

- Large amounts of capital are needed to remain competitive and compliant with regulations
- Providers most in need of an EHR system are often those least able to afford the capital investment and the annual operating expense
- Providers without sufficient capital and revenue to support the investment can face a downward spiral
  - Competitive market is resulting in an eroding growth rate in reimbursement

EHR and Technology Implications

- Government reliance on data analytics makes technology more vital in compliance
- Technology investment increases cybersecurity exposure and requires additional investment and technical expertise to protect data
- Many healthcare entities regard their substantial investment in technology as critical to clinical, operational, and financial success
- Technology and data are critical for the improvement of clinical outcomes and future growth
- Provides the ability to seamlessly transfer patient data between hospital and providers; especially beneficial during natural disasters

Sources: The Boards Of Trustees: Federal Hospital Insurance and Federal Supplementary Medical Insurance Trust Funds



Today's Agenda:

I. Electronic Health Record System (EHR) Implementation
II. Security Challenges Facing Healthcare
III. EHR Drawbacks
IV. Legal Considerations of Shift to EHR

EHR Drawbacks

EHR System Investments Can Have a Disappointing Return on Investment

Lack of Value in a Wind Down or Liquidation

- Typically, only 1/3 of investment spend is on the system/technology. The remainder of the investment cost is on personnel costs to maintain and implement
  - The system/technology spend is commonly in the form of licensed usage rights where there is very little to monetize in a wind down

Records Retention Considerations

- EHR has brought additional considerations for records retention in a wind down
  - Compatibility and readability of data and the variety of formats
    - May require investment to convert certain types of data
  - Requirements for duration of retention and how records should be destroyed vary by state and whether wind down was achieved through filing bankruptcy
    - Bankruptcy law [applicable statute?] can potentially reduce the duration of records retention

Medical Record Retention Requirements Vary by State

Records laws vary by state

Hospital Record Retention Requirements	Adult (Years)	Minor (Years)	Minor (Min Age)
Minimum	0†	0†	
Maximum	Perm**	Perm**	
Selected Sample of States*			
Ohio	0†	0†	
Georgia	5		23
New York	6	6	21
Arizona	6	6	21
California	7	7	19
Illinois	10	10	
Texas	10	10	20
Colorado	10		28
Massachusetts	30	30	
Minnesota	Perm**	Perm**	

* State laws different, some are from time of discharge, others are from last service

† Ohio does not have a specific records retention law; exceptions include Medicare which has a federal 5 year requirement and Medicaid which has an Ohio 6 year retention requirement

** Minnesota requires most medical records to be kept permanently on Microfilm records, other records can be destroyed after 7 years (or 25 in the case of minor's records)

Sources: US Department of Health and Human Services

EHR Drawbacks Cont'd

Hidden Costs can Risk Entire Implementation Process

Major Factors in Management's ROI Analysis

Given the magnitude of investment, EHR decisions will commonly require management to perform ROI analysis for the board. Assumptions include:

- Technology / licensing cost vs. implementation / installation cost
  - General rule of thumb is 1/3 technology vs. 2/3 implementation
- Decrease in productivity, drop in billing activity, and reduction to cash flows during and immediately after implementation
- Increase in productivity and improvements in billing (less billing errors) on a steady state basis post implementation
  - Improved revenue cycle time (reduction in days): one time cash flow improvement
  - Better documentation, coding claim support, and reduction in billing errors: permanent cash flow pick up
  - Improved physician productivity and revenue
  - Reduction in administrative / clerical time
- Ongoing security / upgrade costs are often typically not included in ROI analysis and are in general IT budget

ROI analysis often shows a 1-5 year break even period

- Meaningful use timeline is expiring making any new investment more expensive than in previous years

Today's Agenda:

I. Electronic Health Record System (EHR) Implementation
II. Security Challenges Facing Healthcare
III. EHR Drawbacks
IV. Legal Considerations of Shift to EHR

Legal Issues

Strict HIPAA Regulations Result in High Compliance Costs

Maintaining Compliance

- Network security assessment
- Access rights
- IT
  - Technology
  - Upgrade/maintenance
  - Personnel
- Internet of things
  - Providers often need FDA approval to patch security vulnerabilities

Ramifications of Non-compliance

- Fine / Settlements
  - HIPPA enforced by the Office of Civil Rights (OCR)
  - Civil penalties range from $100 - $50,000 per patient record compromised
- Increased potential for breach
  - Civil suits
- Accessibility results in internal breaches

Jurisdictional Issues

- Inability to use data centers or personnel internationally (i.e., India)
  - This may also include the inability to share data within the US company if it's outside the 48 contiguous states and D.C.
    - [Alaska, Hawaii and Puerto Rico would result in transmitting data across international waters]

Issues for Bankruptcy Consideration

EHR Systems Create Additional Challenges in Court

Significant Investment Required

- EHR vendors achieve critical vendor status as they are not easily replaced
- Investment in technology has pushed hospitals over the brink and worsened their already distressed financial situation
- Independent hospitals that decide not to be involved with an M&A process often find they have wasted precious capital on systems that get scrapped
  - Small hospitals and health systems do not usually have EPIC systems
  - Lack of high-end EHR system creates cost of transition to new buyer which they take out on creditors when considering investment and ROI
- Technology is often financed with expensive debt or leases; financed soft costs usually are rejected outright with no option for lessors
- Technology spend does not translate to value or return to the estate in a bankruptcy
- Assumption and curing contracts often makes negotiation more difficult with creditors and is not easy with a vendor with leverage
- Transition agreements are usually required with key vendors post-acquisition to assist in the wind-down of estate matters
- Cyber security has become a much bigger issue given its direct relationship to compliance matters' poor systems with weak controls can create compliance matters that are expensive and embarrassing to overcome

American Bankruptcy Institute
Winter Leadership Conference
November 30-December 2, 2017
Palm Springs, California

Health Care, Real Estate, Technology & IP Committees

Industry Perspective on Technology and Capital Investment

Patrick Darby
HealthSouth Corporation

The author's views are personal and not attributable to HealthSouth Corporation or its affiliates.

Forward-Looking Statements

Statements contained in this presentation that are not historical facts, such as those relating to the likelihood, timing and effects of any program design, implementation or regulatory response, are forward-looking statements. In addition, HealthSouth may from time to time make forward-looking public statements concerning the matters described herein. All such estimates, projections, and forward-looking information speak only as of the date hereof, and HealthSouth undertakes no duty to publicly update or revise such forward-looking information, whether as a result of new information, future events, or otherwise. Such forward-looking statements are necessarily estimates based upon current information and involve a number of risks and uncertainties. HealthSouth's actual results or events may differ materially from those anticipated in these forward-looking statements as a result of a variety of factors. While it is impossible to identify all such factors, factors which could cause actual results or events to differ materially from those anticipated include, but are not limited to, the regulatory review and approval process; any adverse outcome of various lawsuits, claims, and legal or regulatory proceedings that may be brought by or against HealthSouth or any potential development partner or counterparty; the possibility any project will experience unexpected delays; the ability to successfully complete and integrate any acquisition consistent with HealthSouth's growth strategy, including realization of anticipated revenues, cost savings, and productivity improvements arising from the related operations and avoidance of unforeseen exposure to liabilities, including cyber or privacy security breaches; changes in the regulation of the healthcare industry at either or both of the federal and state levels; competitive pressures in the healthcare industry and HealthSouth's response thereto; the ability to maintain proper local, state and federal licensing; potential disruptions, breaches, or other incidents affecting the proper operation, availability, or security of HealthSouth's or any of its partner's information systems; the ability to attract and retain nurses, therapists, and other healthcare professionals in a highly competitive environment with often severe staffing shortages and the impact on labor expenses from potential union activity and staffing shortages; changes, delays in (including in connection with resolution of Medicare payment reviews or appeals), or suspension of reimbursement for services by governmental or private payors; general conditions in the economy and capital markets; and other factors which may be identified from time to time in HealthSouth's SEC filings and other public announcements, including HealthSouth's Form 10-K for the year ended December 31, 2016 and Form 10-Q for the quarter ended June 30, 2017.

A. About HealthSouth

HealthSouth Corporation is a leading provider of post-acute healthcare. Patients leaving an acute-care hospital may be discharged to a number of settings, based on acuity and healthcare needs, including (in descending order of acuity):

- Hospice.
- Long-term acute care hospitals.
- In-patient rehabilitation facilities.
- Skilled nursing facilities.
- Home health.

HealthSouth is the nation's largest owner and operator of inpatient rehabilitation facilities (IRFs) and the fourth-largest provider of Medicare-certified skilled home health services. As of August 15, 2017, HealthSouth owns and operates 125 hospitals in 32 states (including Puerto Rico) and 193 home health agencies and 37 hospice locations in 25 states. IRFs are fully-licensed hospitals, but do not have emergency rooms or intensive care units. IRFs provide physicians to oversee the patient's rehabilitation program and to manage and treat medical conditions. IRFs are fully staffed, around the clock, with nurses that provide personal care and oversee treatment plans. Physical, occupational and speech-language therapists provide a full range of rehabilitation therapy. IRFs are subject to strict admissions and coverage requirements. Patients must meet medical necessity requirements for hospital admission and must be medically stable and have the potential to tolerate at least three hours of rehabilitation therapy per day. To maintain IRF status, at least 60% of patients must have at least one medical diagnosis or functional impairment from a list of 13 conditions (CMS-13).

B. Healthcare Trends: Technology and Data

The healthcare industry is in the early stages of several seismic shifts. The overriding force is the aging of the American population. Baby boomers started turning 65 in 2011. The compounded annual growth rate in Medicare beneficiaries now exceeds 3%. The government projects the Medicare population to exceed 81 million by 2030, compared to approximately 56 million today. Estimates vary, but about half of the U.S. population spends little or nothing on healthcare. In contrast, about 5% of the population accounts for about half of healthcare spending. Spending is greatly concentrated in the aging populace.

Medicare's Hospital Insurance Trust Fund projects modest surpluses from 2017 through 2022, deficits thereafter, and insolvency by 2029. Even as the sickest portion of the population increases significantly, these projections assume substantial long-term reduction in per capita expenditures for healthcare.

As a result, healthcare providers must become more efficient to absorb lower reimbursement growth rates. Providers without substantial capacities in technology and data will face severe challenges in several areas.[i]

1. Integrated Delivery Payment Models, Value Based Purchasing, and Site Neutrality

Payors, including the Centers for Medicare and Medicaid Services (CMS) and private insurers, are moving away from traditional fee-for-service reimbursement. The transition to alternative payment models will stress provider integration and accountability. "Value based purchasing" ties reimbursement to patient outcomes, with tight focus on objective quality metrics such as discharging patients from the healthcare system rather than to another provider, and hospital readmission rates. Payors aggressively are pursuing reimbursement models that incentivize providers to reduce expensive outcomes.

Payors also are developing various models of "episodic payments," such as bundling several services together for a single payment. In episodic pricing, the payor provides a single reimbursement for an entire healthcare episode, such as a heart attack or a joint replacement, instead of breaking payment down by specific services. This practice cuts across providers as well as service lines. Traditional reimbursement for a knee replacement, for example, might involve separate fees for the orthopedic surgeon, the operation and short term stay at an acute care hospital, a longer stay at an IRF, further therapy at home, and outpatient therapy afterwards. An episodic payment provides a lump sum for the entire treatment and leaves the providers to figure out how to allocate payment to services.

Episodic payment is a step towards "population health management" and capitation. Today there are approximately 480 Accountable Care Organizations (ACO) nationwide. An ACO consists of a coordinated group of providers that accepts care of an assigned population of patients for negotiated fees. Reimbursement levels are tied to quality metrics and reductions in the total cost of care for the population. The ACO must allocate resources, services and reimbursement among its members. CMS recently tweaked the ACO model to create "next generation" ACOs, which appear to be gaining traction across the country. Commentators expect the trend towards capitation to continue. Increasingly, payment will be based not on services or episodes but per patient.

For existing fee-for-service Medicare payments, CMS has stated near term goals of making 50% via integrated payment models and 90% via payments tied to quality and value by 2018. The disintermediation of services will accelerate a drive towards site neutrality, where reimbursement will not be determined by sending patients to particular settings for particular services. The division of the post-acute care industry, for example, into separate sectors for IRFs, long-term acute care hospitals, home health agencies, skilled nursing facilities and hospice, will dissolve over time in favor of providers who offer the full range of services. Providers will have to leverage operational expertise over a wider base and manage across locations and service lines that traditionally have been separately defined and organized. Mastery of data will become more vital to identify the appropriate services and settings for large patient populations.

In addition, all of these alternative payment models will put greater emphasis on quality reporting metrics. Value based pricing programs already are creating winners and losers, and most hospitals are losing. Of 3,807 hospitals in value based pricing programs in 2015, only 1,700 qualified for quality bonus payments. After application of other program penalties, only

792 received net payment increases. Technology and data management are critical to clinical initiatives to improve quality through predictive modelling to identify patients at risk, design and implement intervention strategies, standardize protocols and practices through evidence-based decisions, and to transition patients between settings and services.

Finally, the ultimate purpose of episodic and population pricing is to save money. The payment models will not provide guaranteed reimbursement on a traditional "cost plus" method. Rather, providers will have to assume risk in negotiating lump sum payments that may be adjusted up or down based on outcomes. Providers must use technology to control costs, reduce overhead and streamline service. Hospitals no longer can afford to allow late test results reporting to delay discharges, or to allow beds to sit empty over weekends. In addition to using technology to meet quality measures and provide more efficient service, providers must have sufficient command of their data to understand the cost of their services and to negotiate flexible pricing and risk adjustment. For example, ACO models may provide "gain sharing" incentives, where participants divide a portion of the cost savings from their initiatives. Many providers lack the technical capacity to understand whether and how they can profit from, or even survive, such arrangements.

Due to changing payment models, the Congressional Budget Office estimates that if hospitals are unable to increase productivity or reduce costs, "the share of [hospitals] with negative profit margins [will] increase to 60% in 2025, and the average profit margin [will] fall to negative 0.2%."

2. Market Pricing

The alternative payment models discussed above in part represent the first, timid forays of CMS into market pricing. Although federal agencies typically distrust and do not understand market dynamics, a growing consensus recognizes that some element of competition will be necessary to control healthcare costs.

On September 20, 2017 the Centers for Medicare and Medicaid Innovation (CMMI) issued a Request for Information (RFI) calling for a "new direction" within the organization and seeking suggestions to promote patient-centered care, "test market-driven reforms," provide price transparency, and increase choices and competition to improve quality and reduce costs. The first guiding principle of the RFI is to promote choice and competition in the market. CMMI wants the industry to suggest voluntary payment models that the industry will embrace and is offering regulatory relief in return. Potential models are subject to testing and adoption if they are data-driven and objectively supported. For example:

> Consumer-directed care models could empower Medicare, Medicaid, and CHIP beneficiaries to make choices from among competitors in a market-driven healthcare system. To better inform consumers about the cost and quality implications of different choices, CMS may develop models to facilitate and encourage price and quality transparency, including the compilation, analysis, and release of cost data and quality metrics that inform beneficiaries about their choices. CMS will consider new options for beneficiaries to promote

> consumerism and transparency. For example, beneficiaries could choose to participate in arrangements that would allow them to keep some of the savings when they choose a lower-cost option, or that incentivize them to achieve better health. Models that we are considering testing include allowing Medicare beneficiaries to contract directly with healthcare providers, having providers propose prices to inform beneficiary choices and transparency, offering bundled payments for full episodes of care with groups of providers bidding on the payment amount, and launching preferred provider networks.[ii]

Many healthcare providers do not know how to set market prices for their services. Decades of top-down pricing dictated either directly or indirectly by the federal government has eroded the capacity to track and understand cost structures. To participate meaningfully in transparent, market-driven pricing, most providers will have to build pricing models from scratch. Data-driven pricing models based on actual costs, quality and outcome, will require significant technology to design and implement.

3. Electronic Claims Review and Submission

Submission of correct claims to CMS and other payors is critical to timely and accurate reimbursement. The American Medical Association, CMS and other organizations strongly recommend use of electronic claims. Electronic claim submission (a) reduces the amount of time and resources devoted to manual administrative functions; (b) allows providers to pre-audit claim fields automatically for potential errors before submission to a payer; and (c) allows providers to track a claim's progress between intermediaries and a payor. Submitting paper documentation can delay claims processing exponentially. For example, Administrative Law Judges that hear Medicare appeals accept paper records only by regular U.S. mail. ALJs presently are sitting on an enormous backlog of appeals stretching back at least 8 years. Staffers log paper submissions by hand and add them to a growing queue. Streamlining and eliminating manual processes through electronic records and submissions has become a material cash flow concern.

4. Compliance

Government prosecution of healthcare providers under the False Claims Act (FCA) has increased exponentially over the past 30 years. In 2016 alone, relators filed over 700 new cases. FCA settlements and judgments have surpassed $1.5 billion in recoveries in 2017. The government is on track to collect more than $3 billion annually from FCA cases for the eighth consecutive year. Most cases focus not on actual fraud but on billing errors, inaccurate or incomplete certifications, and disputed interpretations of regulations that are ambiguous and inconsistently applied. Electronic systems to create and track medical documentation are increasingly in demand to reduce compliance mistakes.

Increasingly, the government is relying on data analytics to identify potential FCA cases. Prosecutors then use statistical analysis to extrapolate damages well beyond provable losses for false claims. To the government, any statistical outlier is evidence of fraud. Providers need a strong data analytics program to counter government claims.

Moreover, the Department of Justice (DOJ) has indicated a data analytics program should be an important part of all providers' compliance programs. Earlier this year, the Fraud Section of DOJ issued an Evaluation Guidance that included a more granular look at the elements of an effective compliance program. One of the elements cited in the Evaluation Guidance relates to internal data analysis. The DOJ seeks to understand the type and frequency of internal audits, testing, and monitoring companies use to ensure that compliance programs are being followed, are effective, and are regularly enhanced as issues or weaknesses are identified in the program. For example: "Kaplan had policies and procedures in place to ensure compliance and there is no evidence that those policies and procedures were not followed. . . . . Thus, the evidence does not show that Kaplan 'buried its head in the sand' or failed to make basic inquiries to ensure compliance." U.S. ex rel. Gillespie v. Kaplan Univ., 09-20756-CIV, 2013 WL 3762445 (S.D. Fla. July 16, 2013).

In sum, data analytics is necessary to (a) identify mistakes, outliers and address compliance issues; (b) defend government compliance claims; and (c) demonstrate a culture of compliance to satisfy federal regulators. Technology is crucial to the effort.

C. Introduction of Electronic Health Record Technology

Through the American Recovery and Reinvestment Act of 2009 and the Health Information Technology for Economic and Clinical Health Act (HITECH), Congress granted the U.S. Department of Health and Human Services (HHS) authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health information technology, including electronic health records.[iii] Specifically through electronic health record incentive programs, certain hospitals and healthcare professionals were eligible for higher payments if such healthcare providers implemented electronic health record technologies and met certain specific criteria enumerated by CMS.[iv] As a provider of inpatient rehabilitation services, HealthSouth's hospitals were not eligible to participate in the incentive programs.[v] However, in 2011, HealthSouth determined that investing in electronic health record technologies complimented HealthSouth's dedication to constant improvement of the quality and efficiency of the patient care offered by its hospitals.

1. HealthSouth and Electronic Health Record Technology

In June 2011, HealthSouth executed an agreement with Cerner Corporation for the development and implementation of a company-wide rehabilitation specific electronic medical record (EMR). At the time, HealthSouth was the only multi-facility inpatient rehabilitation provider implementing such an EMR system. HealthSouth's unique system is referred to as Advancing Clinical Excellence through Information Technology (ACE IT).

In 2012 HealthSouth began a five-year implementation and completed the installation of ACE IT at 13 hospitals. HealthSouth has installed ACE IT in 120 of its 125 IRFs, with the remainder to be complete by mid-2018. ACE IT has earned an Analytics Stage 6 designation from the Healthcare Information Management Systems Society on its electronic medical record adoption model, a measure of the adoption and utilization of EMR functions by healthcare

organizations. HealthSouth believes it is the only post-acute provider to earn this recognition on an enterprise scale. Currently 81 HealthSouth hospitals have earned this exclusive recognition.

2. The Benefits of HealthSouth's EMR System

HealthSouth considers its proprietary and innovative rehabilitation-specific technologies as a significant driver of operational excellence, patient care, and financial performance. HealthSouth has devoted substantial effort and expertise to use technology to improve patient-centered care, promote operating efficiencies and to position its hospitals to collect, analyze, and share information on a timely basis. HealthSouth's ACE IT system automates the preponderance of all clinical functions and clinical data acquisition. Specifically, ACE IT capabilities and characteristics include:

- Clinical Data Repository
- Workflow Management
- Inpatient Rehabilitation-Specific Clinical Documentation
- Orders Management
- Computerized Provider Order Entry
- Clinical Decision Support
- Pharmacy and Medication Management
- Scheduling
- Document Imaging
- Clinical Reporting and Dashboards
- CMS Quality Reporting Capture
- Internal and External Interfacing (including labs and vendors)
- Dictation to Structured Documentation Tool (medical transcription)

The ACE IT system also facilitates compliance with key requirements integral to conditions of payment for inpatient rehabilitation hospitals, including, (i) pre-admission screening, (ii) post-admission physician evaluation, (iii) individualized plan of care, (iv) inpatient rehabilitation facility patient assessment instrument (includes functional independence measurements collected at key points of a patient's admission and discharge), (v) compliance with CMS-13 and other regulations and (vi) documentation of collaborative weekly team meetings as required to demonstrate an interdisciplinary approach to care.

Investment in successful clinical technologies requires continuous efforts to improve the system through user input and revisions to increase efficiencies. For example, HealthSouth has worked closely with Cerner to develop an algorithm that predicts patients with a high risk of acute care transfers. The tool allows HealthSouth to customize its care to achieve the best possible outcome for its patients. HealthSouth has further invested in products that promote care coordination and post-acute network management. These tools enhance patient care through predictive analytics (e.g. sepsis prevention) and positions HealthSouth to participate in alternative payment models.

The recent hurricanes in Houston, Florida and Puerto Rico required HealthSouth to evacuate patients from affected hospitals and relocate them to secure locations. ACE IT allowed

the instantaneous transfer of patient charts between hospitals. The transfer of paper records would have presented a major logistical challenge and a threat to seamless patient care.

3. Additional Beneficial Technologies

In addition to an EMR system, HealthSouth has developed several other information technology platforms, a performance management reporting system and an electronic pre-admission assessment application and customer relationship management system. Through these combined technologies, HealthSouth is in a position to connect with acute care hospitals, health information exchanges (HIEs), referral management companies, and accept and send direct messages related to patient care. To ensure connection between as many internal and external sources as possible, HealthSouth's information technology group has developed a patient hub to receive, transmit, store and integrate data for accuracy across internal and external systems. These functions are vital to the emerging models of collaborative care and to improve patient outcomes.

HealthSouth's continued investment in technology has positioned it to continue to be the leading provider of inpatient rehabilitation and home health services through efficient integrated coordination of patient care with acute care hospitals and physicians, reduction of cost and duplicative efforts related to the sharing of information and analyze aggregate clinical date to further the goals of population health initiatives.

4. Post-Acute Collaborative Initiative with Cerner

HealthSouth has entered into a post-acute innovation collaboration with Cerner. The goal is to develop evidenced-based tools to manage patient care after discharge from the acute care hospital. The tools will analyze massive amounts of data to help determine the proper placement of patients, help design programs and protocols to improve patient care, facilitate coordination among providers and settings, and control costs. The post-acute network management tools currently available in the market were developed either by non-healthcare providers with limited clinical expertise or providers that have not made the necessary technology investments to advance efficient, patient-focused care. Combining HealthSouth's experience with clinical experience and outcomes, its EMR system and other information technologies, with Cerner's leading health information technology solutions and data analytics, will create clinical decision support tools to more effectively and efficiently manage patients across multiple care settings.

D. Implications for Companies that Fail to Implement Electronic Medical Records

Certain health care providers that do not adopt and successfully demonstrate meaningful use of EMR technology by 2015, will receive negative payment adjustments from Medicare and Medicaid and the amount of the adjustments will increase in subsequent years. According to information published by the American Hospital Association, about 200 hospitals received payment penalties in 2016.[vi]

The Affordable Care Act (ACA) created Bundled Payments for Care Improvement (BPCI) initiatives to test innovative payment and service delivery models that had the potential to reduce Medicare and Medicaid expenditures while preserving or enhancing the quality of care for beneficiaries.[vii] Successful participation in a BPCI initiative and other alternative payment models requires collaboration by all participating health care providers to effectively manage payment distributions for the coordinated patient care. Absence of a functional EMR system makes this collaboration impossible, placing limits on the patients and services a non-EMR health care system can provide.

E. Potential Costs of EMR and Other Technology Initiatives

1. Investment

The industry faces a gap in capital and in expertise in implementing EMR technology. Many health care systems throughout the country cannot afford the implementation costs, maintenance expenses and ongoing research and development costs of EMR. EMR is a practical necessity in today's healthcare market. Providers at a competitive disadvantage over a lack of EMR investment are likely to be the providers least able to afford the capital investment EMR demands. Similarly, many EMR users lack the technical capacity to capitalize on EMR platforms. For example, health care providers attempting their own data analytics with inadequate support face the burden of significant costs and allocation of IT resources. In addition to the capital outlay, data analytics is cost prohibitive for many health care providers from an operating standpoint and creates an unmanageable strain on IT resources. Adopting an EMR system that merely performs operational tests and data entry and retrieval compounds the challenges presented by lack of capital.

2. HIPAA Breaches: Cyber Attacks, Ransomware, Employees, Third Party Vendors, and Improper Security Protocols

The Health Insurance Portability and Accountability Act (HIPAA) provides for civil and criminal penalties for breaches of patient health information (PHI). The U.S. Department of Health and Human Services Office of Civil Rights (OCR) investigates these breaches and levies the applicable fines. Currently, the OCR has 375 open cases under investigation for breaches reported in the last 24 months that involve a breach of PHI for 500 or more individuals. These breaches result from a range of activities, including, cyber-attacks and hacking of network servers and electronic mail, loss of laptops by employees, unauthorized access by employees, unauthorized use and disclosure by third party vendors, and failure to maintain proper security protocols to prevent unauthorized use and disclosure of PHI.

Various industries, including healthcare, "have been the targets of advanced cyber-attacks where millions of personal identifiable information was stolen.[viii] Cyber-attacks in healthcare saw an increase from 20% to 40% in the period between 2009 and 2013.[ix] "The FBI has warned the healthcare industry that the IT systems and medical devices [of healthcare providers] were at

risk for increased attacks from hackers due to lax cyber security standards and practices.[x] According to the HIPAA Journal:

> 2015 was a record year for healthcare industry data breaches. More patient and health plan member records were exposed or stolen in 2015 than in the previous 6 years combined, and by some distance. More than 113 million records were compromised in 2015 alone, 78.8 million of which were stolen in a single cyberattack. 2016 saw more healthcare data breaches reported than any other year, and 2017 looks set to be another record breaker.[xi]

Although it is critical for healthcare providers to protect themselves from cyber-attacks, ransomware and other malicious cyber activities, internal activities pose significant dangers to protecting PHI. Improper or unauthorized access by current employees of patients' medical records, third-party vendor breaches, and even unauthorized access by former employees poses just as great of risk, if not more, than the "outside" dangers.[xii] In addition, a vast majority of healthcare facilities and providers use third-party vendors for both their day-to-day operations and for document storage and maintenance. Notwithstanding the security protocols implemented by a healthcare provider, a breach by a third-party vendor may affect all of a provider's patients. [xiii]

The federal government essentially has declared its inability to protect American businesses from cyberattack (it retains the ability to fine the victims of attacks -- see below). EMR naturally increases exposure to cyberattack. In addition to the initial EMR investment, and the operational cost of maintenance and use, providers must invest heavily in personnel, systems and procedure to protect cybersecurity.

3. Penalties for HIPAA Breaches

Civil penalties range from $100 per patient record to $50,000 per patient record depending on the level of negligence of the health care provider responsible for the breach. Breaches resulting from willful negligence can also carry criminal charges and jail for the responsible parties. In 2016, payments to OCR to settle alleged HIPAA violations totaled over $22.8 million.[xiv] Seven settlements were in excess of $1,500,000. By July of 2017, OCR had levied fines in excess of $17 million for alleged HIPAA breaches.[xv]

4. The Internet of Things

The internet of things refers to electrical devices that communicate data via the internet. Hospitals are filled with devices connected to the internet. Each device compounds the risk to cybersecurity. During recent ransomware scares, providers were unable to patch vulnerable devices because they lacked FDA approval.

[i] 2017 Annual Report of the Boards of Trustees of the Federal Hospital Insurance and Federal Supplementary Medicare Insurance Trust Funds, July 13, 2017.

[ii] Centers for Medicare & Medicaid Services: Innovation Center New Direction (September 20, 2017)

[iii] https://www.healthit.gov/policy-researchers-implementers/health-it-legislation

[iv] https://www.healthit.gov/providers-professionals/ehr-incentive-programs

[v] https://www.healthit.gov/providers-professionals/ehr-incentive-programs

[vi] http://www.aha.org/advocacy-issues/factsheets/fs-meaningfuluse.pdf

[vii] https://innovation.cms.gov/initiatives/bundled-payments/

[viii] Karen Painter Randall & Steven A. Kroll, *Getting Serious About Law Firm Cybersecurity*, 300-JUN. N.J. LAW. 54 (2016).

[ix] Samantha Singer, *'The Greatest Wealth Is Health': Patient Protected Health Information in the Hands of Hacker*s, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 657, 667 (2015)

[x] Jane Kim & David Zakson, *Health Information and Data Security Safeguards*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 133, 134 (2016).

[xi] See https://www.hipaajournal.com/category/healthcare-cybersecurity/

[xii] *See* Akanksha Jayanthi, *12 latest healthcare data breaches*, BECKER'S HEALTH IT & CIO REVIEW (Jun. 20, 2016), http://www.healthcareitnews.com/news/health-data-breaches-march-surpassed-january-and-february-combined-study-finds. HIPAA Journal, in its June 2016 posting even stated: "Insider data breaches can be the hardest to prevent, although controls can be put into place to reduce the likelihood of snooping by employees." *ProMedica Uncovers Unauthorized Accessing of PHI by 7 Employees*, HIPAA JOURNAL (Jun. 3, 2016), http://www.hipaajournal.com/promedica-unauthorized-accessing-phi-7-employees-3457/; *see also* Erin McCann, *Snooping staff still top security issue*, HEALTHCARE IT NEWS (Aug. 19, 2014, 10:54 AM), http://www.healthcareitnews.com/news/snooping-staff-still-top-security-issue (stating: "Employee snooping and insider misuse also prove to be among the biggest privacy threats in the healthcare sector today.").

[xiii] Akanksha Jayanthi, *Vendor breach exposes 87,000 Southeast Eye Institute patients' data*, BECKER'S HEALTH IT & CIO REVIEW (May 27, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/vendor-breach-exposes-87-000-southeast-eye-institute-patients-data.html; *Third Parties a Major Culprit in Healthcare Breaches*, SECURITY SCORECARD, https://blog.securityscorecard.com/2015/10/29/third-parties-breaches-healthcare/.

[xiv] See https://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/

[xv] See https://medcitynews.com/2017/07/hipaa-settlements-so-far-this-year/