

American Health Lawyers Association  
In House Counsel Program  
Chicago  
June 24, 2012

---

## Doing Good and Avoiding Evil with Electronic Patient Information Technology



**Bernadette M. Broccolo**  
**McDermott Will & Emery LLP**  
**[bbroccolo@mwe.com](mailto:bbroccolo@mwe.com)**  
**312.984.6911**



**Cynthia F. Wisner**  
**Assistant General Counsel**  
**Trinity Health**  
**[wisnerc@trinity-health.org](mailto:wisnerc@trinity-health.org)**



## Introduction and Overview

---

- The “Triple Aim” Calls for Organizing Care To:
  - Improve the health of the population
  - Enhance the patient experience of care (including quality, access, and reliability); and
  - Reduce, or at least control, the per capita cost of care.  
(Source: Institute for Healthcare Improvement  
<http://www.ihl.org/IHI/Programs/StrategicInitiatives/TripleAim.htm>)
- Goes beyond payment-focused goals of managed care integration/alignment initiatives to address both the payment and care delivery components of the recent federal health reform legislation.

## Introduction and Overview

---

**Accelerating** the development and implementation of an effective IT strategy is essential not optional.

- Need meaningful electronic exchange of patient information to meet the demand for comprehensive and accurate information exchange in the real-time clinical care delivery context.
  - Discharge planning, care consultation and coordination
  - Service delivery via telemedicine
  - Increased patient involvement
- Payers (both public and private) will select providers based on a value equation (i.e., cost v. quality, coordination, accountability, improved patient experience and population health)
  - Requires access to and analysis of robust retrospective information to support:
    - Benchmarking of quality and cost performance
    - Conducting comparative effectiveness and outcomes studies

3 3

## The Mantra ... It's ALL about the DATA!!!

---

“...what we know is that **transfer of information is critical ... [t]hat's the human rocket science** of how you make health care systems work well.”

*Source: Bill Moyers Journal, Transcript of Interview of Dr. Jim Yong Kim, President of Dartmouth College and co-founder of Partners in Health, September 11, 2009, <http://www.pbs.org/moyers/journal/09112009/transcript2.html>*

4 4

## Developing a Electronic Information Strategy

---

- Key Elements of any Strategy
  - Access to Data
  - Exchange of Data
  - Analysis of Data
  - Artificial Intelligence (e.g., Decision Support)
- Critical to orient developers, architects and analysts to both clinical and financial processes and workflow so that electronic information strategy and workflow are synchronized.
- No one approach will be free of compliance and business risk.

5 5

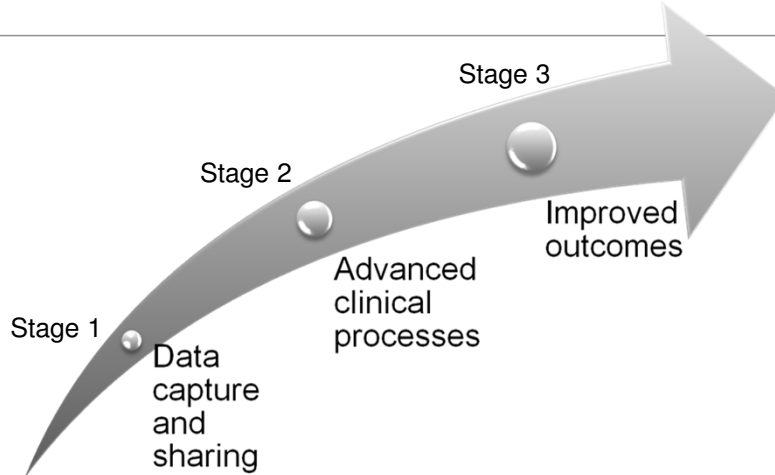
## Myriad Stakeholders/Participants

---

1. Stand-alone community hospital
2. Regional multi-hospital system
3. National multi-hospital system
4. Small single specialty medical group
5. Large single specialty medical group
6. Government payer
7. Private payer
8. IT vendor
9. Health care consultant (strategy, planning, etc.)
10. IT consultant

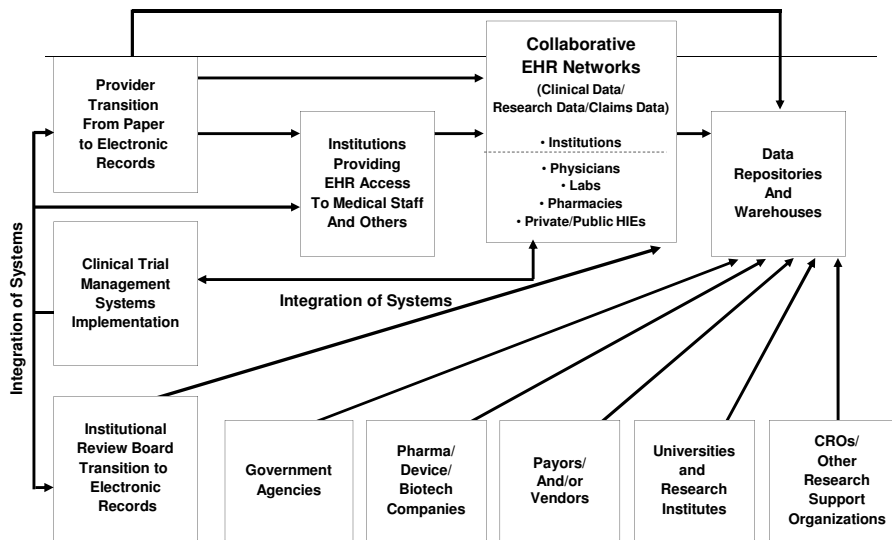
6 6

## EHR Initiatives: Evolution of Meaningful Use



7

## Harnessing EHR Capabilities to Create Robust Repositories



8

## Health Information Exchanges (HIEs)

---

- Health Information Exchange
  - Electronic movement of health-related information among organizations according to nationally recognized standards
- National Health Information Network (NHIN)
  - NOT a central data repository
  - A set of standards and core services and policies that enable the secure exchange of information over the internet between and among state and regional exchanges
- HITECH Act Funding of Various State HIE Initiatives
- 7th Annual *eHEALTH INITIATIVE* HIE Survey:
  - 234 Known HIE Initiatives are underway
  - 73 are “operational”

9

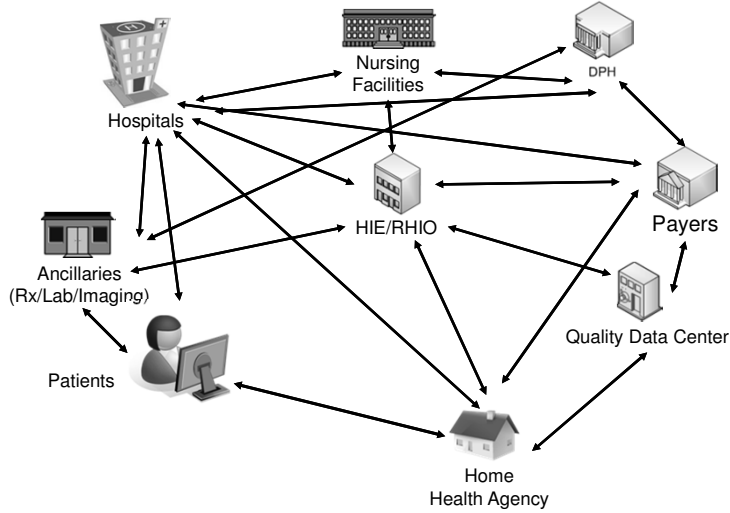
## Health Information Exchanges (HIEs)

---

- A small but critical mass of sustainable HIEs exists
- Use of HIEs can reduce staff time and testing redundancy
- Scope of exchange
  - Initially is limited to treatment and primarily laboratory results and diagnostic images
  - Use for healthcare operations and/or clinical research will likely evolve
- Payor participation
  - Most initially have no Payor Participation
  - But, a significant Increase in Payor Participation occurred last year and will likely continue to increase
- Key Challenges remain:
  - Sustainability absent/after federal funding
  - Adapting to challenges presented by federal policy changes and evolving standards
  - Governance

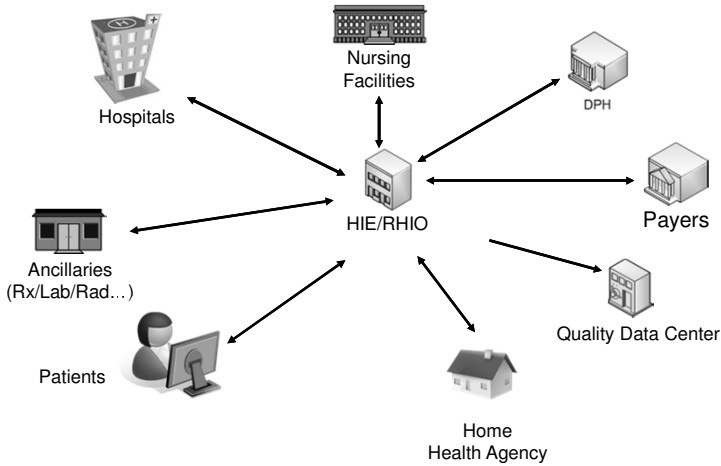
10 10

# HIE – “Direct” Interface Alternative



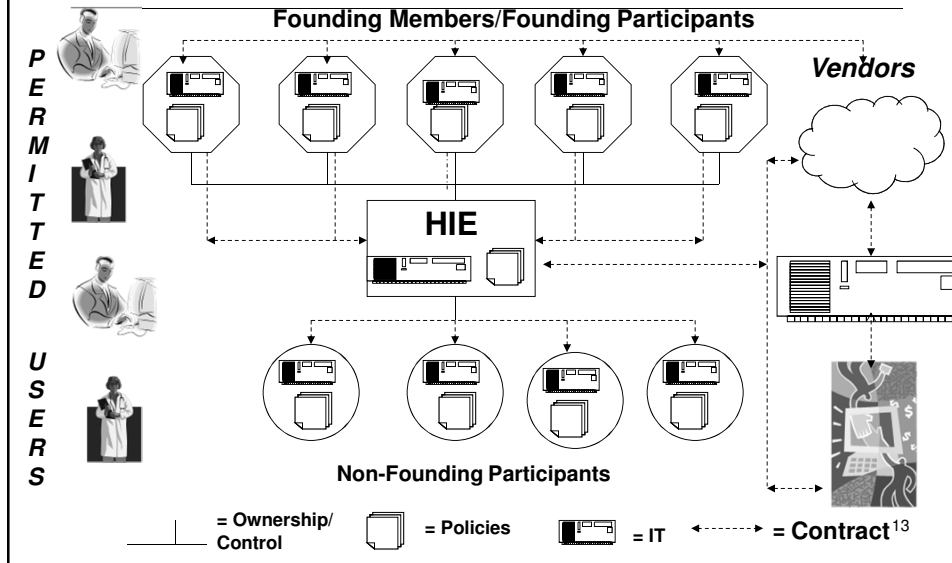
11  
11

# HIE – “Federated” Approach



12  
12

## HIE Relationship Complexities



## Telemedicine Initiatives

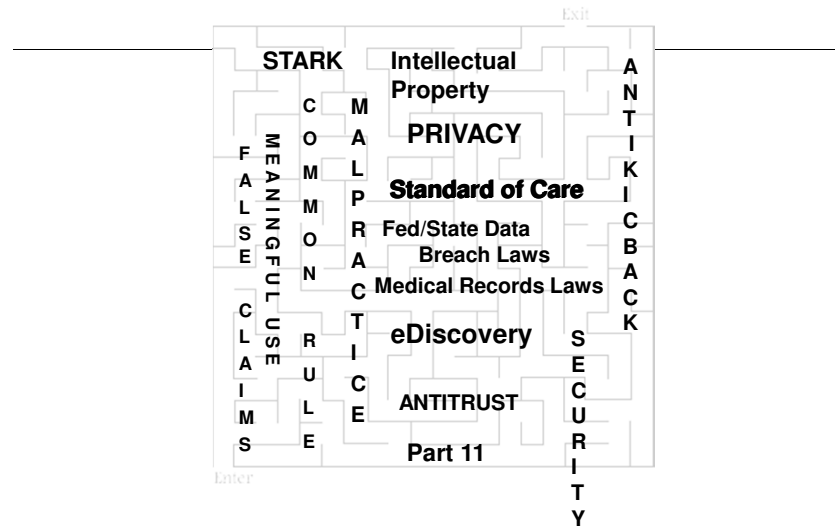
- **Public and Private initiatives that fund/oversee/service high-speed internet networks to connect rural facilities with specialists at larger institutions**
  - Nearly-instantaneous transfer of diagnostic images such as MRI or CT scans
  - Real-time virtual consults for trauma patients whose injuries surpass the capabilities of small-hospital practitioners
  - Psychiatric services in real time
  - Home monitoring of at-risk patients
  - Better access to important patient information via electronic medical records
- **OIG is open to technology sharing and funding**
- **OIG Advisory Opinion 11-18** *Issued 11-30-2011 posted 12-7-2011*  
OIG issued favorable Advisory Opinion re: an online service to facilitate the exchange of information between healthcare practitioners, providers, and suppliers
- **OIG Advisory Opinion 11-12** *Issued 8-29-2011, posted 9-6-2011*  
OIG issued favorable Advisory Opinion re: health system's provision of neuro-emergency clinical protocols and immediate consultations with stroke neurologists via telemedicine technology to certain community hospitals

## Leveraging Resources through Cloud Computing

- An evolving “service model” paradigm
  - Enables ubiquitous, convenient, “on-demand,” network access to a shared pool of configurable computing and data resources housed in a remote environment
- Service Models
  - **Platform (PaaS)**: security, workflow, database management
  - **Infrastructure (IaaS)**: storage, computing power
  - **Software (SaaS)**: application suites or services
- Relationship Models – private, community, public, hybrid
- Akin to ASPs, Hosting and Utility Computing
- Servers often housed in various locations
  - domestically and internationally
- Current players ... to name just a few
  - Google, Amazon, Microsoft, Yahoo
  - Boutique, niche vendor

15

## Key Legal and Compliance Challenges



16



## Federal and State Privacy and Security Law Compliance

---

- HITECH Act HIPAA Enhanced Privacy and Security Protections
  - Security breach notification requirement
  - Expanded applicability beyond current “covered entities” (including sanctions) to business associates
  - Accounting for all treatment, payment and health care operations disclosures
  - “Shutting down the secondary market” for sale and mining of data
  - Preserves flexibility for research.
  - Some movement to streamline informed consent and HIPAA authorization procedures for research for such secondary purposes
  - Modified and expanded sanctions for violations
- FTC Breach Notification Rule Applies to Vendors of PHR and PHR Related Entities
- State Breach Notification Rules (e.g., MA, CA)
  - May be more stringent than HIPAA and FTC rules

17

## Federal and State Privacy and Security Law Compliance

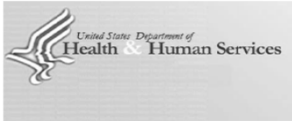
---

- State “Sensitive Information” Privacy/Confidentiality Laws create additional restrictions that can preempt HIPAA
  - The nature of the restriction can vary by state and by category of information
- State laws may require a consent to:
  - Disclose information for any purpose (even treatment or healthcare operations purposes) to other than members of the “treatment team”
  - Retain a Business Associate to create a Limited Data Set or to De-Identify information
  - Use sensitive information even in fully De-Identified form to conduct quality studies, comparative effectiveness and outcomes research, and clinical research
- State law may not recognize key aspects of HIPAA
  - De-Identified Data and Limited Data Set
  - Distinction between “Healthcare Operations” and “Research”
- Compliance challenge is exacerbated for information exchange across multiple state lines.

18

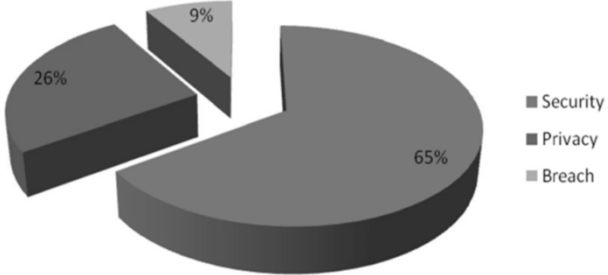
# Federal and State Privacy and Security Law Compliance

- Consent challenges:
  - Timing, specificity, duration
  - Future v. retrospective data
  - Conducting future research
  - Opt-in v. Opt-out
  - Affect on integrity and utility of the information exchange/repository?
- Disclosure in Notice of Privacy Practices may be needed to supplement consent.
- Consider including permission to create a repository and develop future limited data sets early in patient relationship.
- Reconcile State privacy law consent requirements with HIPAA, Common Rule and FDA consent/authorization requirements.



## OCR initial review of 20 audited covered entities

Analysis of Findings by Rules



## KPMG HIPAA Audit Findings

---

### SECURITY FINDINGS

- ✓ user activity monitoring & granting and modifying user access
- ✓ disaster recovery/contingency planning
- ✓ authentication/integrity
- ✓ media reuse and destruction;
- ✓ risk assessment

21

## KPMG HIPAA Audit Findings

---

### PRIVACY FINDINGS

- ✓ patient access to records
- ✓ policies and procedures
- ✓ decedent information
- ✓ personal representatives
- ✓ business associate contracts

22

## NIST: Top 3 Potential For Harm Concerns with EHRs

---

### 1. Patient identification errors

Without full patient identification with integrated apps like imaging, the wrong actions could be performed on the wrong patient

### 2. Data accuracy errors

truncated data, when discontinued meds aren't eliminated and when changes in status aren't displayed accurately

### 3. Medication errors

Medication errors are generally associated with manual transcription between medication charts and discharge summaries

National Institute of  
Standards and Technology

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

23

## Documentation Integrity Errors

---

- Biggest integrity issue in the EHR is over-writing
  - Alteration of records implicates state law
- Second biggest integrity issue in the EHR is cut and paste



24



## Privacy/Security Problems

---

- HHS report concludes hosp-doctor links are being layered on system that already has glaring privacy/security problems.
- HHS examined computer security at seven large hospitals and found 151 security vulnerabilities. The report **classified 4 out of 5 flaws as "high impact,"** meaning they could result in costly losses, even injury and death.
- Among the flaws were:
  - inadequate passwords;
  - computers that did not automatically log off inactive users; unencrypted laptops that contained pt. data.
- HHS also criticized agencies' lax enforcement HIPAA security rules.

25

## Fundamental Risk Management Guideposts

---

- **ALL** parties play a role in creating and managing potential risks.
- Need to anticipate scope of the risk in both the short-term and the long-term
- Key Questions/Guideposts
  - Who is in the best to manage/prevent against the risk?
  - Who is able to insure against the risk?
- A thoughtful and thorough approach to risk allocation and risk management at the front-end will enhance the likelihood of short-term and long-term success and overall sustainability
- Risk management strategy will likely be multi-faceted:
  - Business processes – synchronization with IT and proper training
  - Policies, procedures and training and enforcement related to them
  - Technology infrastructure features, functions and performance capabilities
  - Contract allocation of risk in third party relationships
- There is no "one size fits all" solution

26

## Fundamental Risk Management Guideposts

---

- Contracting Considerations and Strategies
  - Develop a contract for all relationships involved
    - All players, large and small
    - Consider both primary contractors and subcontractors
  - Allocation of Relevant Responsibilities
    - Source of potential risk
    - Control over management/avoidance of the risk
    - Liability for costs/damages
- Where and how to draw the lines is unclear in many respects
- Risk posture of vendors and other third parties has changed on some key issues, demanding new approaches to allocation of risk on key issues

27

## Scenario 1 - Stolen Laptop

---

Joe Jackson takes his laptop everywhere. His laptop is encrypted and he is careful to save on his laptop only the info he needs for his travels and to back up the laptop on the shared drive. Sadly Joe's apartment was broken into last week and the laptop was stolen.



28

## Is It a Breach?

---

- HITECH Breach involves unsecured PHI
- PHI on an encrypted laptop is not unsecured PHI
- Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance

29

## Is the Device Encrypted?

---

- State laws also generally require notice to the state and patients if the information is on an unencrypted device
  - California's consumer security breach notification law was the nation's first to require data owners to disclose a data breach to any California resident whose **unencrypted personal information** is reasonably believed to have been acquired by an unauthorized person
  - 46 states currently have breach notification laws



30

BOSTON.COM CARS | JOBS | REAL ESTATE TEXT SIZE | GE

**The Boston Globe** **Health & wellness**

---

NEWS METRO ARTS BUSINESS SPORTS OPINION LIFESTYLE MAGAZINE TODAY'S PAPER MY SAVED

---

FOOD & DINING HEALTH & WELLNESS STYLE TRAVEL COMICS CROSSWORD NAMES

---

**In this section**  
Health & wellness

---

State mental hospital in Taunton has uncertain future

---

N.H. officials: Needle-swapping employee may have caused outbreak

---

Nursing homes miss out on aid targeting antipsychotic drugs

## Laptop lost with data for more than 2,000 patients, Boston Children's reports


By [Chelsea Conaboy](#) | GLOBE STAFF MAY 22, 2012

---

ARTICLE PREVIEW
COMMENTS
SUBSCRIBE


While at a conference in Buenos Aires, a Boston Children's Hospital employee lost a laptop containing a file with information about 2,159 patient, including names, birth dates, diagnoses, and treatment information. The laptop was password protected but not encrypted according to a hospital press release

31



## Scenario 2

### Stolen Smart Phone

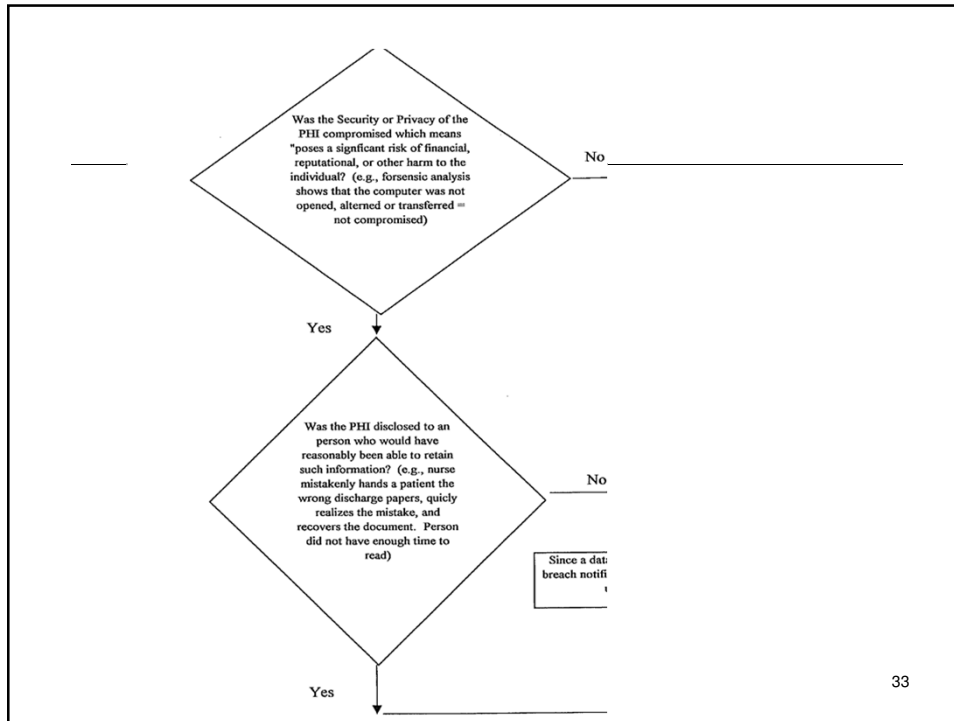


Jill Langster has a smart phone and was able to link her work email to her phone. She works in the coding and billing area and receives a lot of email with patient information.

She has added a password to her phone, but the email icon, when touched, displays all of her email. She left her smart phone plugged in to the charger in the hotel. The hotel staff called her and let her know that they have the phone and that she can pick it up.

32





33

### Major HITECH Act Breaches Affect More than 20 Million

Breaches involving more than 500 patients rose to 435 and affected 20,066,249 individuals according to the latest analysis of OCR statistics from April 18 through May 17 by *Health Information Privacy/Security Alert*. That represented an increase of 25 reported breaches affecting an additional 904,179 patients.

Theft was a reason for a breach in more than half of the reported incidents. Unauthorized access/disclosure issues were involved in 99 incidents.

Business Associates were involved in only one of the newly listed breaches. They accounted for a total of 96 incidents (10 of the latest 25 breaches) or about 22% of all breaches.

# of Breaches	Reason
36	Theft
29	Unauthorized Access/ Disclosure
18	Loss
5	Hacking/IT Incident
3	Unauthorized Access/Disclosure and Hacking IT/ Incident
2	Improper Disposal

Source: *Health Information Privacy/Security Alert* Analysis of HHS Office for Civil Rights

34

## BUT, not everyone is honest

---

**Ochsner Medical Center:** On March 3, 2009, Washington brought the stolen patient information sheets to the residence of his girlfriend, Blair, who then created online accounts with companies such as Kohl's, Target, American Eagle, Old Navy, Citizen's Bank, and Best Buy, in the names of the hospital patients contained on the information sheets.

**Howard University:** Six weeks after Howard University Hospital told more than 34,000 patients that a contractor's laptop containing their personal health information had been stolen; federal authorities have filed criminal charges against a hospital worker accused of selling people's medical records.



35

Now, suppose Mr. Washington was employed by a company acting as a Business Associate of Oschner...

---

- BAA is subject to enforcement by OCR
- Nonetheless, the Covered Entity will want the BAA to cooperate if a potential breach occurs and bear the associated liability and costs CE incurs to the extent caused by BAA and its personnel
  - BAA to promptly notify Covered Entity of incidents
  - BAA to cooperate with Covered Entity in investigating and determining whether breach occurred
  - Allocate responsibility for notice to patients and OCR/CMS between BAA and Covered Entity for data breach responsibility
  - Carve costs and liability CE incurs for the breaches out of the limitation on/disclaimer of damages
- Would the Covered Entity Consider Reporting a BAA to the Secretary?
- Consider a No PHI acknowledgment



36

## Scenario 3 Billing/Coding Error



- An audit revealed that the Hospital and its physicians complied with Medicare requirements for 15 of the 100 Evaluation and Management (E&M) services. However, the Hospital incorrectly billed for the remaining 85 services, resulting in overpayments totaling \$8,100.
- According to the audit overpayments occurred because the Hospital had inadequate billing system controls over billing E&M services related to outpatient eye injection procedures, and the Hospital's physicians, who performed the eye injection procedures, did not fully understand the Medicare requirements for separately billable E&M services.

37

**REPORT FRAUD** Home • FAQs • FOIA • Careers • HEAT • Contact Us

U.S. Department of Health & Human Services  
**Office of Inspector General**  
U.S. Department of Health & Human Services

Report #, Topic, Keyword... Search

Advanced

About OIG Reports & Publications Fraud Compliance Recovery Act Oversight Exclusions Newsroom

Home > Reports & Publications > Office of Audit Services > Center For Medicare and Medicaid Services > Report

### Audit (A-01-11-00515)

05-21-2012  
Fletcher Allen Health Care Did Not Always Bill Correctly for Evaluation and Management Services Related to Eye Injection Procedures

**Executive Summary**

Fletcher Allen Health Care (the Hospital), located in Burlington, Vermont, and its physicians complied with Medicare requirements for 15 of the 100 Evaluation and Management (E&M) services that we sampled. However, the Hospital incorrectly billed for the remaining 85 services, resulting in overpayments totaling \$8,100. Based on these sample results, we estimated that the Hospital and its physicians received overpayments totaling \$211,000 for calendar years 2008 through 2010. Overpayments occurred because the Hospital had inadequate billing system controls over billing E&M services related to outpatient eye injection procedures, and the Hospital's physicians, who performed the eye injection procedures, did not fully understand the Medicare requirements for separately billable E&M services.

Complete Report

**I'm looking for**  
Let's start by choosing a topic  
Select One

- All Reports and Publications
- Archives

**EXCLUSIONS DATABASE**

**REPORT FRAUD**

38



## Unbundling

---

- Incorrectly billed for 85 out of 100 services
- The Hospital and its physicians were not eligible for additional E&M payments since services that physician performed were not significant, separately identifiable, and above and beyond usual preoperative work of eye injection procedure.
- Specifically, Hospital stated that its physicians incorrectly believed that care they provided allowed for separately billable E&M services.
- However, care was part of usual preoperative work of eye injection procedure .

39

## E&M Component Not Documented

---

- Providers believed in good faith that care included a separately billable E&M service
- Provider not only assessed and prepared patient for eye injection and provided injection, provider also examined patient's other eye and assessed potential effects of patient's other conditions, such as diabetes and hypertension, on that eye
- On further review of these claims by certified coders, however, Hospital recognizes that documentation in 85 claims did not support a separately billable E&M service because one component of E&M service (medical decision making) was not documented regarding eye not receiving injection



40

## How to Fight a Bogus Bill

*Many Medical Bills Contain Errors That Could End Up Wrecking Your Credit Score. Here's What You Need to Know*

By JESSICA SILVER-GREENBERG

THAT SUSPICIOUS CHARGE on your medical bill might be a mistake—but if you let it fester, it could end up damaging your credit score.

There are no comprehensive statistics on medical-billing mistakes, but Stephen Parente, a professor of health finance at the University of Minnesota who has studied medical billing extensively, estimates that 30% to 40% of bills contain errors. The Access Project, a Boston-based health-care advocacy group, says it's closer to 80%.

41

## Contractual Allocation of the Risk for Liability Arising from Legal and Regulatory Non-Compliance

- Vendor obligation to provide “IT features, functions and service that enables hospital to perform billing and coding function in compliance with applicable law”
  - The problem here did not arise from problems with vendor’s product such as failure to provide key features and functions, defects etc.
  - Vendor will likely rely on disclaimer of responsibility for problems arising from use of the system by hospital and decisions made by hospital in connection with such use.

42



## Scenario 4

### Artificial Intelligence Alert Fatigue

---

- Jenny Blum has been working on 6E for the past three years. This week the new EHR called for her to give the patient 6 mg of a medication that she has always in the past limited to 2 mg. Jenny questioned the dosage and her supervisor agreed that she could call the physician to verify the order. Following the incident the investigation determined that the medication and dose were triggered by a standing order based on the clinical decision support program.
- However, the CDSP triggered an alert to the physician to check the dosage. The alert had been disabled. The physician changed the order when called and acknowledged that he had asked for the alert to be turned off. Further investigation revealed a flaw in the formula that doubled the patient's weight because the program ran twice.

43

### **May 16, 2012 (HHS) released final rule**

---

§ 482.24(c)(3) allows pre-printed & electronic standing orders, order sets, & protocols for patient orders *only* if

- (1) Orders & protocols were reviewed & approved by medical staff in consultation with hospital's nursing & pharmacy leadership;
- (2) Orders & protocols are consistent with nationally recognized & evidence-based guidelines;

44

## **May 16, 2012 (HHS) released final rule**

---

### **§ 482.24(c)(3) allows pre-printed & electronic standing orders, order sets, & protocols for patient orders *only* if**

- (3) Periodic & regular review of such orders & protocols is conducted by medical staff, in consultation with hospital's nursing & pharmacy leadership, to determine continuing usefulness & safety of orders & protocols; &
- (4) Orders & protocols are dated, timed, & authenticated promptly in patient's medical record by ordering practitioner or another practitioner responsible for care of patient as specified under § 482.12(c) & authorized to write orders by hospital policy in accordance with State law.

45

## **Savings from Standing Orders**

---

### **Zinxhealth estimates**



- **provisions would affect 13 million patients (roughly one-third of hospital admissions).**



- **“reduction of 700,000 burden hours valued at \$124 per hour for a savings of \$86,800,000.”**

<http://www.zinxhealth.com/News/Press-Releases/2012/5/CMS-Participation-Rule.aspx>

46

## Malpractice Liability – Evolving Standard of Care

- Today's HIT capabilities provide ready access to more robust and meaningful information to assist in making medical judgments.
  - "If a physician does not utilize new information or is negligent in gathering the results, this could qualify as substandard care and expose the physician to liability." *Jacobsen, P.D., Medical Liability and the Culture of Technology, Project on Medical Liability in PA, 7/2004*
  - Das v. Thani - MD used "1960s-style" maternal fetal monitoring" instead of ultrasound available in his office. Experts testimony went both ways.
- Data Integrity (Accuracy and Completeness) and Availability
  - Input by various participants
  - Aggregation methodologies
  - Consumer access – the Patient Health Record Model

## Risk Allocation

- ONCHIT guide states, "Your practice, not your EHR vendor, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR and comply with HIPAA Rules and CMS' Meaningful Use requirements."
- **Vendor Disclaimer: Clinical Content.** Purchaser understands that the Clinical Content is an information management and diagnostic tool only and that the Clinical Content does not have the ability to diagnose disease, prescribe treatment, or perform any other tasks that constitute the practice of medicine. Clinical Content reflects clinical interpretations and analyses and cannot alone either (a) resolve medical ambiguities of particular situations; or (b) provide the sole basis for definitive decisions. All ultimate care decisions are strictly and solely the obligation and responsibility of the health care provider.
- Customer rather than Vendor control of:
  - Patient request for access
  - Response to subpoenas





## Scenario 5 - HIE Disclosures

---

- In the course of a routine, pre-surgical consultation visit, Mary Moriarity's orthopedic surgeon asked her if she was still taking Zoloft for her depression diagnosis.
- Mary immediately noted that she had never shared any information about her depression with him, had never given permission for any of her other physicians to do so, and demanded to know how he happened to know that information.
- The surgeon proudly reported that he had obtained the information from the regional health information exchange (HIE) in which he participates through the use of his newly implemented EHR that has a patient portal.
- He then presented her with a consent form for that purpose and explained that his practice is to collect all relevant patient information through a regional HIE before an appointment so that he is fully informed for the patient's visit and to request the execution of the consent at the time of the visit.
- Following the visit, she called her psychiatrist to complain about his having made the information available through the HIE.

49

## Scenario 5 - HIE Disclosures

---

- HIE participation agreements typically allocate to the provider participants the full responsibility for obtaining patient consent and taking all other actions necessary to comply with federal and state privacy laws as well as all associated liability.
- Moreover, the IT infrastructure of the HIE participants EHR systems and of the HIE itself is not able to identify and either segregate or delete certain data fields from a record either in the context of an electronic "dump" of EHR information into and HIE repository or when one provider accesses and pulls information from another provider's EHR through a federated model HIE.
- The Behavioral Health confidentiality laws of many states are more restrictive than HIPAA and other state sensitive information confidentiality laws concerning the need for consent, even for the sharing of the information among certain treatment providers for treatment purposes.
- State laws are also unclear and inconsistent concerning whether an "opt-in" approach to consent is required or an "opt out" consent approach is permitted, but the HIE has been built upon the premise that state law in this case permits and "opt-out" consent approach.

50

## Scenario 5 - HIE Disclosures

---

- Should the surgeon have obtained the consent prior to the appointment through the patient portal feature?
- Does the HIE's determination that the state law takes an opt-out approach mitigate the surgeon's potential liability?
- Did the psychiatrist have any responsibility for obtaining the consent?
- Does the importance of having complete information on a patient's medications outweigh the potential privacy risk?
- Should the participation agreement assign to the HIE at least some of the responsibility to provide privacy/confidentiality compliance management features and functions in the HIE infrastructure (either directly or through IT vendor agreements)?
  - E.g., flagging records with regard to consent, identifying sensitive data fields, firewalls, access controls, auditing and monitoring
- Will the provider's insurance cover any damages and costs the surgeon incurs in connection with an OCR or state AG investigation, private action brought by Mary Moriarity? The HIE's insurance, if any?

51

## Scenario 6 – Copy of Medical Record

---

Cynthia Thomas has asked for a copy of her medical record. She has shared a copy with her brother who is a physician. Her brother has contacted the hospital's medical records department to ask for more pages from the electronic record advising that it appears to him that the record is incomplete.

52

## Definition of Legal Health Record

---



- AHIMA's definition
  - LHR is the documentation of the healthcare services provided to an individual in any aspect of healthcare delivery by a healthcare provider organization. The LHR is individually identifiable data, in any medium, collected and directly used in and/or documenting healthcare or health status.
- HIPAA provides patient the right to access Designated Record Set
  - “Designated record set:” That group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems
- Metadata

53

## EHR Vendor Contracting Considerations

---

- Anticipate in the initial vendor contract negotiation the role of the EHR system in meeting the provider's obligations to:
  - maintain the legal medical record
  - provide the patient with access to and a copy of the medical record
  - provide an accounting of disclosures required by HIPAA
  - achieve meaningful use
- A detailed and thorough description of features, functions, and data structure (and corresponding documentation, specifications etc) is key.
- Include provisions that anticipate the gray and evolving legal standards and requirements in these areas
  - E.g., vendor's obligation to update/upgrade the system

54

## EHR Vendor Contracting Considerations

---

- Affirmatively address HIE's use of cloud vendors and other third parties whose products/roles can affect the availability and integrity of the data
  - Location of Data Centers (domestic v. foreign)
  - Security and Privacy infrastructure
  - Service levels consistent with those in prime contract
  - Legal and Regulatory Compliance
    - Privacy
    - Jurisdictional reach (US and Foreign cloud location)
  - Other participants/customers (e.g., competitors, payors, government agencies)
  - Cloud vendor's use of subcontractors

55

American Health Lawyers Association  
In House Counsel Program  
Chicago  
June 24, 2012

---

### Doing Good and Avoiding Evil with Electronic Patient Information Technology



***Bernadette M. Broccolo***  
***McDermott Will & Emery LLP***  
***[bbroccolo@mwe.com](mailto:bbroccolo@mwe.com)***  
***312.984.6911***



***Cynthia F. Wisner***  
***Assistant General Counsel***  
***Trinity Health***  
***[wisnerc@trinity-health.org](mailto:wisnerc@trinity-health.org)***



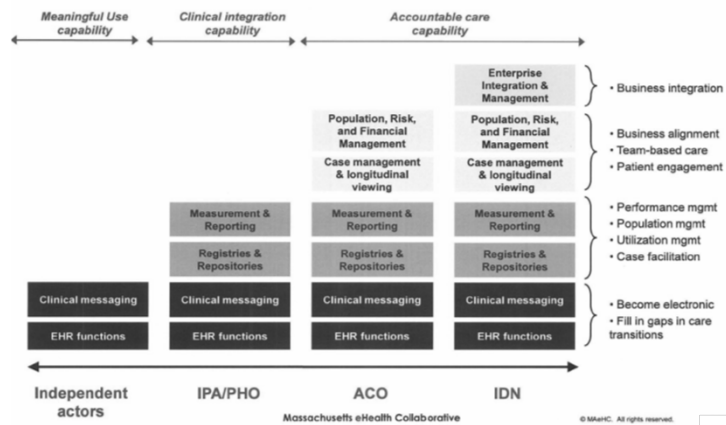
## Doing Good and Avoiding Evil with Electronic Patient Information Technology

### Illustrations

**Bernadette M. Broccolo**  
 McDermott Will & Emery LLP  
[bbroccolo@mwe.com](mailto:bbroccolo@mwe.com)  
 312.984.6911

Illustration 1

## Accountable Care = Data + Analytics



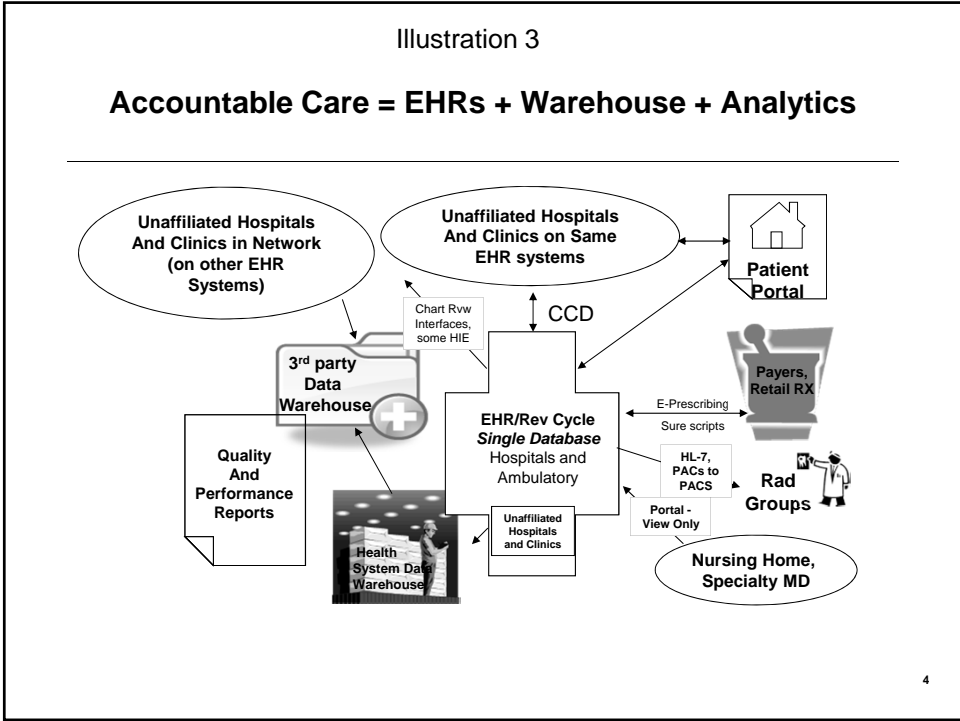
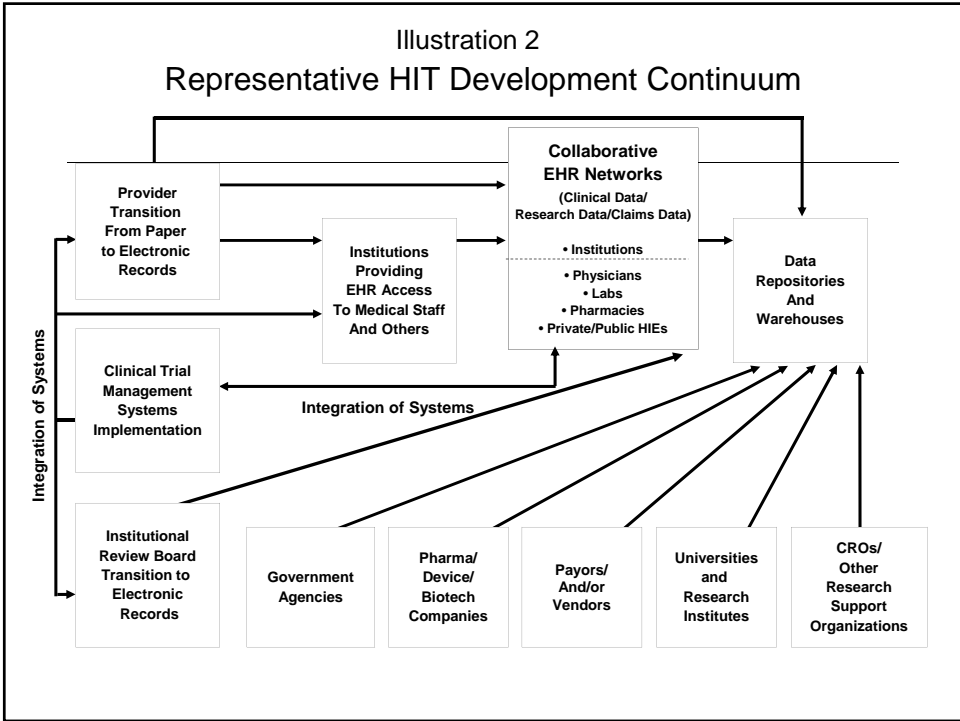
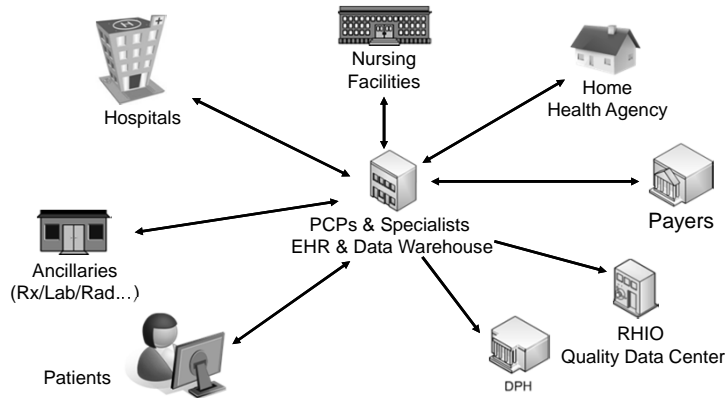


Illustration 3 (cont'd)

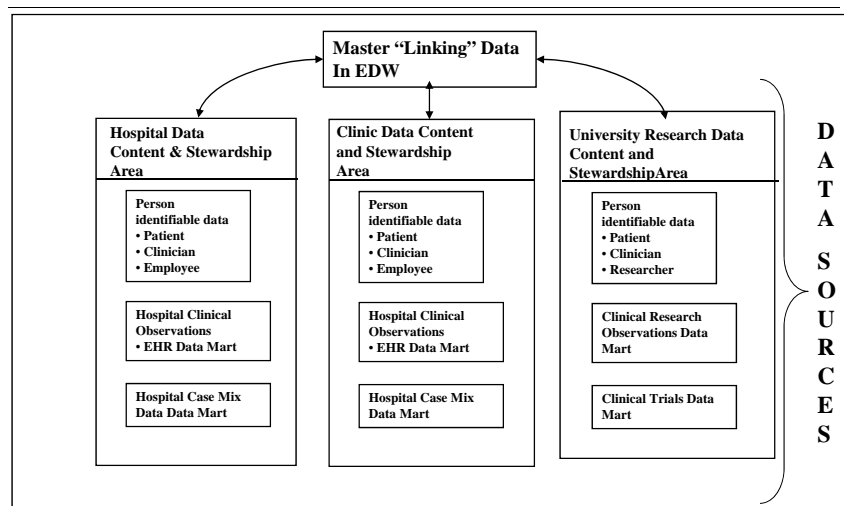
## Interface Approach – Another Alternative



5  
5

Illustration 3 (cont'd)

## Centralized Data Repository/Warehouse Collaboration

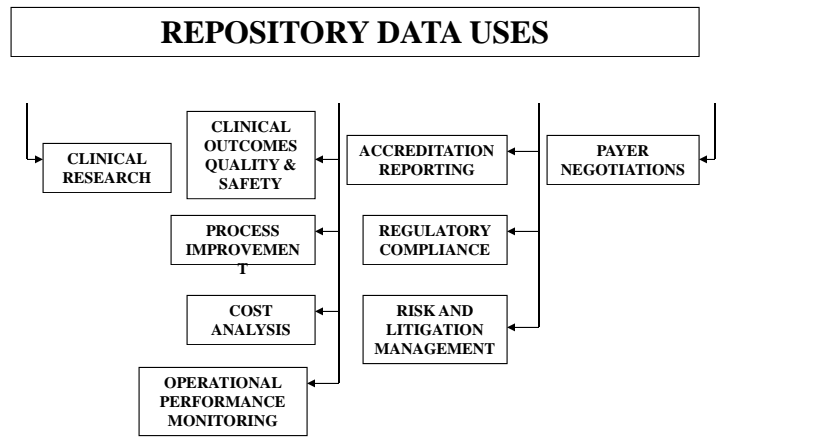


www.mwe.com

6

Illustration 3 (cont'd)

### Centralized Data Repository/Warehouse Collaboration

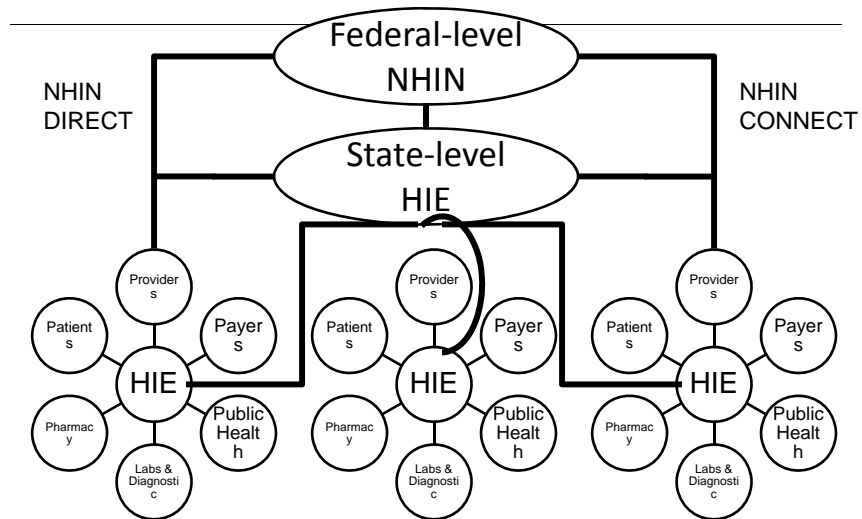


www.mve.com

7

Illustration 4

### Public HIE concept: Federated (multi-layer)



Source: Illinois Health Information Exchange Authority February 2012

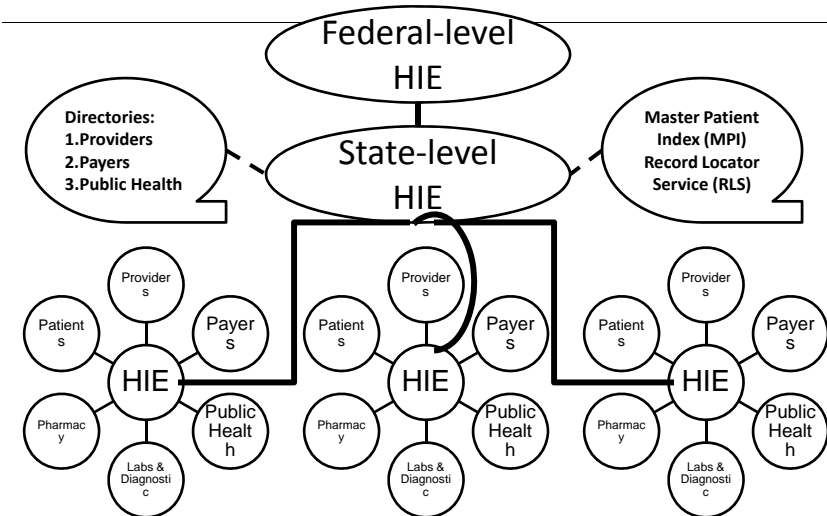
DRAFT

8



Illustration 4 (cont'd)

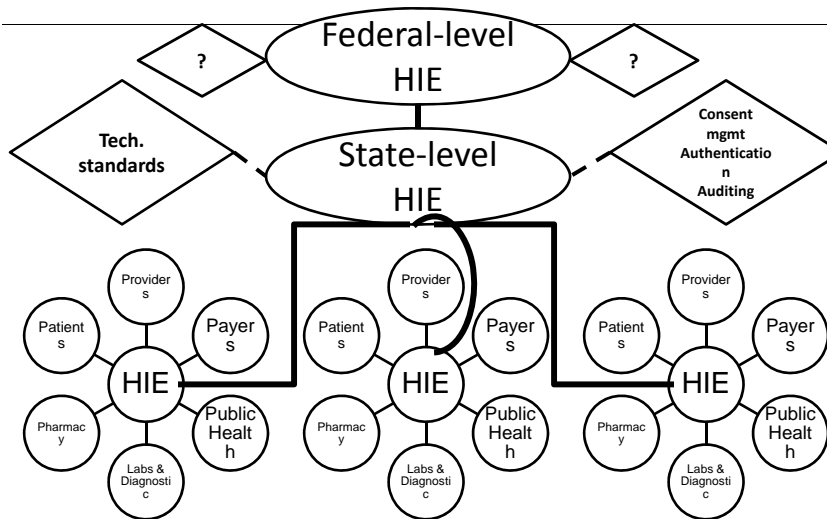
Public HIE concept: Centralized Core Services



Source: Illinois Health Information Exchange Authority February 2012

Illustration 4 (cont'd)

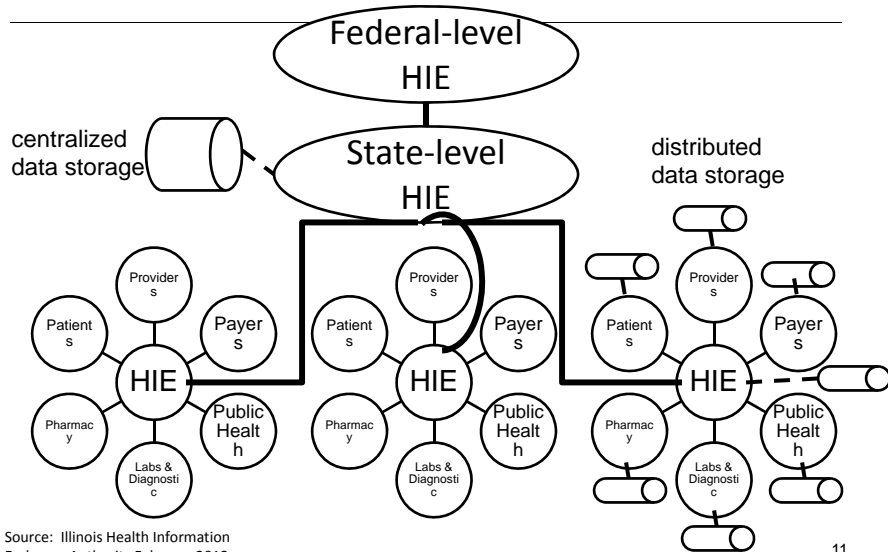
Public HIE concept: Centralized Standards



Source: Illinois Health Information Exchange Authority February 2012

Illustration 4 (cont'd)

Public HIE concept: Clinical Data Storage



Source: Illinois Health Information Exchange Authority February 2012

Illustration 5

Private HIE Scenario

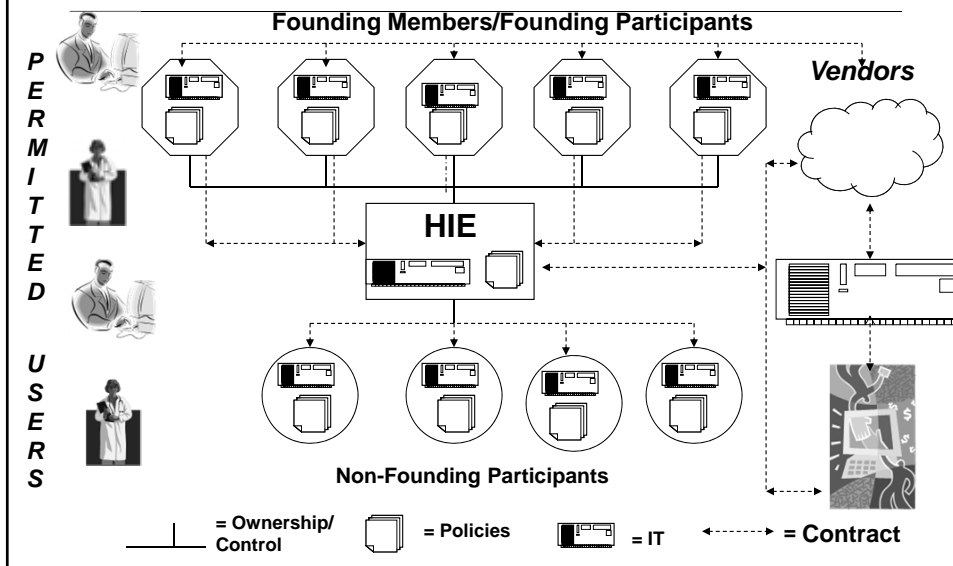
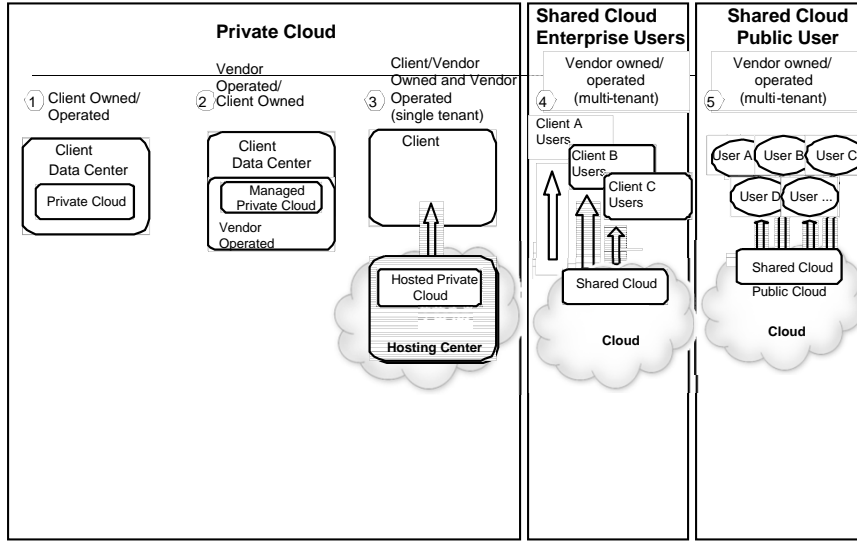


Illustration 6

### Models of Cloud Delivery



Client or Vendor owns infrastructure/dedicated access.  
Fees based on model

Vendor owns infrastructure/Client has shared access/Fees based on usage metrics

**DOING GOOD AND AVOIDING EVIL WITH  
ELECTRONIC PATIENT INFORMATION**

**Bernadette M. Broccolo  
McDermott Will & Emery LLP  
bbroccolo@mwe.com  
312.984.6911**

<b>I.</b>	<b>INTRODUCTION: HIT DEVELOPMENT CONTINUUM.....</b>	<b>1</b>
A.	Interests of the Key Stakeholders .....	1
B.	No one Size Fits All.....	1
C.	Key Design and Development Considerations .....	2
<b>II.</b>	<b>GLOSSARY OF KEY TERMS .....</b>	<b>3</b>
A.	Clinical Information System .....	3
B.	Centralized HIE .....	3
C.	Clinical Data Repository (CDR).....	3
D.	Clinical Decision Support (CDS).....	3
E.	Comparative Effectiveness Research (CER). “A rigorous evaluation of the impact of different options that are available for treating a given medical condition for a particular set of patients.” Focuses on whether an item or service is effective and safe and comparison of similar treatments (competing drugs) or analyzes different approaches (surgery and drug therapy) .....	4
F.	Cloud Computing.....	4
G.	Computerized Provider Order Entry (CPOE).....	4
H.	Data Maps .....	4
I.	Data Repository .....	4
J.	Electronic Health Record.....	4
K.	Electronic Master Patient Index (EMPI) or Master Patient Index (MPI) .....	5
L.	ePrescribing.....	5
M.	Health Information Exchange (HIE).....	5
N.	Health Information Organization (HIO) .....	5
O.	Interface .....	5
P.	Interface Engine .....	6
Q.	Interoperability.....	6
R.	National Health Information Network (NHIN). A network of networks that is a set of harmonized standards-based specifications for the exchange of health information sharing between Nationwide Health Information Exchanges (NHIEs). .....	6
S.	Open Source Systems .....	6
T.	Personal Health Record or PHR .....	6
U.	Provider Matching Software .....	6

V.	Record Locator Service (RLS).....	6
W.	Regional Health Information Organization .....	7
X.	REMS.....	7
Y.	Secondary Use .....	7
Z.	Web Portal .....	7
<b>III.</b>	<b>ELECTRONIC HEALTH RECORDS (EHR).....</b>	<b>7</b>
<b>IV.</b>	<b>HEALTH INFORMATION EXCHANGES .....</b>	<b>7</b>
A.	Background.....	7
B.	Additional Resources .....	8
C.	Representative Example – Illinois Health Information Exchange.....	8
<b>V.</b>	<b>CLOUD COMPUTING.....</b>	<b>10</b>
A.	Five Essential Characteristics .....	10
B.	Three Service Models .....	10
C.	Four Models of Accessibility.....	11
D.	Clinical and Research Applications of Cloud Technology.....	11
E.	Application to Personal Health Records .....	12
F.	Application to HIEs .....	13
<b>VI.</b>	<b>CLINICAL DECISION-SUPPORT (CDS).....</b>	<b>13</b>
A.	Benefits .....	13
B.	Risks and Unintended Consequences .....	13
<b>VII.</b>	<b>KEY LEGAL AND REGULATORY PLANNING CONSIDERATIONS - GENERALLY .....</b>	<b>14</b>
A.	Federal and State Privacy Laws.....	14
B.	State Laws on Medical Records Form, Content and Retention .....	18
C.	Standard of Care for Malpractice Liability.....	19
D.	Federal Laws Regulating the Donation of EHR Technology by Hospitals to Physicians .....	20
E.	Antitrust .....	21
F.	Ownership of Networks/Exchanges, Repositories and their Contents .....	23
<b>VIII.</b>	<b>CONTRACTING STRATEGIES FOR MITIGATING AND MANAGING RISKS.....</b>	<b>23</b>
A.	HIT Vendor Contracts.....	23
B.	Special Considerations in Cloud Computing Agreements.....	27
C.	Special Considerations in Contracting for EHR Network, HIE and Repository Collaborations .....	28
<b>IX.</b>	<b>RESOURCES AND REFERENCES .....</b>	<b>30</b>

## I. INTRODUCTION: HIT DEVELOPMENT CONTINUUM

### A. Interests of the Key Stakeholders

The ability to access robust, reliable electronic health information networks and repositories will be a key element in all industry stakeholders' strategies for responding to the health reform legislation's emphasis on care coordination, quality and outcomes measurement and reporting, comparative effectiveness research and evidence-based medicine. See **ILLUSTRATIONS 1, 2 and 3**.

1. For all providers, networks and repositories will be essential to fulfill health reform's Triple Aim of (1) reducing/controlling the cost and improving the quality of healthcare services, (2) enhancing patient experience, and (3) improving population health.
2. For academic medical centers, universities and research institutes, such networks and repositories will also be essential to qualify for future federal research funding.
3. Pharmaceutical and device manufacturers need them now to support expanded regulatory requirements for mandated post-market surveillance, inclusion in product approval applications submitted to the FDA of a risk evaluation and mitigation strategies ("REMS") for ensuring that the benefits of the drug or biologics outweigh the risks, and to adapt product reimbursement and development strategies to respond to the CER and to the personalized medicine movements.<sup>1</sup>
4. Clinical research support organizations are rapidly realizing how such HIT resources can diversify and enhance the scope and quality of their services.
5. Governmental agencies such as the FDA will need massive electronic data repositories that are built, in part, using Electronic Health Records (EHRs) and Health Information Exchanges (HIEs).

### B. No one Size Fits All

1. The design of the electronic health information technology ("HIT") infrastructure for electronic health information systems, networks and repositories will vary, as will the participants involved in and the pathways followed in the development process.
2. For illustration purposes, **ILLUSTRATION 2** depicts just one possible, hypothetical development continuum, which begins with a single provider's conversion from paper medical records to an EHR system, the provider's collaboration with other providers (directly or through public or private, regional or state-wide health information exchanges) to achieve meaningful use of interoperable EHR systems, its implementation of a clinical trial management system and integration of that system with the EHR system, and ultimately,

---

<sup>1</sup> In particular, Section 905 of the Federal Food, Drug and Cosmetic Act Amendments (FDAAA) requires the FDA to develop methods to obtain access to different data sources (including, public, private and academic entities, many of which are likely to be hospitals, health system and some of which will be HIEs) and validated methods to link and analyze safety data of at least 25 million patients by 2010 and 100 million patients by July 2012. FDAAA § 905(a), adding § 505(k) to the, amending 21 U.S.C. § 355. These methods would then be used to establish procedures for a post-market risk identification and analysis system in the near future.

collaboration between and among the provider and other stakeholders such as universities, payors, manufacturers, research institutes or research support organizations, and

governmental entities for the creation and use of a robust, multi-disciplinary electronic information repository.

### C. Key Design and Development Considerations

Key HIT infrastructure design considerations are likely to include, among others:

1. With which other stakeholders will information be exchanged (e.g., provider-to-provider within a healthcare system or with unaffiliated providers in the community, only between and among employed and affiliated physician practices and physicians or with unaffiliated physicians in the community, between providers and payors, between one health information exchange and another within a community and between an exchange in one community and an exchange in another);
2. What data and technical standards will be needed to support harmonization of different information systems, networks, software applications, interoperability infrastructures and vocabularies;
3. When and how can interoperability be achieved;
4. Will EHR data from various provider participants be aggregated into a single integrated health record;
5. Will EHR data be integrated with electronic clinical trial information of one or more network participants;
6. Will information in an EHR network be aggregated into a non-EHR data warehouse for secondary uses such as healthcare operations and research;
7. Will the network or repository be made available to other than those who contribute information to it; and
8. Will the infrastructure depend in whole or in part on the support of third parties (e.g., the services and infrastructure of application service providers (“ASPs”)) offering a complete turnkey arrangement or just certain infrastructure such as “cloud computing”<sup>2</sup> or other server capability that will facilitate the exchange of information

---

<sup>2</sup> [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing) (last visited June 27, 2010). See also, Roger Cheng, 'Cloud Computing': *What Exactly Is It, Anyway?*, Wall St. J., Feb. 8, 2010, <http://online.wsj.com/article/SB10001424052748703961104575226194192477512.html?KEYWORDS=cloud+computing>; Walter S. Mossberg, *Learning About Everything Under the Cloud*, Wall St. J., May 6, 2010, <http://online.wsj.com/article/SB10001424052748703580904574638391318085158.html?KEYWORDS=cloud+computing>.

without the need for myriad source-to source interfaces) be needed on a short-term or long-term basis.<sup>3</sup>

It is also critical to take into account existing clinical processes and workflow and to synchronize the electronic strategy with them or to change them as necessary in connection with the development and implementation of the strategy.<sup>4</sup>

## II. GLOSSARY OF KEY TERMS

Following is a selective glossary of key terms in today's HIT terminology focused on the development and implementation of today's HIT infrastructure needs and strategies.

- A. Clinical Information System.** An information system that collects, stores, and transmits information that is used to support clinical care (e.g., transmission of laboratory test results, radiology results, prescription drug orders).<sup>5</sup>
- B. Centralized HIE.** An approach to data sharing and the interchange of electronic information emphasizing full control over data sharing through a centralized data repository (CDR). The components in this architecture refer to the CDR and the requestor. The CDR authenticates the requestor through technological means, authorizes the transaction, and records it for audit and reporting purposes.<sup>6</sup>
- C. Clinical Data Repository (CDR).** A real-time database that consolidates data from a variety of clinical sources to present a unified view of a single patient. It is optimized to allow clinicians to retrieve data for a single patient rather than to identify a population of patients with common characteristics or to facilitate the management of a specific clinical department. Typical data types often included are: clinical laboratory test results, patient demographics, pharmacy information, radiology reports and images, pathology reports, hospital admission, discharge and transfer dates, IDC-9/ICD-10 codes, discharge summaries, and progress notes.<sup>7</sup>
- D. Clinical Decision Support (CDS).** Computer-based system offerings "passive and active referential information as well as reminders, alerts, and guidelines."<sup>8</sup> CDS plays a key role in CPOE and CER.<sup>9</sup>

---

<sup>3</sup> A discussion of financial, technological, strategic and operational considerations involved in the design and development of an HIE or robust electronic data repository are outside the scope of this outline. A useful resource for additional information concerning HIEs in particular is the eHealth Initiative website at [www.ehealthinitiative.org](http://www.ehealthinitiative.org).

<sup>4</sup> See Sittig, Dean F and Joan S. Ash, *Clinical Information Systems Overcoming Adverse Consequences*, Jones and Bartlett (2011) for a thorough discussion of potential adverse consequences in Clinical Information Systems, which, in part, emphasizes the risks of failing to synchronize clinical processes and workflow with the electronic information technology infrastructure, processes and workflow.

<sup>5</sup> HIMSS Quality 101 Definitions/Glossary of Terms, [http://www.himss.org/content/files/quality101\\_glossary.pdf](http://www.himss.org/content/files/quality101_glossary.pdf)

<sup>6</sup> HIMSS Health Information Exchange (HIE) Glossary, <http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>

<sup>7</sup> *Id.*

<sup>8</sup> Bates DW, Kuperman GJ, Wang S., et al. Ten commandments for effective clinical decisions support: making the practice of evidence-based medicine a reality. *J Am Med Inform Assoc.* 2003; 10(6): 523-530

<sup>9</sup> For a thorough discussion of the risks and benefits of Clinical Decision Support, see Sittig, Dean F and Ash, Joan S., *Clinical Information Systems Overcoming Adverse Consequences*, Jones and Bartlett (2011).



- E. Comparative Effectiveness Research (CER).** “A rigorous evaluation of the impact of different options that are available for treating a given medical condition for a particular set of patients.”<sup>10</sup> Focuses on whether an item or service is effective and safe and comparison of similar treatments (competing drugs) or analyzes different approaches (surgery and drug therapy). The analysis may focus only on the relative medical benefits and risk of each option or it may weigh both the costs and benefits of those options.
- F. Cloud Computing.** Allows users to perform various computing tasks using remotely located infrastructure.<sup>11</sup> “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”<sup>12</sup> Through a centralized infrastructure, users are able to circumvent the limitations of their individual devices, such as processing power and storage space. There are three distinct cloud computing service models: (i) Software as a Service (“SaaS”); (ii) Platform as a Service (“PaaS”); and (iii) Infrastructure as a Service (“IaaS”).<sup>13</sup> See further discussion below.
- G. Computerized Provider Order Entry (CPOE).** A computer application that allows a provider’s orders for diagnostic and treatment services (such as medications, laboratory, and other tests) to be entered electronically instead of being recorded on order sheets or prescription pads. The computer compares the order against standards for dosing, checks for allergies or interactions with other medications, and warns the physician about potential problems.<sup>14</sup> **Insert cite to the book I got that discusses CPOE and its advantages and disadvantages in detail.**
- H. Data Maps.** Any and all information that is necessary to HIE’s ability to translate nomenclature and field-level categorical values into a format that allows (i) HIE Users to understand and use the Patient Data, User List and Submissions provided by Participant or Participant’s Users; (ii) proper delivery of electronic orders, results and reports to a Participant; and (iii) matching of patients and providers.
- I. Data Repository.** An independent platform that stores sanitized data retrieved from legacy, transaction-oriented systems for display and use in formats conducive to a specific purpose (research, outcomes analysis, etc.)<sup>15</sup>
- J. Electronic Health Record.** An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff *across more than one health care organization*.<sup>16</sup>

---

<sup>10</sup> Congressional Budget Office Report, “Research on the Comparative Effectiveness of Medical Treatments,” December 2007.

<sup>11</sup> U.S. National Institute of Standards and Technology (NIST), <http://www.law.harvard.edu/students/orgs/nsrc/Cloud.pdf>.

<sup>12</sup> <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>.

<sup>13</sup> HIMSS Health Information Exchange (HIE) Glossary, <http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> Department of Health & Human Services Office of National Coordinator for Health Information Technology and Alliance for Health Information Technology Glossary, [http://healthit.hhs.gov/defining\\_key\\_hit\\_terms](http://healthit.hhs.gov/defining_key_hit_terms)

1. **Shared EHR.** A model of health information exchange that exists when all participating organizations deploy the same EHR technology which operates from a common database structure. No exchange platform is necessary in this model as each participant is working in the same patient centric record.<sup>17</sup>

**K. Electronic Master Patient Index (EMPI) or Master Patient Index (MPI).** A database that contains a unique identifier for every patient in the enterprise; organizes patient IDs from external systems, allowing cross-referencing of patient records and access to them using their medical record numbers from external or legacy systems.<sup>18</sup>

**L. ePrescribing.** A prescriber's ability to electronically send an accurate, error-free and understandable prescription directly to a pharmacy from the point-of-care.<sup>19</sup>

**M. Health Information Exchange (HIE).** The reliable and interoperable electronic movement of health-related information among organizations according to nationally recognized and in a manner that protects the confidentiality, privacy and security of the information. A "health information exchange" is defined as the mobilization of health care information electronically across organizations within a region, community or hospital system.<sup>20</sup>

1. **Private HIE.** An HIE deployed by an organization other than a RHIO and uses that organization's existing IT systems or newly built IT HIE infrastructure and systems. This is generally a closed-system model that connects multiple select facilities within an owned or affiliated organization.<sup>21</sup>

2. **Federated HIE.** A decentralized approach to the coordinated sharing and interchange of electronic information emphasizing partial, controlled sharing among autonomous databases.<sup>22</sup>

3. **State HIE or RHIO.** An HIE or RHIO that is governed and operated at the state level. The federal stimulus package extended \$548 million to states to deploy HIEs across the country by state governed initiatives.<sup>23</sup>

**N. Health Information Organization (HIO).** An organization that oversees and governs an HIE.<sup>24</sup>

**O. Interface.** A boundary across which two independent systems meet and act or communicate with each other in order to translate information provided by one information system into a format that

---

<sup>17</sup> Designing the Health IT Backbone for ACOs," PricewaterhouseCoopers Health Research Institute, <http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>

<sup>18</sup> HIMSS Health Information Exchange (HIE) Glossary, <http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>

<sup>19</sup> <http://www.cms.gov/Medicare/E-Health/Eprescribing/index.html?redirect+/eprescribing>

<sup>20</sup> www.ssa.gov. See also, "Designing the Health IT Backbone for ACOs," PricewaterhouseCoopers Health Research Institute, <http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>

<sup>21</sup> Designing the Health IT Backbone for ACOs," PricewaterhouseCoopers Health Research Institute, <http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>

<sup>22</sup> *Id.*

<sup>23</sup> Designing the Health IT Backbone for ACOs," PricewaterhouseCoopers Health Research Institute, <http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>

<sup>24</sup> Glossary of Acronyms and Terms Commonly Used in Informatics, [www.amia.org/glossary](http://www.amia.org/glossary)

can be sent to or accessed through another information system either directly between the two systems or through an exchange mechanism.<sup>25</sup>

- P. Interface Engine.** Software that enables many disparate systems to pass information back and forth using a set of defined standards and typically perform functions such as store and forward of messages, message translation, message routing, management tools, and alerts and monitoring.<sup>26</sup>
- Q. Interoperability.** The ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of healthcare for individuals and communities.<sup>27</sup>
- R. National Health Information Network (NHIN).** A network of networks that is a set of harmonized standards-based specifications for the exchange of health information sharing between Nationwide Health Information Exchanges (NHIEs).<sup>28</sup>
- S. Open Source Systems.** Software distributed in source in licenses guaranteeing anybody rights to freely use, modify, and redistribute the code.<sup>29</sup>
- T. Personal Health Record or PHR.** The Health Information Technology for Economic and Clinical Health (“HITECH”) Act defines the term as “an electronic record of [personally] identifiable health information . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily by the individual.”<sup>30</sup> Alternatively, the Centers for Medicare & Medicaid Services (“CMS”) recently described PHRs as “confidential, easy-to-use electronic tools that can help you manage your health information.”<sup>31</sup> Ideally, PHRs “provide a complete and accurate summary of the health and medical history of an individual by gathering data from many sources, including [electronic medical records] and [electronic health records],” and allow such information to be accessible by those with the necessary electronic credentials.<sup>32</sup>
- U. Provider Matching Software.** Type of middleware that matches providers across independent systems.
- V. Record Locator Service (RLS).** A file of locations of patient records, able to be queried only by authorized participants, that determines what records exist for a patient and where they are located. An RLS manages participating provider identities, maintain and publish a patient index, match patients using an algorithm, look up patient record locations (but not the records themselves), communicate securely and maintain an audit log, and manage patient consent to record sharing).

---

<sup>25</sup> HIMSS Health Information Exchange (HIE) Glossary, <http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009. Pub. L. No. 111-5 (Feb. 17, 2009); see HITECH Act, Title XIII of Division A, Subtitle D § 13400(11).

<sup>31</sup> <http://www.medicare.gov/Publications/Pubs/pdf/11397.pdf>.

<sup>32</sup> Glossary of Acronyms and Terms Commonly Used in Informatics, [www.amia.org/glossary](http://www.amia.org/glossary)

- W. Regional Health Information Organization.** A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community. RHIOs are governed at local or regional levels.<sup>33</sup>
- X. REMS.** The risk evaluation and mitigation strategies required by the Federal Food, Drug and Cosmetic Act Amendments (FDAAA).<sup>34</sup>
- Y. Secondary Use.** A term generally used to refer to uses of clinical data for purposes other than direct patient care (e.g., for research purposes, for public health surveillance, for billing, for analysis in disease registries).<sup>35</sup>
- Z. Web Portal.** Middleware that allows a user to log into an information system, through the web, working from any location.<sup>36</sup>

### III. ELECTRONIC HEALTH RECORDS (EHR)

The drive to improve the efficiency and effectiveness of the health care system has resulted in the creation of the electronic medical environment, with health care providers accessing computer systems to record the most relevant and timely facts about a patient's health during an office visit.

*See* Cynthia Wisner materials from this session for a more in-depth coverage of EHRs and associated risks and regulatory issues, including meaningful use.

### IV. HEALTH INFORMATION EXCHANGES

#### A. Background

1. The Health Information Technology for Economic and Clinical Health (“HITECH”) Act allocated \$300 million to support regional or sub-national efforts toward establishing and maintaining HIEs, whether government-initiated or privately-initiated. The HITECH Act specifically outlines how the federal stimulus money will be used to advance the design, development and operation of a nationwide HIE infrastructure that promotes the electronic use and exchange of information.
2. HIEs are intended to enable hospitals, physicians and clinicians to improve the quality and efficiency of patient care through the electronic sharing of patient records.<sup>37</sup>
3. HIEs are typically comprised of multi-stakeholder organizations responsible for motivating and causing integration and secure exchange of patient information for treatment purposes. The geographic footprint of existing HIEs range from a local community to a larger multi-

---

<sup>33</sup> Glossary of Acronyms and Terms Commonly Used in Informatics, [www.amia.org/glossary](http://www.amia.org/glossary). *See also*, Designing the Health IT Backbone for ACOs,” PricewaterhouseCoopers Health Research Institute, <http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>

<sup>33</sup> FDAAA § 905(a), adding § 505(k) to the, amending 21 U.S.C. § 355.

<sup>34</sup> *Id.*

<sup>35</sup> Glossary of Acronyms and Terms Commonly Used in Informatics, [www.amia.org/glossary](http://www.amia.org/glossary)

<sup>36</sup> HIMSS Health Information Exchange (HIE) Glossary, <http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>

<sup>37</sup> <http://healthinformationexchanges.org/health-information-exchange-growth-doubles/#more-2425>.

state region. Interoperability among these various systems is essential in moving toward the ultimate goal of a national health information network.

4. The number of live HIEs more than doubled to 228 between the beginning of 2010 and mid-2011, with many systems incorporating cloud-based technologies (discussed further below).<sup>38</sup>
5. HIEs can be both public/government controlled/initiated and privately controlled/initiated. See **ILLUSTRATION 4** and **ILLUSTRATION 5**.

## **B. Additional Resources**

The following are additional resources on HIE initiatives across the country:

1. 2011 Report on Health Information Exchange: Sustainable HIE in a Changing Landscape (eHealth Initiative), available for a fee at [http://www.ehealthinitiative.org/store.html?page=shop.product\\_details&flypage=flypage.tpl&product\\_id=83&category\\_id=8](http://www.ehealthinitiative.org/store.html?page=shop.product_details&flypage=flypage.tpl&product_id=83&category_id=8)
2. ONC State Health Information Exchange Program Resources, <http://statehieresources.org/topics-2/>

## **C. Representative Example – Illinois Health Information Exchange**

1. The Illinois state-wide HIE, would serve as an HIE of HIEs in Illinois and in turn would be linked at the national level to state-level HIEs in other States. Consistent with its statutory mandate and its Federal funding commitments, it intends to offer connectivity to all providers in the State, much as the Federal NHIN offers connectivity to all providers nationally. Currently, the Illinois HIE is a “Federated HIE” model – that is, it does not intend to initially store clinical data.
2. The vision of the Illinois HIE is to offer a connection and sharing of health information across interoperable HIT systems among the following:
  - a. Patients: Illinois has nearly 13 million residents
  - b. Providers: More than 50,000 physicians and 170,000 nurses serve Illinois patients in numerous care settings including, nearly 200 acute care hospitals and health systems, 50 of which are critical access hospitals, 400 community health center sites, 100 ambulatory surgical treatment centers, and 1,100 long term care facilities.
  - c. Payors: 7.4 million Illinois residents have commercial insurance coverage, 2.5 million by Medicaid and Medical Assistance programs, 1.9 million by Medicare. The payers of medical claims include the State as the administrator of Medicaid and healthcare offered by the State of Illinois, receiving electronically over 82 million claims annually,.

---

<sup>38</sup> <http://www.ihealthbeat.org/articles/2011/7/11/report-number-of-health-data-exchanges-doubled-since-2010.aspx>; <http://www.informationweek.com/news/healthcare/interoperability/231001868>. Live public HIEs increased from 37 in early-2010 to 67 in mid-2011, and private HIEs grew from 52 to 161 during the same period.

- d. Public Health: the Illinois Department of Public Health needs health data to administer over 200 health and safety programs, as do 95 local public health authorities
  - e. Laboratories and Diagnostic Services providers: 9,225 CLIA-certified laboratories process millions of tests annually in Illinois;
  - f. Pharmacies: Nearly 90% of the 3,193 pharmacies in Illinois IL electronically routed approximately 8.4 million prescriptions in 2009, and was projected to rise to 16.8 million by the end of 2010.
3. Conceptually, the responsibilities and functions of the Illinois state-level HIE would encompass the following:
- a. provide certain centralized core service which would enable and facilitate the exchange of patient health records between participating local HIEs (including directories containing routing address details for sending of data to providers, payers and public health authorities);
  - b. establish and maintain a master patient index (MPI) and an index of all locations in which a patient's records may be stored (a record locator service) to enable the location and retrieval of patient health records distributed among multiple healthcare providers;
  - c. establish and maintain certain centralized standards to facilitate the exchange of data between systems supplied by multiple vendors;.
  - d. would access and utilize both data whose storage is distributed among healthcare providers, as well as data stored at a centralized state level.
4. The Act identifies the following as the duties that the Authority may decide to perform:
- a. Conduct rulemaking proceedings in accordance with the Illinois Administrative Procedure Act,
  - b. adopt standards for HIT systems and products used by State agencies,
  - c. obtain patient-specific data from State agencies,
  - d. appoint or designate an institutional review board to approve requests for research
  - e. protecting patient privacy and security
  - f. suspend, limit or terminate right to participate in the HIE, and
  - g. seek all remedies allowed by law.
5. See **ILLUSTRATION 4**.

## V. CLOUD COMPUTING<sup>39</sup>

### A. Five Essential Characteristics

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet. Regardless of service or deployment model, there are five essential characteristics of cloud computing:<sup>40</sup>

1. on-demand self-service offerings that enable users to access cloud-based services at their convenience, without having to interact directly with the service provider;
2. broad network access, effectively allowing users to access cloud-based services from any internet-enabled device;
3. availability of pooled resources so that multiple consumers can be served, “with different physical and virtual resources dynamically assigned and reassigned according to consumer demand;”<sup>41</sup>
4. flexibility with respect to system capabilities, which may be “rapidly and elastically provisioned to quickly scale out, and rapidly released to scale in;”<sup>42</sup> and
5. control and optimization of resources by “leveraging a *metering capability* at some level of abstraction appropriate to the type of service.”<sup>43</sup>

### B. Three Service Models

While some overlap exists among the three principal cloud computing service models, each model possesses distinguishing characteristics relating to the services offered and varying levels of control of the parties over the technology involved.

#### 1. Software as a Service (SaaS)

SaaS currently occupies, and is expected to continue to occupy – a majority of the global public cloud market.<sup>44</sup> With the SaaS model, consumers access the cloud provider’s software applications from various client devices through a thin client interface such as a web browser.<sup>45</sup> While the computing, processing and storage capabilities of the application are perceived by consumers to exist “in the cloud,” these processes actually take place in the cloud provider’s data center. The user does not manage or control the underlying cloud infrastructure.<sup>46</sup> Examples include Google’s Gmail and Google Docs.

---

<sup>39</sup> The author acknowledges the contributions of Jean Pechette, her partner at McDermott Will & Emery LLP, for her contributions to this section.

<sup>40</sup> <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>

<sup>41</sup> Id.

<sup>42</sup> Id.

<sup>43</sup> Id.

<sup>44</sup> <http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702>.

<sup>45</sup> <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>

<sup>46</sup> Id.

## 2. Platform as a Service (PaaS)

The PaaS model allows consumers to use the cloud network to create, deliver and deploy software applications on the cloud infrastructure. As with the SaaS model, PaaS users do not control the underlying cloud infrastructure. However, in contrast with the SaaS model, PaaS users maintain a significant level of control over the applications that are deployed into the cloud.

While SaaS applications are routinely used by even the most novice consumers, PaaS services generally appeal to individuals with technical expertise. The PaaS consumer-base is likely to include application developers, administrators, testers and deployers.<sup>47</sup> Once a PaaS consumer deploys an application into the cloud, that application will be perceived by end-users – and rightly so – as a SaaS application. Thus, PaaS services can function as a step in the process of developing and deploying SaaS applications. Examples include Google Apps, Force.com.

## 3. Infrastructure as a Service (IaaS)

The IaaS model provides consumers with access to additional computing resources, such as processing, storage and other fundamental computing resources on an as-needed basis.<sup>48</sup> In simplest terms, IaaS services function as an alternative to purchasing new hardware. The consumer does not have control over the underlying cloud infrastructure, but maintains control over operating systems, deployed applications, storage and some network features, such as firewalls. Examples include Rackspace, IBM, Amazon Web Services.

### C. Four Models of Accessibility

Generally, there are four deployment models: (i) Private Clouds; (ii) Community Clouds; (iii) Public Clouds; and (iv) Hybrid Clouds. In large part, the appropriate deployment model depends on the relationship between the service provider and the end-user and among the end-users. The deployment model selected affects which users may access the cloud, who manages the cloud and where the cloud is located.<sup>49</sup> See **ILLUSTRATION 6**.

### D. Clinical and Research Applications of Cloud Technology

#### 1. Clinical Support

Cloud computing is also being used to assist with clinical decision support. For example, it is being used to facilitate consultation concerning radiation oncology images among independent medical practitioners specialized in a variety of different aspects of breast cancer treatment.<sup>50</sup> Clinicians working in the cloud can perform radiation treatment planning by contouring of images generated by various programs.<sup>51</sup> “Processors in the cloud system convert the augmented pictures into a format that can be read by a linear accelerator, which

---

<sup>47</sup> Id.

<sup>48</sup> Id.

<sup>49</sup> Id.

<sup>50</sup> [http://www.cmio.net/index.php?option=com\\_articles&article=25427](http://www.cmio.net/index.php?option=com_articles&article=25427).

<sup>51</sup> Id.



tells the irradiation device where and how much radiation to deliver to a patient.”<sup>52</sup> A woman at one location can receive a mammogram, and those images and physician annotations are made available to the other locations via the cloud.<sup>53</sup> Timely access to results correlates with the timeliness of informed treatment, thereby improving the quality of patient care.<sup>54</sup>

## 2. Research

Cloud-based applications are being developed to assist clinicians and researchers with computation-intensive projects.<sup>55</sup> For example, researchers at the Johns Hopkins Bloomberg School of Public Health “use an internally developed open-source cloud computing pipeline called Myrna for calculating gene expression in large RNA-sequencing datasets.”<sup>56</sup> Without the cloud, an analysis “for a single RNA sequence on one laptop could take up to three weeks to complete on a local computer network”<sup>57</sup> compared to the two hours needed when using the computational capabilities of the cloud.<sup>58</sup>

## E. Application to Personal Health Records

1. Cloud technology is also used to deploy PHRs by allowing patients and providers to access and update information across multiple locations. An early example, Microsoft HealthVault,<sup>59</sup> maintained personal accounts on the cloud that allowed users to access their records via the internet.<sup>60</sup> Consumers are purportedly in control of their personal health information, with functionality to manage access rights among various users, including health care providers.<sup>61</sup> Consumers can input their own data, or health information can be imported from connected doctors, hospitals and retail pharmacies.<sup>62</sup> HealthVault accounts are accessible from mobile devices and, when accessed from mobile platforms, users automatically see their information in a layout specifically-designed for quick access during a health encounter.<sup>63</sup> Other vendors have since entered the market with comparable offerings of PHRs and internet-enabled kiosks with capabilities to collect and monitor health data and track health statistics. Such consumer-facing PHRs allow patients to collect comprehensive data from multiple organizations,<sup>64</sup> and because the data is managed exclusively by the patient, it can be utilized

---

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> [http://www.cmio.net/index.php?option=com\\_articles&article=25427](http://www.cmio.net/index.php?option=com_articles&article=25427).

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*

<sup>59</sup> <http://www.microsoft.com/en-us/healthvault/organize/medical-records.aspx>. Google previously launched a similar product, Google Health. However, perhaps indicative of the challenges inherent in convincing consumers that the cloud is safe for storing sensitive health information, Google Health was closed to new customers effective January 1, 2012 and will be retired at the end of the year. Responding to this development, Microsoft has released functionality to allow Google Health users to transfer their health information to Microsoft HealthVault.

[http://www.microsoft.com/en-us/healthvault/google-health.aspx?WT.mc\\_id=M11071401&WT.ad=Text::GoogleConvert::GoogHealthLifeboat::HvGH::1401](http://www.microsoft.com/en-us/healthvault/google-health.aspx?WT.mc_id=M11071401&WT.ad=Text::GoogleConvert::GoogHealthLifeboat::HvGH::1401).

<sup>60</sup> <http://www.microsoft.com/en-us/healthvault/>.

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> <http://blogs.msdn.com/b/familyhealthguy/archive/2011/05/31/healthvault-breaks-free-from-the-desktop.aspx>.

<sup>64</sup> <http://www.google.com/intl/en-US/health/about/>.

by any health care organization where the patient receives treatment – provided the health care provider is granted appropriate access.<sup>65</sup>

2. PHRs may also be health care organization-specific (rather than consumer-facing) and offer unique features that seek to increase patient involvement in the management of care. These services can also exist in the cloud and be accessed via the internet, but they do not offer patients the ability to incorporate outside health encounter information.<sup>66</sup> For example, Kaiser Permanente's PHR product, My Health Manager, allows patients to access their medical records and test results over the internet,<sup>67</sup> email their doctors, refill prescriptions and schedule, review or cancel appointments online.<sup>68</sup> Beginning in 2009, over three millions Kaiser members were able to access the service, and during the same year, 6,854,722 prescriptions were refilled, 1,852,178 appointments were requested and over 8.5 million emails were sent using My Health Manager.<sup>69</sup> A recent Kaiser study observed 35,423 patients with diabetes, hypertension, or both.<sup>70</sup> In any two-month period, patient use of secured patient-physician messaging through Kaiser's My Health Manager was associated with statistically significant improvements in various health care effectiveness measurements.<sup>71</sup>

#### **F. Application to HIEs**

Cloud-based HIEs enable users spread over increasingly broad geographic areas to access patient information.

### **VI. CLINICAL DECISION-SUPPORT (CDS)**

#### **A. Benefits**

Clinical Decision-Support Systems, working together with CPOE, can decrease medical errors and improve hospital efficiency and practitioner performance.

#### **B. Risks and Unintended Consequences**

Related risks and unintended consequences can occur and are commonly attributable to either the content of the decision support module itself, or the presentation of the information on the computer screen.<sup>72</sup> Critics warn against considering CDS a substitute for the exercise of thoughtful, independent clinical judgment as opposed to a source of information that can be factored into the exercise of clinical judgment.

---

<sup>65</sup> [http://www.google.com/intl/en\\_us/health/privacy.html](http://www.google.com/intl/en_us/health/privacy.html).

<sup>66</sup> <http://healthplans.kaiserpermanente.org/federalemployees/why-kp/complete-health/mhm/>.

<sup>67</sup> Id.

<sup>68</sup> Id.

<sup>69</sup> Kaiser Permanente HealthConnect® Electronic Health Record – Frequently Asked Questions, <http://xnet.kp.org/newscenter/aboutkp/healthconnect/faqs.html>.

<sup>70</sup> *Use of Health Information Technology Leads to Improved Care Quality*, News Center – Press Releases: National (July 7, 2010), <http://xnet.kp.org/newscenter/pressreleases/nat/2010/070710ehrupquality.html>.

<sup>71</sup> Id.

<sup>72</sup> For a comprehensive discussion of these and related considerations, see Sittig, Dean F and Ash, Joan S., *Clinical Information Systems Overcoming Adverse Consequences*, Jones and Bartlett (2011), pp. 105-114.

1. Content-related risks and unintended consequences are commonly attributable to the currency of the CDS content, wrong or misleading content, and the elimination or changing roles of clinicians and staff.
  - a. The currency of content can be influenced by outside sources such as mandates by CMS and the Joint Commission or the availability of new clinical knowledge (e.g., the monumental changes involved in the transition from ICD-9 codes to ICD-10 codes).
  - b. Contexts in which wrong or misleading content occurs is inappropriate/inconsequential alerts, contradictory advice offered by alerts (e.g., the system both suggests something be ordered issues an alert against placing such an order), and medication reconciliation (e.g., list of medications dispensed to a patient over time v. list of all medications patient is actually taking at the time when care is being provided).
  - c. Other sources of potential error include auto-complete features, and alerts that arrive late and either lead to delayed action or no action at all.
2. Presentation of information issues can be caused by the rigidity of systems, sources of alert fatigue and source of potential error. Rigidity problems arise from the conflict between the need to gather and use structured data in the CDS and the need for clinicians to work easily and quickly and from linear order sets that fail to reflect the complex reality of clinical ordering. Alert fatigue occurs most from clinicians feeling there are too many alerts (e.g., drug-drug interactions, weight-based dosing, other drug alerts) and can lead to hasty deletions of relevant information (i.e., clicking OK or deleting an alert without even reading the message on the screen)..

## **VII. KEY LEGAL AND REGULATORY PLANNING CONSIDERATIONS - GENERALLY**

An EHR, HIE and robust health data repository each can be a powerful resource for achieving reform in healthcare delivery, payment and research, and a valuable asset in its own right, if critical legal and regulatory compliance requirements are addressed early in the planning and development process. Conversely, a lack of careful upfront compliance planning can result in an HIT infrastructure that cannot be used without serious compliance risk and a corresponding loss of the substantial time, effort and financial resources devoted to the infrastructure development effort.

Following is a brief overview of key legal and regulatory planning considerations that should be addressed at the outset of any network or repository/warehouse initiative.

### **A. Federal and State Privacy Laws**

Various domestic and international laws governing the privacy and security of personal health information will apply to the exchange of information between and among participants in an electronic health information network or data repository collaboration of any size and scope. Any strategy for addressing these laws should address the extent to which compliance steps are required both for the initial inclusion of data in a repository and for each subsequent use of the data and for each exchange of information across an electronic network.<sup>73</sup>

---

<sup>73</sup> For example, HIPAA and the Common Rule will treat as two separate research studies needed appropriate authorization or informed consent (or corresponding exceptions to or waivers from the authorization and informed

(continued...)

## 1. HIPAA Privacy and Security

- a. Both the HITECH Act and the Patient Protection and Affordable Care Act (“ACA”) incentivize investment in HIT infrastructure that will support widespread electronic exchange and analysis of healthcare information. Recognizing that this health reform policy also elevates the privacy and security risks regulated by the Health Insurance Portability and Accountability Act of 1993 and accompanying regulations<sup>74</sup> (“HIPAA”), however, the HITECH Act strengthened existing HIPAA privacy and security requirements in several significant respects.
  - (i) In particular, the Act extended the applicability of the HIPAA security standards and penalties for security and privacy violations directly to business associates; established rigorous data security breach notification requirements; extended the accounting for disclosures requirement to treatment, payment and healthcare operations; imposed an express prohibition on the “sale of data” other than in limited circumstances; and significantly modified the categories of HIPAA violations, the range of civil money penalty amounts and the available defenses to a HIPAA action.
  - (ii) The new federal data security breach notification requirements apply in addition to those recently adopted in various states for the breach of either personal health information or personal information of any kind.<sup>75</sup> Increased and more aggressive HIPAA privacy and security compliance enforcement is expected.<sup>76</sup>
  - (iii) **NOTE: The final regulations implementing these HITECH Act changes are expected to be published in July 2012 and should be closely reviewed for additional requirements and insights.**
- b. Whether and to what extent HIPAA will permit providers to share protected health information (“PHI”) (as defined by HIPAA)<sup>77</sup> from their EHR systems with each other and with non-providers will be driven by various considerations, including:

---

consent requirement), and both the creation of a data repository that is intended to be used for research regulated by the Common Rule and a subsequent research study conducted using the data in the repository.

<sup>74</sup> 45 C.F.R. §§ 160, 162 and 164.

<sup>75</sup> See, e.g., M.G.L.A. 93H § 1 *et seq.*; Cal. Health & Safety Code § 1280.15.

<sup>76</sup> See, Economic Stimulus Package: Policy Implications of the Financial Incentives to Promote Health IT and New Privacy, McDermott Will & Emery White Paper (February 20, 2009), *available at* [http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object\\_id/ea996ed0-ba3b-480a-988a-135230c441d6.cfm](http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/ea996ed0-ba3b-480a-988a-135230c441d6.cfm) (last visited June 14, 2010); HHS Issues Interim Final Rule Conforming HIPAA Civil Money Penalties to HITECH Act, McDermott Will & Emery White Paper (November 12, 2009), *available at* [http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object\\_id/ae68626d-301b-4aa7-9a20-911cbe1b1f4a.cfm](http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/ae68626d-301b-4aa7-9a20-911cbe1b1f4a.cfm) (last visited June 20, 2010); Regulatory Update: HITECH’s Security Breach Notification Requirements, McDermott Will & Emery White Paper (April 22, 2009), *available at* <http://www.mwe.com/info/news/wp0409e.pdf> (last visited June 20, 2010); Regulatory Update: HITECH’s HHS and FTC Security Breach Notification Requirements, McDermott Will & Emery White Paper (August 27, 2009) *available at* [http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object\\_id/8e9bbcf4-afe4-4992-a277-6c3ce953a249.cfm](http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/8e9bbcf4-afe4-4992-a277-6c3ce953a249.cfm) (last visited June 20, 2010).

<sup>77</sup> 45 C.F.R. § 160.103.

- (i) The purpose for which the information is being shared (i.e., treatment, payment, healthcare operations, research);
  - (ii) Whether the providers sharing the network are participants in the same organized health care arrangement (“OHCA”);<sup>78</sup>
  - (iii) The nature and extent of the information in the EHR to which they are permitted access (e.g., their own patient information only, information of patients of the hospital or other physicians);
  - (iv) Who will have access and the purpose of the access and use (e.g., treatment, payment, health care operations)<sup>79</sup> (including those of an OHCA that engages in joint quality assurance and utilization review or joint managed care contracting involving financial risk), and research);
  - (v) Whether the information is in individually identifiable or in de-identified form,<sup>80</sup> or part of a limited data set;<sup>81</sup> and
  - (vi) Whether the network includes HIPAA’s administrative, physical, technical and organizational security safeguards.
- c. Worth noting here is that studies undertaken using an electronic network or repository for purposes of cost, quality and safety studies may be considered “health care operations” rather than “research” under HIPAA and that use for such health care operations purposes are not subject to the HIPAA authorization requirement. Careful consideration must nonetheless be given to whether the study is research under the Common Rule.<sup>82</sup> Drawing the lines is not always easy.
- d. Any electronic sharing of PHI, other than sharing by providers in connection with treatment or payment matters for common patients, should be carefully analyzed to verify compliance with HIPAA privacy requirements such as:
- (i) the need for patient authorizations and eligibility for exceptions to or waivers of the authorization requirement;
  - (ii) establishing access controls to meet minimum necessary standards and comply with the provisions of authorizations, authorization exceptions and authorization waivers;
  - (iii) patient record access and amendment rights provisions;
  - (iv) patient rights to accounting of disclosures;
  - (v) the criteria and contracting requirements for engaging business associates;

---

<sup>78</sup> *Id.*

<sup>79</sup> 45 C.F.R. § 164.501

<sup>80</sup> 45 C.F.R. §§ 164.514(b)(1) and (2)(i).

<sup>81</sup> 45 C.F.R. §§ 164.514(2)(i) and (e)(2).

<sup>82</sup> In December 2008, an official of OHRP publicly addressed the need to carefully draw lines between these two activities. “OHRP Official Recommends Drawing Lines To Determine Which Activities are Research,” *BNA Medical Research Law and Policy Report*, 7 MRLR 761 (December 3, 2008).

(vi) the criteria and contracting requirements relating to creation and use of de-identified data and limited data sets; and

(vii) the new prohibition against the sale or data.

Typically, the strategy for meeting these requirements will involve a combination of the HIT infrastructure design elements, policies and procedures, and associated training.

## 2. Other Federal Privacy Laws and State Laws Protecting the Confidentiality of Sensitive Health Information

- a. Certain other federal laws protect particular categories of information that may be included in the electronic information exchange. Principal among them is the federal law protecting the confidentiality of alcohol and drug abuse patient records.<sup>83</sup> Further, use of information from the exchange for clinical research may also trigger applicability of (a) the protections afforded human subjects in research by the federal regulations that protect human subjects who participate in federally funded research (i.e., the Common Rule),<sup>84</sup> (b) the FDA regulations applicable to research conducted in support of an application for FDA approval of the marketing of a new product,<sup>85</sup> and the Genetic Information Nondiscrimination Act of 2008 (“GINA”) which addresses the use of genetic information by group health plans, health insurers in group and individual markets, and issuers of Medigap policies in connection with certain insurance business functions.<sup>86</sup>
- b. Similarly, the laws of most if not all states prohibit or restrict uses and disclosures of information relating to mental health, developmental disabilities, AIDS and other sexually transmitted diseases, and genetic testing and counseling information, and some states have laws protecting the confidentiality of health information generally.<sup>87</sup>

In certain respects, these other federal and state privacy and confidentiality laws are more restrictive than, and thus preemptive of, HIPAA. In particular, they may require a written patient consent for both uses and disclosures for which HIPAA would not require an authorization, even at times when the information is being used internally by a covered entity

---

<sup>83</sup> 42 U.S. C. § 290dd-2 and 42 C.F.R. Part 2. *See also* “The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs” (June 2004), *available at* <http://www.samhsa.gov/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf> (last visited June 20, 2010), and “Frequently Asked Questions, Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE),” (June 16, 2010) *available at* <http://www.samhsa.gov/HealthPrivacy/docs/EHR-FAQs.pdf> (last visited June 20, 2010).

<sup>84</sup> 45 C.F.R. § 46(A)-(D).

<sup>85</sup> 21 C.F.R. § 50.1.

<sup>86</sup> The Genetic Information Nondiscrimination Act of 2008, Pub.L. 110-233, § 1(a) (May 21, 2008). *See also*, 45 C.F.R. § 144.103.

<sup>87</sup> A comprehensive review of state sensitive information confidentiality laws is outside the scope of this article. Examples of such state laws include the following: IND. CODE. ANN. § 16-18-2-226 (mental health information); MASS. GEN. LAWS. ch. 111, § 70F; ARIZ. REV. STAT. 12-2802; 74 ILCS 110/ (mental health information); 410 ILCS 305/ (HIV/AIDS information); 410 ILCS 513/ (genetic information); 410 ILCS 50/ (medical information generally).

or being exchanged only between or among treatment providers or with a business associate who has been hired to convert the information to a limited data set or fully de-identified form. Obtaining consent to use of data collected over several years and from a large number of patients prior to the creation of the electronic network or repository can be particularly challenging. Other challenges arising from a consent requirement include: (a) developing ways to track and firewall all information from a patient who refuses to give consent or who withdraws consent, and (b) attempting to segregate sensitive from non-sensitive information contained in a single patient record of a non-consenting individual (particularly in the context of mental health information where the lines between the two can be extremely gray).

### 3. EU and Other Foreign Data Protection Laws

Electronic information exchanges and repositories that contain identifiable health information of a foreign national may be subject to privacy requirements under myriad privacy laws of foreign countries, including those of the twenty-seven countries comprising the European Union (“EU”). The cornerstone of privacy protection in the EU is the EU Data Privacy Directive.<sup>88</sup> The EU adopted the Data Privacy Directive to establish a minimum level of protection among the member states and to prevent diverse national laws from becoming an obstacle to the integration of a single European market. While it provides some level of harmonization, it does not establish uniformity among the various national laws of the member states. Countries outside the EU also have privacy laws needing to be addressed.

## B. State Laws on Medical Records Form, Content and Retention

1. A lack of uniformity among current state laws governing the form, content and retention of medical records, which impedes the standardization of electronic health records and retention and destruction practices.<sup>89</sup>
2. Further, the development of necessary changes to these laws is unlikely to keep pace with the rapidly accelerating exchange and integration of EHR databases. Challenging medical records issues that will likely arise in an effort to apply these state laws include: (1) what is the medical record and what information comprises it (e.g., pop-ups, alerts, and reminders, video files (e.g., videos of office visits, procedures, and telemedicine consultations), information stored in audio files (for example, recorded patient telephone conversations, physician dictations, data from multiple electronic source systems));<sup>90</sup> (2) who owns the information and the record

---

<sup>88</sup> Directive 95/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing personal data and on the free movement of such data. Official Journal of the European Communities, November 23, 1995, No. L. 281/31.

<sup>89</sup> See William H. Roach, Jr., Robert G. Hoban, Bernadette M. Broccolo, Andrew B. Roth, Timothy P. Blanchard, Medical Records and the Law, 4th ed. Jones and Bartlett, MA (2006), pp. 31-50.

<sup>90</sup> The Electronic Health Record has been defined by the Health Information and Management Systems Society <http://www.himss.org/ASP/topics-EHR.asp>; by the American Health Information Management Association (“AHIMA”), “Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes,” *Journal of AHIMA* (September 2005): 64A; and by the Federal EHR Regulations *supra* at Notes 66 and 67.

containing the information; (3) who controls the record; and (4) who has the obligation to maintain it for purposes of applicable legal requirements.

3. As patients create their own personal health records as part of integrated, community-wide health data networks and personalized healthcare delivery, an organization must also determine whether and to what extent these personal health records should be incorporated into its legal health record.

### C. Standard of Care for Malpractice Liability

1. Widespread proliferation of electronic health record networks and repositories may ultimately elevate the standard of care for negligence purposes, at least in certain communities or regions. The question which has been asked in other contexts that may well be asked in this one is whether a physician is negligent or provides substandard care if he or she does not utilize information that is available for making medical decisions.<sup>91</sup>
2. Also, maintaining the integrity and reliability of health information used to exercise medical judgment will be increasingly challenging as information is aggregated and exchanged electronically between and among key stakeholders in the public and private sectors. Failure to do so clearly carries professional liability risk.
3. An important consideration is the risk that the secondary use of an individual's health information will create an implicit obligation to notify an individual of observations made when using the data that may relate to the individual's health or propensity for certain diseases or conditions. Necessary consents and authorizations should be carefully drafted with this risk in mind.
4. Finally, the availability of electronic health information networks will also likely fuel the growing trend toward e-Discovery litigation. Important considerations relevant to the use of and defense against the use of e-Discovery include: (a) what portion of the electronic health record constitutes the medical record (clinical care information, administrative information, laboratory test results, etc.)(discussed further below); (b) will the electronic health record meet the standards for admissibility, particularly in light of the challenges of authentication; (c) how to manage the increased risk of inadvertent "destruction of evidence" under electronic record and retention practices; (d) what will be the cost of electronic discovery and who should bear it; and (e) the ease of searching and the persistence/indestructibility of electronic health information.

---

<sup>91</sup> Jacobsen, P.D., Medical Liability and the Culture of Technology, Project on Medical Liability in PA, 7/2004, <http://medliabilitypa.org>. See also Das v. Thani, 2002 N.J. Lexis 548, 171 N.J. 518 (N.J., 2002) (fetal monitoring case in which physician did not use ultrasound available in his office in favor of "1960s-style" maternal fetal monitoring; expert testimony went both ways); Suniga v. Eyre, 2004 Tex. App. Lexis 486 (unpublished)(regarding whether the standard of care included the duty to consult past medical records); Susnis v. Radfar, 2000 Ill. App. Lexis 859, 739 N.E. 2nd 960 (Ill. App. 2000)(involving allegations that the standard of care included the duty to consult past medical records); Primus v. Galgano, 2003 U.S. App. Lexis 9803, 329 F. 3rd 236 (1st Cir., 2003)(failure to obtain past medical records is a departure from the standard of care).



#### D. Federal Laws Regulating the Donation of EHR Technology by Hospitals to Physicians

1. The health reform related HIT strategy of many hospitals and health systems is likely to include the donation of EHR technology to physicians to expedite their adoption of EHR. Such donations raise implications under federal healthcare fraud and abuse laws as well as tax-exemption laws.
2. Prior to the adoption of the HITECH Act's financial incentives for meaningful use of Certified EHR Technology, the federal government implemented some relief from the fraud and abuse concerns that were impeding EHR initiatives.
  - a. Specifically, in August 2006, the Centers for Medicare & Medicaid Services ("CMS") published final regulations setting forth an exception to the Stark Law for the provision of EHR items and services by hospitals to physicians ("**EHR Exception**")<sup>92</sup> and the Office of the Inspector General ("**OIG**") published final regulations setting forth a corresponding safe harbor under the Anti-Kickback Statute<sup>93</sup> ("**EHR Safe Harbor**" and collectively, with the EHR Exception, the "**Federal EHR Regulations**").
  - b. The EHR Regulations provide a roadmap for structuring permissible donations of EHR technology by hospitals to physicians. The structural considerations and conditions relate to (i) which individuals and entities are permitted to be donors; (ii) which individuals and entities are permitted to be recipients; (iii) what items and services may be donated; (iv) what agreements must be in place to document the donation; (v) what requirements exist for cost sharing; and (vi) certain other conditions that must be satisfied in order to assure that the arrangement avoids improper inducements to make referrals for Medicare and Medicaid-covered items and services and that the hospital makes prudent use of the resources it has available to invest in a donation program.<sup>94</sup>
3. The Internal Revenue Service ("**IRS**") subsequently issued a directive concerning the tax-exemption implications of the EHR donations contemplated by the Federal EHR Regulations under the private inurement and more than incidental private benefit prohibitions of Section 501(c)(3) of the Internal Revenue Code ("**Code**") (the "**IRS EHR Directive**").<sup>95</sup>
  - a. The IRS EHR Directive states that the IRS will not treat the corresponding benefits a hospital provides to its medical staff physicians as an impermissible

---

<sup>92</sup> 42 C.F.R. § 411.357(w).

<sup>93</sup> 42 C.F.R. § 1001.952(y).

<sup>94</sup> For a more detailed discussion of the criteria and conditions, see the Federal EHR Regulations themselves *supra* at Notes 66 and 67 and McDermott Will & Emery White Paper "Donating Health Information Technology: Final Regulations Compete with HR 4157 for Public Policy Control," *available at* <http://www.mwe.com/info/news/wp1006a.pdf> (last visited June 24, 2010).

<sup>95</sup> IRS Memorandum, "Hospitals Providing Financial Assistance to Staff Physicians Involving Electronic Health Records" (May 11, 2007).

private benefit or inurement if the hospital meets several requirements: (a) the hospital and the participating physicians comply with the requirements of the Federal EHR Regulations on a continuing basis; (b) to the extent permitted by law, the hospital may access all of the electronic medical records created by a physician using the donated items or services; (c) the hospital ensures that the donated items and services are available to all of its medical staff physicians; and (d) the hospital provides the same level of subsidy to all of its medical staff physicians or varies the level of subsidy by applying criteria related to meeting the healthcare needs of the community.<sup>96</sup>

- b. The IRS subsequently clarified that for any entity that is not able to meet all of these requirements, it would utilize a facts and circumstances analysis to determine whether the arrangement poses any tax concerns. The directive thus amount essentially to a “safe harbor” that can be varied from as necessary so long as alternative facts and circumstances exist to provide a defensible position.

## E. Antitrust

1. Inclusion of fee and non-fee related information in a health information network that integrates the data of multiple providers, other than those that are under common ownership or control or part of an integrated economic risk sharing arrangement,<sup>97</sup> creates risk under federal antitrust laws that seek to promote competition and restrict anti-competitive behavior.<sup>98</sup> In August 1996, the FTC and the DOJ issued joint statements on health care antitrust issues that established two safety zone for the exchange of information between providers and payors. These safety zones remain in effect today and are instructive for purposes of managing antitrust risk in the formation of HIEs.<sup>99</sup>
  - a. The first of the two applies to the exchange of non-fee-related information such as medical data (e.g., outcomes data for a particular medical procedure collected by a medical society from its members) that may help to conduct activities that address issues related to the mode, quality or efficiency of treatment such as the development of practice parameters (i.e., standards for patient management developed to assist providers in clinical decision-making) or clinical protocols.<sup>100</sup>

---

<sup>96</sup> IRS Circular 230 Disclosure: To comply with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained herein, unless specifically stated otherwise, is not intended or written to be used, and cannot be used, for the purposes of: (1) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter herein.

<sup>97</sup> See FTC 2004 Report *supra* at Note 17 and discussion *supra* at Note 18.

<sup>98</sup> *E.g.*, Section 1 of the Sherman Act, 15 U.S. C. §§ 1-7. *See also United States v. Burgstiner*, 1991-1 Trade Cas. (CCH) Par. 69422 (S.D. Ga. 1991), and discussion *supra* at note 16.

<sup>99</sup> Federal Trade Commission and Department of Justice Statement of Antitrust Enforcement in Healthcare (August 1996), 4 Trade Reg. Rep. ¶¶ 20,809-11 (“FTC 1996 Statements”) available at <http://www.ftc.gov/reports/hlth3s.pdf> (last visited June 22, 2010).

<sup>100</sup> *Id.* At p. 41.

- b. The second one applies to the exchange of fee-related information and sets forth three qualifying criteria for qualifying for “safety zone” for use of an integrated data network to share financial information among non-integrated competing providers: (a) the collection of financial data must be managed by a third party (e.g., a purchase, government agency, consultant, academic institution or trade association); (b) even if current fee-related information is provided to purchasers, any information shared among or available to competing providers furnishing data must be more than three months old; and (c) if information is available to providers furnishing data, the information disseminated must be sufficiently aggregated that it would not allow recipients to identify the prices charged by any one provider (there must be at least five providers reporting data upon which each disseminated statistic is based and no individual provider’s data may represent more than 25 percent of that statistic on a weighted basis).<sup>101</sup> For surveys of price or cost (e.g., surveys of employee compensation), there is an additional requirement that the data collected must be more than three months old.<sup>102</sup> Information exchanges outside of the safety zone are analyzed under the Rule of Reason.<sup>103</sup>
2. In April 2010, the DOJ announced that it will not challenge a proposal by the Hospital Value Initiative (HVI) to establish an information exchange program that will provide data on the relative costs and resource efficiency of more than 300 hospitals in California because the proposed information exchange may reduce health care costs by improving competition among hundreds of hospitals in California and facilitating more informed purchasing decisions by group purchasers of health care services. Consistent with the above safety zone requirements, the DOJ concluded that a low risk of anticompetitive effect existed in part because the exchange would involve data that is at least 10 months old and the program would not disclose disaggregated data or any hospitals’ actual services fees.<sup>104</sup>
3. In mid-June 2010, the FTC announced its plan to hold a public workshop on health care competition policy, payment reform, and new models for delivering health care that seek to incentivize high-quality, cost-effective care, including ACOs, and to create a workshop website that will contain the program agenda, list of speakers, materials, etc. as these are developed.<sup>105</sup> These efforts of the FTC and any corresponding efforts of the Department of Justice should be watched closely for policy and enforcement guidance concerning the antitrust implications of implementing the HIT infrastructure incentivized by ARRA and ACA, including any changes to the two 1996 safety zones applicable to such exchanges.

---

<sup>101</sup> *Id.* at pp. 43-48.

<sup>102</sup> *Id.*

<sup>103</sup> *Id.*

<sup>104</sup> “Department of Justice Will Not Challenge Hospital Cost Information Exchange Program in California, PR Newswire (April 26, 2010), *available at* <http://www.prnewswire.com/news-releases/departments-of-justice-will-not-challenge-hospital-cost-information-exchange-program-in-california-92101269.html> (last visited June 22, 2010).

<sup>105</sup> *See* the full-text of the Chairman’s speech *available at* <http://www.ftc.gov/speeches/leibowitz/100614amaspeech.pdf> (last visited June 14, 2010).

## **F. Ownership of Networks/Exchanges, Repositories and their Contents**

1. Widespread disagreement currently exists regarding who owns repositories of biological tissue and data and the intellectual property rights associated with and derived from them. This ownership question is critical both to use of such repositories for future research and to commercialization of products based on such use.
2. Recent case law<sup>106</sup> and state laws governing tissue donation will also implicate information exchange networks and information repositories both with respect to the need for an individuals' informed consents and the preservation and allocation of ownership and use rights in agreements between and among the parties involved in an electronic information exchange or data.
3. The law in this regard remains somewhat unsettled. As the debate continues and key legal and ethical questions are addressed, the participants should take steps to confirm that intellectual property ownership and access rights and expectations are clearly articulated and understood.

## **VIII. CONTRACTING STRATEGIES FOR MITIGATING AND MANAGING RISKS**

The evaluation of the HIT needed to establish and operate an EHR, HIE or repository and the vendor contracting to acquire the systems must be carefully undertaken with the legal, financial and strategic considerations in mind. Following is an overview of certain key considerations to be addressed.<sup>107</sup> These and other key considerations are illustrated and discussed in the set forth in the **Illustrative Contract Provision Appendix** to this Outline.

### **A. HIT Vendor Contracts**

1. Technology System Features, Functions and Performance Capabilities
  - a. Key Questions:
    - (i) Whether the system will provide the necessary features, functions and tools to implement the intended strategy and to comply with applicable legal and regulatory requirements, both as they exist at the time of the contract and as they are likely to evolve and change during the life of the contract.
    - (ii) A key strategic consideration is whether the system's plan for interoperability and data integration will accommodate the short and long-term nature and extent of contemplated information exchange, both as mandated by initiatives and demands in both the public and private sectors.

---

<sup>106</sup> See, e.g., *Washington Univ. v. Catalona*, 552 U.S. 1166 (2008).

<sup>107</sup> This discussion is not intended as legal advice and should not be considered exhaustive of the full scope of issues needing to be addressed in the contracting process.

- b. Key compliance considerations for a provider or payor include, without limitation:
  - (i) Whether the technology qualifies as Certified EHR Technology that can achieve interoperability and meaningful use on an ongoing basis as the meaningful use requirements of the various stages are defined and developed.
  - (ii) Whether the system can:
    - (a) establish and manage access rights according to role and purpose of access (e.g., treatment, billing and payment, utilization review and quality assurance, research);
    - (b) limit access to certain records or types of data (e.g., records of patients who have refused or withdrawn consent, categories of information given special protection under federal and state laws );
    - (c) monitor and audit access, and maintain compliance with other federal and state privacy and security requirements;
    - (d) accommodate the centralized administration of the HIPAA patient rights provisions (i.e., the right to request additional restrictions on disclosure of their PHI, the right to access their records, the right to accounting of certain disclosures, and the right to amend records); and
    - (e) enable implementation of a joint notice system for an OHCA.
  - (iii) The extent of the vendor's commitment to update and modify the system as regulatory changes occur (e.g., EHR certification and meaningful use standards) and the financial terms corresponding to that commitment.
- c. If the health system is able to identify essential business and compliance-related features, functions and operations/performance needs prior to contract execution, the agreement should include terms to ensure that such features and functions will be included in the system when it is first delivered and implemented.
  - (i) Listing all features, functions and performance requirements in the specifications for the system provides the most protection and including the specifications as part of the definition of the "system" that is to be delivered, implemented, tested, warranted and maintained by the vendor.
  - (ii) A fall-back preferable, approach is to provide that the vendor will develop certain features and functions as customizations to the system. It will be essential, however, to include the customizations in the definition of the "system" that is to be delivered, implemented, tested, warranted and maintained by the vendor.
- d. It will be impossible at the time of initial contracting to anticipate all relevant business and compliance considerations that could affect the essential features and functions of the system over its useful life. Regulatory changes as well as operational/business process changes will likely occur, and such changes may necessitate system modifications,

enhancements, retrofitting or other measures. An important contracting consideration is whether and to what extent the vendor will commit to make necessary changes and whether that will be provided as part of the ongoing maintenance fee or for an additional support fee.

- (i) The preferred approach is to require the vendor to make the changes to the system needed to achieve compliance changes and additions at no additional charge. This obligation could be included as a part of the vendor's ongoing support obligations, such as its obligation to make regulatory changes.
- (ii) A fall-back position is to require the vendor to make such revisions via a change order process specifically provided for in the IT agreement. Adding the necessary features and functions through a change order procedure, however, could result in additional, unanticipated and unbudgeted costs. Any additional charges should be negotiated prior to executing the vendor agreement. In addition, the vendor Agreement should affirmatively obligate the vendor to make the changes if needed.

## 2. Responsibility for Data Accuracy, Integrity and Completeness

- a. Maintaining the accuracy, integrity and completeness of the data in an electronic health information network and repository, at all times, is essential. Doing so will become more challenging as the number and diversity of the participants expands.
- b. The vendor agreement should expressly articulate the relative responsibility of the customer's and the vendor in this regard. The customer's responsibility should be to input/include only accurate and complete information and to establish and maintain technical and administrative security protections in their facilities and operations. The vendor's responsibilities should include providing and maintaining technology that is free from defects and meets functional and performance expectations and covenanting and warranting that the system infrastructure (features, functions, performance standards, etc.), both as initially implemented and as supported by the vendor during its useful life, will be sufficient to maintain data accuracy, integrity and completeness as providers access and use it. A vendor's obligation to assist with migration of existing data should also be articulated.

## 3. Malpractice Liability

Allocation of risk for malpractice liability is closely related to the issues discussed in 1 and 2 above. Vendors typically seek to disclaim all responsibility for malpractice liability. Disclaimer of liability is acceptable in most cases other than to the extent the vendor's failure to deliver and implement, as well as maintain, the system in accordance with the product description and performance standards set forth in the agreement contribute to the patient harm.

## 4. Privacy and Confidentiality

In most if not all cases, the vendor will be a business associate under HIPAA and, therefore, the agreement must meet include the required HIPAA business associate

provisions. The HITECH Act provisions now holds the vendor directly responsible for HIPAA privacy and security compliance requirements. (See related limitation/disclaimer liability discussion below.)

#### 5. Defining Vendor Rights to Access and Use Data

Vendors themselves can have an interest in having accessing and using data in an EHR or HIE for secondary purposes (e.g., future product development, testing and marketing). Including a provision that clearly establishes the exclusive data ownership rights of the hospital, physicians and other participants and appropriate limits on the vendor's ability to use the data for other than providing services is essential. The Business Associate Agreement corresponding to any vendor relationship may be the appropriate place for such provisions.

#### 6. Scope of License Rights to Accommodate the Universe of Intended Uses and Users

- a. The scope should be consistent with the short term and long-term business plan. For example, in agreement for an EHR system, the license scope should contemplate both an initial roll-out to a hospital's medical staff physicians and a subsequent roll-out to other community physicians, laboratories and other ancillary providers, pharmacies, etc. Similarly, an agreement for technology to support an HIE should contemplate exchange of information initially among entities within a health system and ultimately with unaffiliated providers, vendors, and other HIEs and it should take into account any phasing of the scope of the purposes for which information will be exchanged over time among HIE participants.
- b. Affordability and predictability of license, implementation and support fees will be important to the short-term and long-term feasibility of the HIT initiative. Rights to expand the scope of permitted use and users over the license of the agreement and associated fees should be addressed in the negotiation of the vendor agreement at the front end.

#### 7. Assuring Cross-Vendor Accountability and Cooperation

The establishment and ongoing operation of the EHR, HIE or repository agreement will likely involve the technology and services of various vendors. An agreement with each vendor that contains a clear and complete description of the technology and services the vendor is providing will enhance the basis for effective overall management of the endeavor and minimize the risk of "finger-pointing" among the vendors that can produce project disruption, delays and failures. Also, including an affirmative commitment by each vendor to cooperate with other vendors is advisable.

#### 8. Narrowing Liability Limitations and Disclaimers

- a. Vendors typically impose caps on direct damages and disclaimers of all liability for consequential, incidental and special damages.
- b. Harm resulting from violations of federal and state privacy, confidentiality laws and data breach notification laws (e.g., injury to patients, penalties and fines, and internal costs incurred to meet notification requirements and implement other remediation steps) will likely fall into one or more of the categories of disclaimed harm (e.g., incidental, special and consequential damages) and thus should be expressly addressed as an affirmative

obligation of the vendor and that obligation should be carved out of any vendor damage limitations and disclaimers.

- c. As a related matter, vendor disclaimers of malpractice liability arising from the use of data in the exercise of medical judgment is acceptable in most cases other than to the extent the liability arose from the vendor's failure to perform from defects in the system.

## 9. Anticipating Changing Relationships

Exceptions to common restrictions on assignments will be needed to accommodate structural and relationship changes that are likely to occur as an organization's HIT strategy evolves over time.

## **B. Special Considerations in Cloud Computing Agreements<sup>108</sup>**

Like any business transaction, contracting for cloud computing services raises several legal issues that must be adequately addressed in the contract to ensure an acceptable level of services, to maintain compliance with various federal and state laws, and to provide adequate protections and remedies for both the end-user customer and the service provider. The following is a checklist of some key contracting considerations:

### 1. Service Level Agreements ("SLAs")

Contracts for cloud-based services should explicitly spell out service level requirements, including, but not limited to: (i) times of access and operation; (ii) uptime commitments; and (iii) remedies for chronic downtime.

### 2. Disaster Recovery and Business Continuity Plans

Although cloud computing is designed to provide a maintenance-free infrastructure for health care organizations, it also leaves such organizations at the mercy of the vendor when and if something goes wrong. For services or applications that are mission-critical, organizations should ensure that the service level agreements with the vendors adequately address how the services will continue in the event of a disaster.

### 3. Audit Rights

The agreement with the vendor should include a right to audit the vendor's data security program and compliance with applicable privacy and data security laws at least annually or more frequently in the event of any actual or suspected security breach or failure of vendor to comply with the law. The guidance for reporting on vendor organizations controls is now SSAE 16 replacing SAS 70. At a minimum, customers should consider obtaining industry standard certifications and any reports

---

<sup>108</sup> The author acknowledges the contributions of Jean Pechette, her partner at McDermott Will & Emery LLP, for her contributions to this section.



of deficiencies and corrective measures. Customers should also consider requiring the vendor to permit regulators to conduct audits of the vendor as may be required.

#### 4. Cross-Border Concerns

Organizations should consider whether to incorporate provisions addressing cross-border concerns, particularly when dealing with foreign vendors or arranging for the provision of services for a provider located outside the U.S. The cloud contract should specify the location of the data centers to be used for storage of PHI and other information. If use of overseas data centers is permitted, the privacy policy provided to patients should indicate that their information may be transferred outside the U.S.

#### 5. Use of Subcontractors

Particularly with regard to privacy and security compliance concerns, customers will want to control/limit the cloud vendor's ability to use subcontractors. In short, in addition to meeting the HIPAA downstream Business Associate Agreement requirements, the primary vendor should in all respects be held directly and fully accountable for all acts and omissions of permitted subcontractor as if they were those of the primary vendor. Further, no contractual protections will be a substitute for also conducting up front due diligence concerning the nature and extent to which the cloud vendor will outsource some or all of its responsibilities to third parties.

#### 6. Exit Strategy and Associated Data Issues

Cloud contracts should include termination rights for each party with proper allocation of the risks and costs for early termination, adequate transition services and data migration. In the event of a termination or unwind for any reason, organizations will want the ability to extract data from their current vendor and migrate data to their new vendor. In this regard, the contract should be clear that, as between the vendor and the user, the data is owned and continues to be owned exclusively by the user, even if hosted by the vendor. The contract should also provide for the transferability of the data, specify the format and other relevant details, and explicitly obligate the vendor to assist the user and cooperate with its new vendor to effectuate such potential transfer.

### **C. Special Considerations in Contracting for EHR Network, HIE and Repository Collaborations**

1. An EHR network, HIE and robust health information repository can emanate from any one stakeholder's HIT initiatives and evolve into subsequent collaborations and relationships of various types among two or more industry stakeholders, such as an institutional provider, large medical practices, payors, universities, research institutes, governmental bodies, other HIEs, and/or product manufacturers. See **ILLUSTRATIONS 2 THROUGH 6**.
2. Whether the collaboration exists solely by contractual agreement or creation of a new entity, a detailed written agreement is essential and should include the following:

- a. A clear articulation of the purpose, scope and goals of the collaboration as contemplated over its anticipated life;
  - b. The nature and extent of the HIT infrastructure being created through the implementation of new systems and the integration of existing systems; Current or future plans to create a new entity to assume all or part of the responsibility for operation of the network;
  - c. The relative rights and responsibilities of the participants with regard to: (1) governance and management of the network, HIE or repository; (2) funding, both initial and future; (3) integrity of data (accuracy, completeness, timeliness); (4) judgments made using the data in a clinical care context; (5) ownership of, and rights to access and use, the systems and data; (6) extension of access to non-participants; (7) responding to electronic discovery requests; (8) liability and compliance risk and indemnification and insurance; (9) development and management of a legal and regulatory compliance plan (including patient consent considerations); (10) strategic planning and budgeting; (9) communications and relationships among the participants and with external constituencies (e.g., government, HIT vendors); (11) maintaining the long-term sustainability of the network/repository and implementing changes needed to do so; and (12) termination and withdrawal of the relationship by one or more participants.
3. Allocation of risk and responsibility in a private HIE relationship can present unique challenges arising from the fact that providers often wear two hats – that of a founder/owner of the HIE itself and that of a provider participant in the information exchange offered by the HIE.
- a. In the early stages, there can be a tendency to think of the HIE and the provider participants as one and a corresponding failure to recognize that the HIE is in fact a separate business operation regardless of whether it is a creature of contract alone or a newly formed entity. If the HIE is successful, it will evolve into an endeavor that should be recognized as separate from the participants, even the founder participants, and held accountable for risks and liabilities arising from what it is providing for the participants (both directly and indirectly through contractual relationships with vendors and support organizations).
  - b. For example, the HIE will be providing the IT infrastructure and ongoing maintenance of it, support services, compliance policies and procedures, etc., some or all of which can ultimately affect the integrity (accuracy, completeness and timeliness), as well as the availability, of the data upon which the provider participants will rely for the delivery of and payment for patient care. Why would the HIE not be held accountable for, and obtain insurance to cover, liability arising from its own acts and omissions in these respects (again, whether the acts or omissions are those of its own personnel or those of vendors and other support organizations to whom it outsources certain of its responsibilities).
  - c. A reluctance to burden the HIE in the early stages, and a corresponding tendency to shift the bulk of the risk to the providers as participants, must be assessed against other key factors such as the nature and the nature and extent of the role the HIE will have over time, the nature and extent to which ownership/control will be afforded to others beyond the original provider founders, the anticipated

expansion over time of the nature and extent of the purposes of which the providers will exchange information through the HIE, and the extent to which the founder/participants will over time have the ability to control or influence the operation and management of the HIE.

## **IX. RESOURCES AND REFERENCES**

1. **PWC: Designing a Health IT Backbone for ACOs**,  
<http://www.pwc.com/us/en/health-industries/publications/designing-a-health-it-backbone-for-acos.jhtml>
2. Managed Care Magazine Online, ©MediMedia USA: “ACOs Will Depend on HIEs, With an Assist from Plans,” **January 2011**.  
<http://www.managedcaremag.com/archives/1101/1101.hies.html>
3. **Medicity Technology Fundamentals for Realizing ACO Success**,  
[http://resource.medicity.com/free-whitepaper-realizing-aco-success/?utm\\_campaign=Medicity.com-WP-ACO-Success&utm\\_medium=Medicity.com&utm\\_source=Referrals&utm\\_content=ACO%20Success](http://resource.medicity.com/free-whitepaper-realizing-aco-success/?utm_campaign=Medicity.com-WP-ACO-Success&utm_medium=Medicity.com&utm_source=Referrals&utm_content=ACO%20Success)
4. **Health Level Seven International Glossary of Terms**,  
<http://www.himss.org/content/files/Code%20188%20HL7%20Glossary%20of%20Terms.pdf>
5. **eHealth Initiative HIE Toolkit**, <http://www.ehealthinitiative.org/hie-toolkit.html>
6. **HIMSS Health Information Exchange (HIE) Glossary**,  
<http://www.himss.org/content/files/2009HIEGUIDEGlossary.pdf>
7. Department of Health & Human Services Office of National Coordinator for Health Information Technology, Acronym Guide,  
[http://healthit.hhs.gov/portal/server.pt/community/health\\_it\\_hhs\\_gov\\_\\_acronyms/1217](http://healthit.hhs.gov/portal/server.pt/community/health_it_hhs_gov__acronyms/1217)
8. **HIMSS Quality 101 Definitions/Glossary of Terms**,  
[http://www.himss.org/content/files/quality101\\_glossary.pdf](http://www.himss.org/content/files/quality101_glossary.pdf)
9. **AMA Meaningful Use Glossary and Table**,  
[http://www.himss.org/content/files/Code49\\_%20AMA%20Meaningful%20use%20glossary%20and%20requirements-table.pdf](http://www.himss.org/content/files/Code49_%20AMA%20Meaningful%20use%20glossary%20and%20requirements-table.pdf)
10. Department of Health & Human Services Office of National Coordinator for Health Information Technology and Alliance for Health Information Technology Glossary (Also contains a robust bibliography),  
<http://www.himss.org/content/files/Code%205%20Defining%20Key%20Health%20Information%20Technology%20Terms.pdf>

11. **2011 Report on Health Information Exchange: Sustainable HIE in a Changing Landscape (eHealth Initiative)**, available for a fee at [http://www.ehealthinitiative.org/store.html?page=shop.product\\_details&flypage=flypage.tpl&product\\_id=83&category\\_id=8](http://www.ehealthinitiative.org/store.html?page=shop.product_details&flypage=flypage.tpl&product_id=83&category_id=8)
12. Department of Health & Human Services Office of National Coordinator for Health Information Technology State Health Information Exchange Program Resources, <http://statehieresources.org/topics-2/>
13. AHRQ (Agency for Healthcare Research and Quality) Study: Liability Coverage for RHIOs and HIEs AHRQ Publication No. 09-0071-EF (June 2009), <http://www.ehealthinitiative.org/resources/viewcategory/60-liability.html>
14. **Massachusetts Attorney General Enforcement of Data Breach Laws**, <http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-05-24-south-shore-hospital-data-breach-settlement.html>
15. Sittig, Dean F and Ash, Joan S., *Clinical Information Systems Overcoming Adverse Consequences*, Jones and Bartlett (2011).

Appendix

**ILLUSTRATIVE CONTRACT PROVISIONS**

*The contract provisions set forth herein are for discussion and illustration purposes only. They are not intended as model provisions for any stakeholder or as legal advice and should not be considered exhaustive of the full scope of issues needing to be addressed in the contracting process. Nor should they be used without the advice of qualified legal counsel.*

<b>VENDOR HIT SYSTEM LICENSE, IMPLEMENTATION AND SUPPORT AGREEMENT</b>	
<b>Customer's Proposed Language</b>	<b>Commentary</b>
<p><b><u>Compliance With Laws.</u></b> Vendor and Customer shall comply with all applicable laws and regulations with respect to this Agreement, including U.S. export control laws. <b>Vendor represents and warrants that the Software and Services are and will be provided in compliance with, and will enable Customer and its Affiliates at all times to use the Software in compliance with, all applicable laws and regulations.</b> Neither party shall have any liability to the other for any non-performance of their obligations under this agreement to the extent that the non-performance is mandated by applicable law.</p>	
<p><b><u>Regulatory Updates</u></b> Maintenance Services shall include, at no additional cost to Customer, any changes(s) to the Software necessary to enable the Customer, the Facility and Permitted Users to operate in a manner consistent with the mandatory requirements of applicable federal and state laws (as in effect from time to time) implicated by the use of the Integrated Solution (a "<b>Regulatory Update</b>") in a manner consistent with Vendor's customary approach to the release of features and functionality in a Generally Available release to those customers to whose business the Regulatory Update applies (regardless of whether Vendor is providing such Regulatory Update to such customers); provided, however, that if any such Regulatory Updates require significantly new features, functionality or extraordinary additional software development efforts beyond that historically and customarily expended by Vendor in providing Software Maintenance Services, Vendor may charge, and Customer agrees to pay, for such efforts at a price not to exceed Customer's pro-rata share of Vendor's actual costs of developing such Regulatory Update (such pro-rata to be based directly on the total number of Customers that have licensed the affected Software and are affected by the Regulatory Update); provided further however that if Vendor is not providing such Regulatory Update to other Vendor customers, Vendor shall (1) offer such Regulatory Update to any Vendor customer to whose business the Regulatory Update applies and (2) charge Customer for such Regulatory Update Customer's pro-rata share of Vendor's actual cost of developing such Regulatory Update and include Vendor customers who accept such offer in the calculation of Customer's pro-rata share.</p>	
<p><b><u>Insurance.</u> Alternative A</b></p>	

<p>Vendor shall maintain (and cause its permitted subcontractors, if any, to maintain) insurance coverage with carriers acceptable to Customer and in the amounts set forth below, and must name Customer as an additional insured on the Comprehensive General Liability insurance policy. Vendor shall furnish to Customer either a certificate showing compliance with these insurance requirements or certified copies of all insurance policies within 10 days of Customer's written request. The certificate will provide that Customer will receive 30 days' prior written notice from the insurer of any termination or reduction in the amount or scope of coverage. Vendor's furnishing of certificates of insurance or purchase of insurance shall not release Vendor of its obligations or liabilities under this contract.</p> <p>(a) Workers' Compensation: statutory limits for the state(s) in which this Agreement is to be performed (or evidence of authority to self-insure);</p> <p>(b) Employer's Liability: with a limit of not less than \$_____;</p> <p>(c) Comprehensive General Liability: covering liability arising from premises, operations, independent contractors, products/completed operations, personal injury and advertising injury, and liability assumed under an insured contract: in combination with Excess or Umbrella Liability Insurance, with limits of \$_____ each occurrence and \$_____;</p> <p>(d) Coverage for embezzlement, other employee dishonesty and forged documents with limits of \$_____ in the aggregate; and</p> <p>(e) Technology Errors &amp; Omissions (or technology professional liability coverage) insurance and other insurance, including coverage for loss, damage or disclosure of electronic data, media and content rights infringement and liability, network security failure, software copyright infringement liability, negligence in the provision of services, computer viruses and other malicious software, and property damage due to the failure of Vendor's System and Services with limits of \$_____ in the aggregate.</p>	
<p><b><u>Insurance. Alternative B.</u></b></p> <p>Vendor agrees to procure and maintain during the term of this Agreement policies of insurance as set forth in Exhibit XX (See <u>Schedule 1</u> to this document). Vendor shall furnish Customer with certificates of insurance at Customer's request.</p>	
<p><b><u>Insurance. Alternative C.</u></b></p> <p>See <u>Schedule 2</u> to this document.</p>	<p>See also AHRQ (Agency for Healthcare Research and Quality) Study: Liability Coverage for RHIOs and HIEs AHRQ Publication No. 09-0071-EF (June 2009), <a href="http://www.ehealthinitiative.org/resources/viewcategory/60-liability.html">http://www.ehealthinitiative.org/resources/viewcategory/60-liability.html</a></p>

**BUSINESS ASSOCIATE AGREEMENT GENERALLY**

Business Associate Agreement; Data Security – Generally.

Vendor shall hold all PHI, Health Records, and Personal Information in the strictest confidence in accordance with applicable law, including but not limited to Minnesota Statutes Section 144.335 and HIPAA, as each may be modified or amended from time to time. Vendor acknowledges that it is a Business Associate (as defined by HIPAA). Vendor shall secure, use and disclose PHI, Health Records and other Personal Information only in accordance with the Business Associate Agreement. In addition, Vendor shall secure PHI in accordance with the guidance issued by the U.S. Department of Health and Human Services from time-to-time pursuant to Section 13402 of the HITECH Act specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals, including the guidance published at 74 Fed. Reg. 19006 - 19010. To the extent the provisions of this Agreement are more protective of Customer’s Confidential Information than is required by applicable laws governing the privacy and/or security of PHI, Health Records or other Personal Information, the provisions of this Agreement shall apply.

Vendor shall exclude from its stage data and any other decrypted Customer Data the following sensitive data elements: Social Security Numbers; governmental health plan identification numbers (including, without limitation, Medicare HIC numbers); driver’s license numbers or state identification card numbers; credit and debit card numbers; bank account numbers; and other similar financial account numbers).

**Reporting of Disclosures of PHI.** Vendor shall report to Customer, as soon as practicable, but in no event later than within seven (7) days of becoming aware of any Security Incident or use or disclosure of PHI not provided for in this Agreement or in violation of the terms of Agreement by Vendor, its officers, directors, employees, contractors or agents or by a third party to which Vendor disclosed PHI pursuant to this Agreement. In such event, Vendor shall, in consultation with Customer, mitigate, to the extent practicable, any harmful effect that is known to Vendor of such improper use or disclosure. In addition, Vendor must report to Customer any unauthorized acquisition, access, use or disclosure of Protected Health Information (whether electronic, oral or in any other medium and whether secure or unsecured) within seven (7) business days of the date on which Vendor first becomes aware of such unauthorized acquisition, access, use or disclosure. Vendor shall also, as a part of such notification, provide Customer with the name and phone number of a contact person, authorized to act on behalf of Vendor, to work with Customer in ensuring that all required HIPAA obligations are met as efficiently and accurately as possible. **Vendor will reimburse Customer for all costs, expenses and damages (including, without limitation, reasonable attorneys fees and any reasonable steps to mitigate an individual’s risk of identity theft) associated with any notification process that may be required under HIPAA with respect to any Breach of unsecured Protected Health Information caused by Vendor or its agents or subcontractors.**

<p>EXCEPT WITH RESPECT TO THE INDEMNIFICATION OBLIGATIONS UNDER SECTION XX (INFRINGEMENT) AND SECTION XX (GENERAL INDEMNIFICATION), EITHER PARTY'S BREACH OF SECTION XX (GENERAL CONFIDENTIALITY), EITHER PARTY'S BREACH OF SCHEDULE X (BUSINESS ASSOCIATE AGREEMENT): (I) EACH PARTY'S ENTIRE LIABILITY FOR ALL DAMAGES INCURRED BY THE OTHER PARTY SHALL IN NO EVENT, IN THE AGGREGATE, EXCEED <b>THREE TIMES THE FEES PAID BY CUSTOMER TO VENDOR</b> REGARDLESS OF WHETHER THE ACTION OR CLAIM FOR DAMAGES IS BASED IN CONTRACT, MISREPRESENTATION, WARRANTY, INDEMNITY, NEGLIGENCE, STRICT LIABILITY OR OTHER TORT OR OTHERWISE; AND (II) IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY OR TO ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL OR EXEMPLARY DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF DATA, GOODWILL, PROFITS, INVESTMENTS, USE OF MONEY OR USE OF FACILITIES; INTERRUPTION IN USE OR AVAILABILITY OF DATA; STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS), EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ARISING OUT OF (i) THE PERFORMANCE OR NON-PERFORMANCE OF THIS AGREEMENT, THE SOFTWARE OR ANY SERVICES, OR (ii) ANY CLAIM, CAUSE OF ACTION, BREACH OF CONTRACT OR ANY EXPRESS OR IMPLIED WARRANTY, UNDER THIS AGREEMENT OR OTHERWISE, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY, OR OTHER TORT.</p>	
<b>HIE PARTICIPATION AGREEMENT</b>	
<p><b>HIE Policies and Procedures.</b> HIE shall develop policies and procedures that describe (i) management, operation and maintenance of the HIE Network; (ii) qualifications, requirements and activities of Participants when exchanging information with other HIE Participants using the HIE Network; and (iii) support of the HIE Participants ("HIE Policies and Procedures"). <b>Prior to approving any new, amended, repealed or replaced HIE Policies and Procedures, HIE shall solicit and consider comments from all HIE Participants and HIE Users, on the new, amended, repealed or replaced HIE Policies and Procedures. HIE will review and consider all comments that it receives from HIE Participants and HIE Users as it finalizes and adopts new, amended, repealed or replaced HIE Policies and Procedures.</b> HIE will use its best efforts to provide notice of such amendments to Participant prior to the effective date of any such amendments and make all HIE Policies and Procedures available at <u>[fill in URL]</u>. HIE shall comply with the HIE Policies and Procedures for operation of HIE, as amended from time to time.</p>	
<p><b>Privacy and Security Generally.</b> HIE is <del>committed to</del><u>responsible for</u> safeguarding the privacy and security of the patient information available or exchanged through HIE. To comply with its obligations as a Business Associate of Participant (and other Covered Entities) and its obligations under the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), HIE has created</p>	



robust privacy and security policies and procedures to govern the use of HIE. These privacy and security policies are part of the HIE Policies and Procedures, **as amended from time to time**. HIE and Participant hereby agree to comply with the HIE Policies and Procedures at all times.

**Data Breach.** HIE ~~is committed to operating~~shall operate in a manner that ~~promotes~~safeguards the privacy and security of the Patient Data transacted through HIE. HIE recognizes that Participant shares this commitment and has methods in place to protect the privacy and security of the Patient Data for which it is responsible. This Agreement contains a specific definition of the term Breach so that it is relevant to the activities of HIE. Participant agrees that as soon as possible after experiencing a Breach, Participant will notify the HIE System Administrator. Such notification will include: (a) one or two sentence description of the Breach; (b) description of the roles of the people involved in the Breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.); (c) the type of information that was Breached; (d) other HIE Participants likely impacted by the Breach; (f) number of individuals or records impacted/estimated to be impacted by the Breach; (g) actions taken by the Participant to mitigate the Breach; (h) current status of the Breach (under investigation or resolved); (i) corrective action taken and steps planned to be taken to prevent a similar Breach.

In accordance with Section XX, Participant will cooperate with HIE in the full investigation of all Breaches. Participant shall also supplement the information provided pursuant to Section XX as it becomes available.

Nothing in this Section shall be deemed to relieve or supersede Participant's obligations (if any) under relevant security incident, breach notification or confidentiality provisions of applicable law.

**Key Allocation of Responsibilities and Risks.**

**Reliance on a System.** Participant acknowledges and agrees that HIE has not and will not confirm the accuracy of any information available through HIE. The parties agree that HIE merely receives such data from HIE Participants and HIE Users and therefore shall not be held responsible by Participant for any quality issues, including negligence, detrimental reliance or any other theory other than to the extent that the nature and content of the information is affected by the HIE's performance or failure to perform its responsibilities under this Agreement. Participant shall be solely responsible for ensuring appropriate use by Participant and Participant Users of such data. The contents of this Section shall be communicated to Participant Users through the execution of Terms of Use pursuant to Section 9 of this Agreement.

**Assumption of Risk for Acts and Omissions.** Except to the extent the HIE has made an express warranty, Participant assumes the sole risk, liability and responsibility for: (a) the accuracy and completeness of the Participant Patient Data, User List, Data Maps and Submissions in the form and with the content it provides to HIE and/or other HIE Participants and HIE Users; (b) the performance of Participant Information Systems; (c) connectivity between the Interface and Participant Information Systems, if applicable; (d) the transmission of the Patient Data, User List, Data Maps and Submissions through the Interface, if applicable, other than to the extent that the transmission is affected by the HIE's

performance or failure to perform its responsibilities under this Agreement; (e) all use by Participant and its Users of HIE including, but not limited to, creation by them of Submissions other than to the extent that the transmission is affected by the HIE's performance or failure to perform its responsibilities under this Agreement; (f) all publication, disclosure, copying and use by Participant and Participant Users of information available through HIE; (g) the receipt or non-receipt of information based on the filters established by Participant pursuant to Section XX, other than to the extent that the transmission is affected by the HIE's performance or failure to perform its responsibilities under this Agreement and (h) all interpretation of Patient Data, Submissions, results and reports available through HIE and advising of patients other than to the extent that the interpretations are made on the basis of Participant data, User Lists and Data maps that are affected by HIE's performance or failure to perform its responsibilities under this Agreement

**Accuracy of Patient Data.** HIE hereby warrants and represents to Participant that all Patient Data it transmits on behalf of Participant through the HIE is and an accurate reproduction of the information sent by the Participant. Except for translating the information based on the data maps provided by Participant and the HIE Participant receiving the information, HIE has not altered the information in any way.

**Indemnification by Participant.** Participant will indemnify and hold HIE and its employees, agents, subcontractors and licensors harmless from and against any and all liability (including reasonable attorney's fees), injury or damage that is occasioned through use of the HIE Network by any of Participant or Participant Users, except to the extent such liability, loss, damage, cost or expense is caused by HIE's breach of this Agreement, negligence, gross negligence or willful misconduct.

**Availability of HIE.** Participant acknowledges and agrees that because HIE: (a) is accessed over the Internet, (b) relies, in part, on the existence and proper operation of equipment and software that is outside of the control of HIE, and (c) relies on access to information from, and the provision of information controlled by, third parties, HIE makes no guarantee as to the availability or accessibility of HIE, Patient Data, User List, Data Maps or Submissions at any particular point in time.

**Patient Care.** Participant, its employees, agents and Participant Users shall be solely responsible for all decisions involving patient care, utilization management and quality management for its patients, and the failure to act in regard to the patients other than to the extent that the decisions are affected by Participant data, User Lists and Data maps that are affected by the HIE's performance or failure to perform its responsibilities under this Agreement.

**Electronic Results and Reports Delivery.** For those results and reports that HIE delivers through an Interface directly into an HIE Participant's EMR, HIE hereby represents and warrants that the results and reports are an accurate reproduction of the results and reports given to HIE by the HIE Participant that performed the services reflected in the results or report. HIE further represents and warrants that it has accurately mapped the results and reports to the HIE User who ordered the test and to the patient who was the subject of the test, but only to the extent that such HIE User (or the HIE Participant with whom the ordering HIE User is associated) has provided to HIE accurate and complete Data Maps in accordance with this Agreement, and the results and reports HIE receives from the HIE Participant that performed the services reflected in the results or reports contain accurate information regarding the

ordering HIE User and patient who was the subject of the test. HIE does not make any other representations or warranties about such results and reports including the clinical accuracy, completeness or correctness of the results and reports.

**Carrier Lines.** The parties acknowledge that access to HIE is provided over various facilities and communications lines, and information shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, “carrier lines”) owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the parties’ control. Provided the parties use reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this Agreement and the HIE Policies and Procedures, neither party assumes any liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted over those carrier lines, which are beyond the party’s control, or any delay, failure, interruption, interception, loss, transmission, or corruption of any information attributable to transmission over those carrier lines which are beyond the party’s control. Use of the carrier lines is solely at Participant’s risk and is subject to all Applicable Law.

**Warranty Pertaining to HIE Network Performance.** HIE warrants, represents and covenants that the HIE Network will be free from programming errors that materially and adversely affect their operation (a “Material Defect”). If any component of the HIE Network contains a Material Defect, Participant shall notify HIE of such Material Defect, and HIE shall, at no additional charge to Participant: (i) promptly investigate and determine the cause of such Material Defect; and, (ii) use commercially reasonable efforts to promptly address and provide a correction for such Material Defect.

**Warranty Pertaining to Malware.** HIE warrants, represents and covenants that the HIE Network have been tested by HIE and will not introduce any viruses, worms, unauthorized cookies, trojans, trap doors, back doors, timers, clocks, counters, malicious software, “malware,” or other program, routine, subroutine, or data which is designed to or which will disrupt the proper operation of the HIE Network or any hardware, software or data used by Participant, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the HIE Network or any hardware, software or data used by Participant, to be improperly accessed, destroyed, damaged, erased or otherwise made inoperable. Notwithstanding the foregoing, HIE does not make any representations or warranties regarding the information that Participant receives from other HIE Participants and HIE Users through the HIE Network other than to the extent that the nature and content of the information is affected by the HIE’s performance or failure to perform its responsibilities under this Agreement.

**DISCLAIMER OF WARRANTIES.** EXCEPT FOR THE EXPRESS WARRANTIES CONTAINED IN THIS AGREEMENT, HIE MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, IN FACT OR IN LAW AS TO ANY MATTER WITH RESPECT TO HIE, THE HIE SYSTEM COMPONENTS, THE DOCUMENTATION OR ANY SERVICES PROVIDED BY HIE UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, TRAINING, DATA MANAGEMENT, SUPPORT, ELECTRONIC RESULTS AND REPORTS DELIVERY OR ANY OTHER SERVICES PROVIDED UNDER THIS AGREEMENT. EXCEPT FOR THE EXPRESS WARRANTIES CONTAINED IN THIS AGREEMENT, THERE IS NO WARRANTY THAT THE INFORMATION AVAILABLE THROUGH HIE IS TRUE, COMPLETE, CORRECT, OR ERROR-

<p>FREE, VIRUS-FREE OR UNINTERRUPTED. EXCEPT AS SET FORTH HEREIN, HIE SPECIFICALLY DISCLAIMS ANY AND ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, FREEDOM FROM INFRINGEMENT AND ANY IMPLIED WARRANTIES ALLEGEDLY ARISING FROM TRADE USAGE OR COURSE OF DEALING. HIE IS NOT AN ELECTRONIC HEALTH RECORD NOR IS IT INTENDED TO REPLACE ANY OFFICIAL MEDICAL RECORDS MAINTAINED BY PARTICIPANT. HIE DOES NOT WARRANT AND WILL NOT BE LIABLE FOR THE INTERPRETATION OF ANY OF THE INFORMATION AVAILABLE THROUGH HIE OR FOR ANY USE OF HIE BY PARTICIPANT OR PARTICIPANT USERS. ANY SUCH INTERPRETATIONS OR DECISIONS RESULTING THEREFROM ARE AT THE SOLE RISK OF PARTICIPANT AND PARTICIPANT USERS. HIE SHALL HAVE NO LIABILITY WHATSOEVER FOR PATIENT DATA, INCLUDING WITHOUT LIMITATION ITS INTEGRITY AND QUALITY WHILE SAME ARE IN THE POSSESSION AND CONTROL OF PARTICIPANT. HIE MAKES NO REPRESENTATION OR WARRANTY WHATSOEVER CONCERNING SUBMISSIONS TO HIE. HIE MAKES NO REPRESENTATIONS OR WARRANTY WHATSOEVER CONCERNING THE COMPATIBILITY OF THE INTERFACE, THE INTERFACE'S EFFECT ON PARTICIPANT'S COMPUTER NETWORK, PARTICIPANT CLINICAL SYSTEMS OR INDIVIDUAL SYSTEMS.</p> <p><b>DISCLAIMER OF INCIDENTAL, SPECIAL AND CONSEQUENTIAL DAMAGES.</b> HIE SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR ECONOMIC LOSS ARISING OUT OF OR IN CONNECTION WITH THE DELIVERY, USE OR PERFORMANCE OF HIE, THE HIE SYSTEM COMPONENTS, OR THE DOCUMENTATION BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY IN TORT OR ANY OTHER LEGAL THEORY, EVEN IF HIE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, REVENUE, EQUIPMENT USE, DATA OR INFORMATION OF ANY KIND.</p> <p><b><u>Liability Cap.</u></b> HIE's maximum liability for damages for all matters arising out of or relating to this Agreement is the limit of any applicable insurance policy.</p>	
<p><b>Support Services.</b> HIE will provide services to support Participant's use of the HIE Network including, but are not limited to, the management and control of the Participant Agent, the Master Participant Directory, the HIE Rendezvous Agent, the HIE Grid, Interfaces and Connected Datastages. HIE will provide these support services pursuant to the HIE Policies and Procedures.</p>	<p>Very open-ended. Policies and procedures can be changed from time to time by the HIE.</p>
<p><b><u>Participant Responsibilities - General.</u></b></p> <p><b>Use of HIE.</b> Participant desires to use the HIE Network to engage in the types of exchange transactions indicated in Exhibit X. Participant shall only use the HIE Network to exchange Patient Data for a Permitted Purpose in accordance with this Agreement.</p>	

**Subsequent Use of Information.** HIE will not maintain a designated record set on behalf of Participant. Participant may retain, use and re-disclose information that it receives from another HIE Participant through the HIE Network in accordance with Applicable Law and Participant's record retention policies and procedures. If Applicable Law requires that Participant obtain a patient consent or Authorization before it uses or re-discloses information that Participant received through the HIE Network, then it is the responsibility of Participant to obtain this consent or Authorization prior to such use or re-disclosure.

**Restricted Use of HIE Network.** Participant shall use the HIE Network exclusively to exchange Patient Data with other HIE Participants, HIE Users and others as permitted by HIE, and for no other purpose, unless another purpose is approved in writing by HIE and Participant. Neither Participant nor its Participant Users shall use the HIE Network nor any data or information obtained through the HIE Network for any purposes contrary to local, state and federal laws and regulations.

**Duties of Participant when Disclosing Information through HIE.** Whenever Participant or Participant Users send, and thereby disclose, Patient Data to another HIE Participant or User, Participant is responsible for ensuring that such information is being disclosed for a Permitted Purpose; is being disclosed by a Participant User who has the requisite authority to do so; and is supported by appropriate legal authority for disclosing such information including, but not limited to, any consent or Authorization, if required by Applicable Law; and is properly addressed to the intended HIE User recipient.

**Participant Established Filters.** Participant may have the ability to establish filters that will operate to prevent certain information from being delivered to Participant or Participant Users through the HIE Network. Participant is solely responsible for establishing these filters.

**Malicious Software.** In providing Patient Data, User List, or Data Maps to HIE or the HIE Network, Participant will take reasonable steps to ensure that the medium containing same does not include, and that any method of transmitting such data will not introduce, any viruses, worms, unauthorized cookies, trojans, malicious software, "malware," or other program, routine, subroutine, or data designed to disrupt the proper operation of the HIE Network or any part thereof or any hardware or software used by HIE, an HIE Participant or HIE User in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the HIE Network or any part thereof or any hardware, software or data used by HIE, an HIE Participant or a HIE User in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable.

**Equipment, Software and Connectivity.** Except as otherwise set forth herein, Participant shall be responsible for procuring and configuring the hardware, software and connectivity necessary for Participant and Participant Users to effectively exchange information through the HIE Network as specified in Exhibit X. **HIE may make reasonable changes to such specifications from time to time in its sole discretion and will provide Participant not less than one hundred eighty (180) days notice of any such change.**

**Compliance with Policies and Procedures.** Participant shall comply and cause Participant Users to comply with all HIE Policies and Procedures that apply to use of the HIE Network to exchange information with other HIE Participants, which are incorporated herein and may be amended from time to time in accordance with Section 9.8. HIE will make all HIE Policies and Procedures available at

www.xxxxx.com.

**Auditing.** Participant shall monitor and audit all access to and use of its Participant Information System related to this Agreement, for system administration, security, and other legitimate purposes. Based on the results of its monitoring and auditing activities, Participant shall attest to compliance with this Agreement and HIE Policies and Procedures as provided in HIE Policies and Procedures.

**Minimum Level of Participation.** Participant shall be required to use the HIE Support Services in connection with its use of the HIE Network. Participant shall also be required to use the HIE Network to send information to and receive information from other HIE Participants and HIE Users as generally described in this Agreement. This means that a Participant shall, at least, receive any results, reports or orders for clinical services that are sent through the HIE Network for Treatment purposes unless to do so would violate Applicable Law or HIE has agreed otherwise in writing.

HIE and Participant recognize that Participant's participation is dependent, in part, on facts and circumstances which are peculiar to Participant, such as organizational structure and the existence of other contractual relationships. As a consequence, Participant's level of participation will be periodically evaluated by HIE and discussed by HIE with Participant. If, in the reasonable opinion of HIE, Participant's participation is not acceptable, then, in that event, HIE may act pursuant to Section 19.4 to summarily suspend Participant's and Participant User's ability to use the HIE Network. If an appropriate plan of correction cannot be timely established by HIE and Participant following Participant's suspension, HIE may act under Section XX to terminate this Agreement and Participant's right to use the HIE Network.

**Participant Responsibilities for Interfaces.**

The following terms only apply if and when Participant creates an Interface between Participant Information Systems and the HIE Network.

**Provision of Patient Data through an Interface.** To the extent not prohibited by state and federal laws, rules and regulations, if Participant elects to use an Interface to exchange information through the HIE Network, all Patient Data transmitted through an Interface shall be in a standard format agreed upon by the parties, and comply with the HIE Policies and Procedures, as amended from time to time.

**Data Maps.** Participant shall provide Data Maps, which are true, accurate, complete, current, in a standard format agreed upon by the parties, and which comply with the HIE Policies and Procedures, as amended from time to time. Participant acknowledges that HIE is relying upon these Data Maps to correctly deliver its services. At least 180 days prior to Participant implementation of changed, amended, updated or newly created Data Maps, Participant shall provide written notice to HIE of such changes, amendments, updates or creation, which shall include the specific details of such changes, amendments, updates or creation. Notwithstanding any rights granted herein to HIE to suspend Participant's access to the HIE Network, Participant agrees that it shall provide Data Maps in accordance with this Section.

**Connectivity to HIE.**

Participant shall be responsible for maintaining the physical connectivity of Participant Information

Systems to the Interface in accordance with the requirements set forth in Exhibit X. HIE shall be responsible for maintaining the HIE Network's ability to receive secure transmissions from Participant Information Systems, as applicable, to the extent that Participant is maintaining physical connectivity in accordance with this Section.

**HIE Responsibilities.**

**Use of HIE Network.** HIE will provide Participant with access and a right to use the HIE Network to exchange health information in accordance with this Agreement and to engage in the type(s) of exchange transaction(s) specified in Exhibit X. The specific technical components of the HIE Network that will be provided by HIE to Participant pursuant to this Agreement are set forth in the HIE Policies and Procedures.

**Electronic Results and Reports Delivery.** For those results and reports that HIE delivers through an Interface directly into an HIE Participant's EMR, HIE hereby represents and warrants that the results and reports are an accurate reproduction of the results and reports given to HIE by the HIE Participant that performed the services reflected in the results or report. HIE further represents and warrants that it has accurately mapped the results and reports to the HIE User who ordered the test and to the patient who was the subject of the test, but only to the extent that such HIE User (or the HIE Participant with whom the ordering HIE User is associated) has provided to HIE accurate and complete Data Maps and the results and reports HIE receives from the HIE Participant that performed the services reflected in the results or reports contain accurate information regarding the ordering HIE User and patient who was the subject of the test. **HIE does not make any other representations or warranties about such results and reports including the clinical accuracy, completeness or correctness of the results and reports.**

**Expanded Capabilities.**

*General.* As electronic health information exchange capabilities continue to evolve, HIE may expand the types of information exchange activities that can be supported by the HIE Network. **Such expansion may impact the way that Participant's Patient Data is used or disclosed,** or may expand the reasons for which HIE Users or others authorized by HIE may access information through the HIE Network. At least sixty (60) days prior to enabling a new type of information exchange activity, HIE will provide notice to Participant of such new activity.

*Testing New Information Exchange Activities.* Before making new information exchange activities available to all HIE Participants and HIE Users, HIE will need to test the capabilities. To do so, HIE will likely be required to use de-identified patient information. Participant hereby agrees to allow HIE to de-identify its Patient Data, in accordance with the HIPAA Regulations and the Business Associate Agreement, and use such de-identified information for purposes of testing new information exchange activities and capabilities of the HIE Network.

**Training Services.** HIE shall provide to Participant Users training services to help enable Participant Users to effectively utilize the HIE Network.

**Maintenance and Support.** HIE shall provide the Support Services and a Help Desk to support

Participant's and Participant Users' use of the HIE Network in accordance with the HIE Policies and Procedures, as amended from time to time.

**Implementation Services.** HIE shall provide to Participant services to assist the Participant with implementing those technical components provided to Participant by HIE that are required to enable Participant to exchange information through the HIE Network.

**Monitoring/Audit.**

*Monitoring and Auditing HIE.* HIE, through its agents, employees and independent contractors, shall, for system administration, security, and other legitimate purposes, monitor and audit all access to and use of the HIE Network and the content of any data or messages communicated to, from or through the HIE Network, or stored on any component of the HIE Network, in accordance with the HIE Policies and Procedures, as amended from time to time.

*Monitoring and Auditing Participant.* HIE shall have the right to conduct such audits of Participant's facilities, data and records as it reasonably determines to be necessary to verify that Participant is in compliance with the terms and conditions of this Agreement, only during business hours, organized so as to not unreasonably disrupt Participant's business operations. HIE shall provide reasonable advance notice to Participant prior to any such inspection or audit, unless such advance notice, in HIE's opinion, would prejudice HIE's ability to ascertain the information desired from the inspection or audit. Participant shall cooperate with and provide such assistance as HIE shall reasonably require in connection with any such inspections and audits, including by making Participant Users and other Participant personnel available to HIE.

**HIE Policies and Procedures.** HIE shall develop policies and procedures that describe (i) management, operation and maintenance of the HIE Network; (ii) qualifications, requirements and activities of Participants when exchanging information with other HIE Participants using the HIE Network; and (iii) support of the HIE Participants ("HIE Policies and Procedures"). HIE will use its best efforts to provide notice of such amendments to Participant prior to the effective date of any such amendments and make all HIE Policies and Procedures available at [www.xxx.com](http://www.xxx.com). HIE shall comply with the HIE Policies and Procedures for operation of HIE, as amended from time to time.

**Professional Responsibility and Clinical Content Disclaimer.**

CUSTOMER ACKNOWLEDGES AND AGREES THAT ANY CLINICAL CONTENT FURNISHED BY VENDOR HEREUNDER (WHETHER SEPARATELY OR INCLUDED WITHIN A PRODUCT) IS AN INFORMATION MANAGEMENT AND DIAGNOSTIC TOOL ONLY AND THAT ITS USE CONTEMPLATES AND REQUIRES THE INVOLVEMENT OF TRAINED INDIVIDUALS. CUSTOMER FURTHER ACKNOWLEDGES AND AGREES THAT VENDOR HAS NOT REPRESENTED ITS PRODUCTS AS HAVING THE ABILITY TO DIAGNOSE DISEASE, PRESCRIBE TREATMENT, OR PERFORM ANY OTHER TASKS THAT CONSTITUTE THE PRACTICE OF MEDICINE. THE PARTIES AGREE THAT, AS BETWEEN CUSTOMER AND VENDOR, CUSTOMER IS RESPONSIBLE FOR THE ACCURACY AND QUALITY OF



CUSTOMER DATA AS INPUT INTO THE PRODUCTS. CUSTOMER ACKNOWLEDGES THAT VENDOR: (A) HAS NO CONTROL OF OR RESPONSIBILITY FOR THE CUSTOMER'S USE OF THE CLINICAL CONTENT, AND (B) HAS NO KNOWLEDGE OF THE SPECIFIC OR UNIQUE CIRCUMSTANCES UNDER WHICH THE CLINICAL CONTENT PROVIDED MAY BE USED BY THE CUSTOMER. THE PARTIES AGREE THAT VENDOR DOES NOT PROVIDE MEDICAL SERVICES TO PATIENTS AND IS NOT ENGAGED IN THE PRACTICE OF MEDICINE, AND THAT CUSTOMER'S USE OF THE PRODUCTS DOES NOT ABSOLVE THE CUSTOMER OF ITS OBLIGATION TO EXERCISE INDEPENDENT MEDICAL JUDGMENT IN RENDERING HEALTH CARE SERVICES TO PATIENTS. CUSTOMER ACKNOWLEDGES THAT THE PROFESSIONAL DUTY TO THE PATIENT IN PROVIDING HEALTHCARE SERVICES LIES SOLELY WITH THE HEALTHCARE PROFESSIONAL PROVIDING THE SERVICES. VENDOR MAKES NO WARRANTY AS TO THE NATURE OR QUALITY OF THE CONTENT OF RESULTS, MESSAGES OR INFORMATION SENT BY CUSTOMER, OR ANY THIRD PARTY USERS OF THE SUBSCRIPTION SERVICES. **NOTWITHSTANDING THE FOREGOING, NOTHING CONTAINED IN THIS SECTION XX RELIEVES VENDOR OF ITS OBLIGATION TO PROVIDE AND IMPLEMENT THE SOFTWARE AND SERVICES IN A MANNER THAT MEET THE WARRANTIES SET FORTH IN THIS MASTER AGREEMENT.**

**BUSINESS ASSOCIATE AGREEMENT CORRESPONDING TO HIE PARTICIPATION AGREEMENT**

**Privacy and Security Obligations.** Consistent with Section 13404(a) of the HITECH Act, Business Associate agrees that the requirements of the HITECH Act that relate to privacy and security and are made applicable with respect to Participant shall also be applicable to Business Associate, and are hereby incorporated into and made a part of this Business Associate Addendum. Without limitation, Business Associate agrees that: (a) Section 13401(a) of the HITECH Act causes 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 to apply directly to Business Associate in the same manner that such sections apply to Participant; and (b) Section 13404(a) of the HITECH Act causes the provisions of 45 C.F.R. § 164.504(e) governing use and disclosure of PHI to apply directly to Business Associate in the same manner that such section applies to Participant.

The Parties acknowledge that certain provisions included in the HITECH Act are expected to become effective in the future, and the Parties expect the Secretary to promulgate and publish additional rules in the future under the authority granted by the HITECH Act. Business Associate will comply with the applicable provisions of the HITECH Act and the future rules promulgated thereunder upon their respective effective dates, and this Business Associate Addendum hereby incorporates the requirements contained in those provisions without the need for further amendment of this Business Associate Addendum.

**CLOUD COMPUTING/HOSTING AGREEMENTS**

**EXAMPLE 1**

**Data Security Audits and Certification.**

**Vendor Security Assessments.** Vendor shall perform commercially reasonable vulnerability scans and penetration testing on the System and Services at least once per month and implement reasonable corrective action to address any risks or vulnerabilities to the security of Customer Data identified by such scans and testing. Vendor shall deliver evidence of the scans, testing and any corrective action to Customer within three business days of completing the scans and testing.

<p><u>Security Assessment of Hosting Sites.</u> If requested by Customer, Vendor shall arrange for Customer (or Customer's authorized agent or contractor) to conduct an assessment of the adequacy of the technical, physical and administrative safeguards in place at any Hosting Site (or prospective Hosting Site) either on site at the Hosting Site or by telephonic interview of a Hosting Site representative with knowledge of the Hosting Site's safeguards and other security measures within 30 days of Customer's request on a date and at a time reasonably acceptable to Customer.</p> <p><u>Security Breaches at Third-Party.</u> If Vendor becomes aware of a Breach (as defined by HIPAA) or Security Incident (as defined by HIPAA) involving Customer Data maintained or transmitted by a third party Hosting Site, Vendor shall notify Customer in accordance with Section 2.2 of the Business Associate Agreement.</p> <p><u>Data Security Audits.</u> Vendor acknowledges and agrees that Customer audit personnel and examiners and representatives of regulatory agencies with jurisdiction over Customer, shall have the right to conduct security risk assessments and other examinations and inspections, upon reasonable written notice, of Vendor's financial records, facilities, procedures, technology security policies and procedures and such other documentation pertaining to Vendor's provision of Services under this Agreement. Vendor may require such persons to provide reasonable evidence of their authority before being admitted to Vendor's facilities. Vendor shall preserve for a period of six (6) years after the completion or termination of services under this Agreement all documents related to the Services hereunder which shall be made available to Customer at Customer's request.</p>	
<p><b><u>Peer Review Information.</u></b></p> <p>Vendor acknowledges and agrees that (1) Customer and other providers participating in an Integrated Delivery Network or similar accountable care-type organization ("<b>Care Network</b>") may establish one or more Peer Review Organizations to gather and review information relating to the care and treatment of patients in furtherance of the purposes described at [insert applicable state peer review statute cite]; and (2) Vendor assists in the performance of peer review activities at the direction of the applicable Peer Review Organization when it receives and maintains information from the applicable Peer Review Organization, and when it uses Customer Data to create analyses, reports, information and other work product at the request or for the purposes of the Review Organization (as set forth in [insert applicable state peer review statute cite] ("<b>Peer Review Organization Information</b>") pursuant to this Agreement. To the maximum extent permitted by law, all Vendor work product shall be deemed to be Peer Review Organization Information, and shall be confidential, privileged and immune from subpoena, discovery or use in any civil action or other litigation, or for any purpose except as permitted by [insert applicable state peer review statute cite]. No provision of this Agreement shall constitute a waiver of the peer review confidentiality protections or peer review immunity under [insert applicable state peer review statute cite].</p> <p>Without limiting the foregoing, all analyses, reports, information and other work product created by Vendor and any requests for such work product shall be treated as Peer Review Organization Information unless Customer or the applicable Peer Review Organization advises Vendor in writing that</p>	

the work product or request for work product is not Peer Review Organization Information. Vendor shall mark each page of all Peer Review Organization Information pursuant to this Agreement as “Confidential Peer Review Information Protected under [insert applicable state peer review statute cite]. Do not duplicate or redistribute without written permission.” Vendor shall maintain all Peer Review Organization Information (whether in electronic or paper form) separate from Customer Data used to create the Peer Review Organization Information. All requests for access to or disclosures of Peer Review Organization Information shall be submitted to the applicable Peer Review Organization for approval of such access or disclosure. Vendor shall hold all Peer Review Organization Information confidential, and may disclose or provide access to Peer Review Organization Information only with the specific written approval or according to the written instructions of the applicable Peer Review Organization. Vendor shall maintain a log of any disclosures of any Peer Review Organization Information to Customer, other Authorized Users or third parties.

If Vendor receives a subpoena or other discovery request for any reports, analysis or other Peer Review Organization Information, Vendor shall provide prompt written notice to Customer and the applicable Peer Review Organization in accordance with Section XX so that Customer and/or the applicable Peer Review Organization may assert the confidentiality requirements limitations on discovery and admissibility pursuant to [insert applicable state peer review statute cite] or seek other appropriate remedy. Vendor shall cooperate with Customer’s efforts to prevent discovery of Peer Review Organization Information.

**EXAMPLE 2**

**Vendor Infrastructure and Systems.**

Cloud. Vendor shall provide Customer with a web-based infrastructure and system, key components of which include, without limitation, software, hardware, connectivity, and Data Centers (, by which the Services will be rendered to Customer is collectively referred to herein as the “**Vendor Cloud**”. Vendor shall ensure that the Vendor Cloud shall enable Customer and/or Customer Members to upload or transmit Customer Data to the Vendor Cloud, but allow only Customer (and its Authorized Users) to view, retrieve, display or otherwise access or use such Customer Data. “**Authorized Users**” shall include Customer employees, agents, and other users as Customer designates to be permitted t access the Vendor Cloud on behalf of Customer.

Internet Access. Vendor shall enable Customer access to the Vendor Cloud through the Vendor website. The “**Vendor Site**” means the Vendor website located at [**web address**]. Vendor shall provide Customer and its Authorized Users with unique log-in codes or other means by which Customer can securely access its Customer Data through a private portal on the Vendor Site (“**Portal**”). Vendor shall identify in advance (prior to Go Live and as part of the SOW) those programs and/or physical requirements necessary for Customer to access the Vendor Cloud.

Data Centers. All Customer Data shall be maintained on secure servers located in at least two data

centers owned, operated and controlled by Vendor and physically located within the United States (each, a “**Data Center**”). The primary Data Center in which the primary server resides shall be located at [Address, City, State] (“**Primary Data Center**”). As part of Vendor’s Services, Vendor shall ensure that redundant mirrored image copies of the Customer Data shall simultaneously reside in a backup server physically located in another Data Center which shall be located at [Address, City, State] (“**Back-Up Data Center**”). Vendor represents and warrants that the Data Centers (including both the Primary Data Center and the Back-Up Data Center) are located within the United States, are Vendor-owned, operated and controlled, and that under no circumstances will Customer Data be transmitted or transported to or from any location outside of the United States.

Hosting Services. Vendor will provide the hosting services to enable Customer to access the Vendor Cloud remotely through the Portal (“**Hosting Services**”) in accordance with the requirements, applicable specifications, documentation and service level standards as set forth in **Exhibit A** (collectively, “**Service Levels**”). As part of the Hosting Services and as further described in this MSA, Vendor shall: (a) procure and maintain the infrastructure (including hardware, software, networks, connectivity, tools and other resources) reasonably necessary to host and provide the Vendor Cloud at the Service Levels, in accordance with the requirements of this MSA; and (b) Vendor shall ensure that Customer Data is logically segregated from all other Vendor data, including its other customers’ data, and shall secure and restrict access to Customer Data solely to Customer and its Authorized Users.

Service Levels; Uptime; Access Speed. Vendor shall (i) ensure that the Vendor Cloud is available 24 hours a day, 7 days a week, 365 days a year ([100]% Uptime), with instantaneous access and retrieval (defined as having a maximum response time of [3] seconds from query (“**Access Speed**”)) except for: (i) planned downtime (of which Vendor shall give at least 48 hours notice to Customer and which Vendor shall schedule, to the extent practicable, during the weekend hours); or (ii) any unavailability caused by circumstances beyond Vendor’s reasonable control and which cannot be prevented or mitigated by Vendor’s disaster recovery plan, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving its employees), or Internet failures or delays not within Vendor’s control, and provide the Vendor Cloud only in accordance with applicable laws and government regulations. In the event of Vendor’s failure to comply with the requirements of this Section, Customer may, at its option, (a) obtain from Vendor a pro-rated refund of the affected monthly Service costs or a credit, at its option, for the time such service levels were not maintained, or (b) terminate this Agreement.

Audits Trails. Vendor shall maintain a complete audit trail of all actions taken in connection with or resulting from the provision of Services under this Agreement, including all financial statements and other financial reporting documents, standard operating procedures, change management records, and other information, records and documentation relating to the Services and Vendor’s performance thereof (collectively, “**Records**”). Such Records shall be designed to enable a third party to readily determine whether Vendor has complied with all Laws, including but not limited to HIPAA, as well as all obligations imposed upon Vendor by this Agreement.

Vendor Personnel.

Vendor Personnel; No Outsourcing. Vendor shall employ individuals to enable Vendor to perform the Services required hereunder, (“**Vendor Personnel**”). Vendor shall not outsource any of its obligations under this MSA to any third party, including but not limited to its data hosting obligations, without the express written consent of Customer. Customer shall bear no responsibility for any Vendor Personnel, and none of Customer’s obligations to Vendor shall extend to Vendor Personnel. Vendor shall be directly responsible for all Services performed under this Agreement and shall require Vendor Personnel to comply with the terms of this Agreement.

Background Checks. Vendor shall perform background checks of employees assigned to provide Customer Services or those employees that will have access to Customer Data or Customer or Customer Members’ premises. Such background checks shall include checks of criminal records related to theft, embezzlement, identity theft, piracy, computer hacking, or any other form of cybercrime. In the event that Customer is dissatisfied on reasonable grounds with any Vendor personnel assigned to provide Services to Customer, Vendor shall replace such Vendor personnel as quickly as reasonably practicable. Customer may immediately require removal from performance of any Services for Customer any Vendor Personnel if such personnel violates Vendor’s code of conduct, or Customer’s reasonable policies made known to Vendor in writing, such as security policies or confidentiality obligations, or if such personnel engages in any act or omission that threatens any person or property. Notwithstanding the above, only Vendor employees that have a “need to know” Customer Data for purposes of Vendor’s performances of the Services shall have access to Customer Data.

Data Privacy and Security Policies and Procedures; Training. Vendor shall maintain written policies consistent with the obligations imposed by this Agreement, with respect to the proper management of Customer Data by Vendor Personnel. Vendor shall institute a disciplinary process to take punitive measures, up to and including dismissal, against any Vendor Personnel that violate this policy. Vendor shall specifically train all Vendor Personnel that will handle Customer Data with respect to the proper handling of Customer Data and the data privacy, data security, and confidentiality obligations imposed under Laws applicable to Vendor and this Agreement.

SAS 70 Type II Certified. Vendor warrants and represents that it is a SAS 70 Type II certified organization and will maintain such SAS 70 Type II certification throughout the term of this MSA. Vendor further warrants and represents that all Data Centers used to host Customer Data are certified as the highest tier storage facilities under current industry standards.

Segregation, Protection and Return of Data. Vendor shall : (i) segregate all Customer Data from that of any other client; and (ii) establish and maintain procedures, systems, processes and controls intended to prevent the unauthorized access, use, disclosure, destruction, loss or alteration of any Customer Data in the possession or control of Vendor or any of its personnel, or while transmitted or transported by Vendor (or any of its personnel) to or from Customer, including, without limitation technical, administrative, physical and organizational safeguards and security measures, that are no less rigorous than the highest industry standards and practices in the health information technology industries and

otherwise meet the requirements of applicable law, including HIPAA, as amended by the HITECH Act, to (i) protect Customer Data against unauthorized destruction, loss, alteration, access, misuse or disclosure, and (ii) ensure the availability, integrity and confidentiality of Customer Data in the possession of Vendor or its affiliates, contractors and personnel (or to which any of the foregoing has access) during the shipping, transporting, electronic transmission and storage thereof (the “**Data Safeguards**”). Vendor shall promptly remove the Customer Confidential Information and Customer Data at Customer’s request. Vendor shall not modify, delete or destroy any Customer Data or media on which such data resides without prior written authorization from Customer. Failure to properly secure, protect, store or maintain Customer Confidential Information or Customer Data, that results in a corruption, alteration, loss or destruction of such data, or unauthorized access or disclosure of Customer Confidential Information or Customer Data, shall be considered an incurable material breach of this MSA. Upon termination of this Agreement, Vendor shall immediately return all Customer Data to Customer (in a format as requested by Customer), at no charge to Customer.

Compliance with Customer Security Policies. Vendor shall comply with all Customer written data security procedures that are in effect during the term of this Agreement (and as reasonably modified from time to time) for the security of Customer Data and other Customer Confidential Information (as defined herein) and/or Customer data and the requirements that follow. In this respect, and without limiting Vendor’s obligations under this Agreement, Vendor shall employ appropriate methods, including encryption and encrypted devices, and secure communication lines, to secure the privacy and security of Customer Data and to minimize the risk of unauthorized access to the Cloud.

Vendor Customers’ Data Security Compliance. Vendor warrants and covenants that it shall require all of its customers who have access to its Data Centers and the Vendor Cloud to adhere to Vendor’s written security policies and procedures regarding remote electronic access or physical access to a Data Center or the Vendor Cloud. Vendor shall enforce such security policies and procedures and shall take appropriate corrective action against customers who fail to adhere to such security policies and procedures.

Access; Breaches. Vendor will not attempt to access or allow access to Customer Data that is not required for the performance of the Services or otherwise authorized by Customer. Vendor shall notify Customer within twenty-four (24) hours of knowledge of a breach of Customer Data or in the event of any unauthorized use, disclosure, acquisition or access to Customer Data that requires Customer, under applicable federal or state law or in its business judgment, to make a notification to any third party (including, without limitation, to any patient) (a “**Triggering Event**”). To the extent Customer is required to notify any third party, including a patient or a Covered Entity, of such breach, Customer shall have the sole right to make such notification, including determining the content, methods, and means of such notification. Notwithstanding the foregoing, Vendor shall reasonably cooperate with Customer in formulating such notification, but Vendor shall not make any such notification at its own initiative without Customer’s prior written consent. Vendor will pay the costs and expenses of investigation, remediation, notification and penalties to the extent the Triggering Event is caused by the acts or omissions of Vendor or any Vendor Personnel or a material breach of this Agreement by Vendor or any

Vendor Personnel.

Virus Protection. Vendor shall ensure that the Cloud and/or programs used by Vendor in providing the Services are protected against known or suspected Disabling Devices by implementing appropriate processes for detecting, preventing and recovering from virus attacks, including all necessary data and software back-up and recovery tools and arrangements. “**Disabling Devices**” shall mean any software, equipment, tools or data (a) designed or able to disrupt, disable, harm or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the systems, or any software, equipment, tools or data (e.g., “viruses” or “worms”); (b) that would disable the Cloud, the Portal, or Customer’s access to the Customer Data, or impair in any way their operation including, for example, based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral (e.g., “time bombs”, “time locks” or “drop dead” devices); (c) that would permit a third party to access the Cloud, Customer Data, Customer system, or Portal, to cause such disablement or impairment, or otherwise to circumvent the security features of the Cloud or Customer Data hosted by Vendor (e.g., “traps”, “access codes” or “trap door” devices); or (d) which contains any other harmful, malicious or hidden procedures, routines or mechanisms which would cause the Cloud, Customer system, or Portal to cease functioning or to damage or corrupt storage media, software, equipment, tools, data or communications or any part of the Cloud, Customer system, or Portal, or otherwise interfere with operations.

Data Availability and Disaster Recovery Plan. Vendor shall implement a disaster recovery plan (consistent with its SAS 70 Type II certification, and certification as a highest tier data center) to ensure that all Customer Data is preserved for as long as Customer requires such Customer Data to be preserved, and readily available at all times to Customer. The disaster recovery plan shall include the following procedures: Vendor shall ensure that a back up of its systems, including the Customer Data, is conducted daily by Vendor, which at a minimum, shall include daily incremental backups. One copy of backups shall be securely transported or transmitted daily offsite to the Back-Up Data Center (or other location as agreed by Customer), and maintained at Vendor’s expense. Vendor shall ensure that all Customer Data hosted by Vendor is securely stored and preserved on both the Primary and the Back-Up Data Centers and in the event of failure of the Primary Data Center or other interruption of access to the Customer Data, that the redundant copy of such Customer Data can be readily restored, accessible and usable by Customer (from the Back-Up Data Center or other location or means as agreed by the parties), within the Fail-Over Time (“**Fail-Over Time**” means the elapsed time between interruption of access and full recovery of access not to exceed sixty (60) minutes.)

Operational Audits. Upon five (5) business days prior written notice, Customer and its auditors, at Customer’s expense, may conduct operational audits (which will include an external auditor review of Systems and controls) of Vendor’s performance of the Services including, without limitation, copies of or access to the Records, to audit the following: (a) verification that Vendor is in compliance with all its obligations under this Agreement; (b) verification of the Service Levels; (c) auditing and inspecting the conduct of Vendor operations and procedures relating to the Services or the performance of the Services and protection of the Customer Data; (d) auditing the Cloud for continued compliance with the documentation and SAS 70 Type II; and (e) determining whether Vendor is in compliance with Laws

applicable to it and/or to Customer. Vendor shall provide reasonable support and assistance during normal business hours for any such audit(s) to include preparation, pre-audit events and physical access to the applicable Vendor facilities. The foregoing audit may not be unreasonably disruptive to Vendor's business operations. Promptly following an audit, Customer and Vendor shall meet to discuss the findings of the audit and to develop and agree upon an appropriate and effective manner in which to respond to the deficiencies, if any, identified through the audit. Vendor shall resolve any such deficiency or risk in a mutually agreeable timeframe, taking into consideration the urgency of Customer's needs and liabilities to which Customer may be exposed as a result of any delays, but in no event longer than thirty (30) days. Vendor shall bear the cost of any necessary remedial action due to a failure to perform in accordance with this Agreement identified during the audit process in order to bring Vendor into compliance with the terms of this Agreement and any applicable laws.

**Insurance**

General and Professional Liability Insurance. Vendor shall maintain in force during the term of this Agreement such insurance coverage of a kind and in amounts that is commercially reasonable and customary for consultants or firms of Vendor's size and scope and in Vendor's field. Notwithstanding the foregoing, Vendor shall maintain in force during the term of this Agreement general liability insurance and professional liability insurance coverage, each in amounts equal to the greater of: (i) \$1,000,000.00 per claim and \$3,000,000.00 in aggregate, or (ii) amounts that are commercially reasonable and customary for consultants or firms of Vendor's size and scope and in Vendor's field and adequate to meet Vendor's obligations under the foregoing indemnification. Upon request, Vendor shall provide to Customer certificates evidencing the insurance coverage(s) maintained by Vendor. Vendor shall provide Customer with thirty (30) days prior written notice of any change in or cancellation or non-renewal of insurance.

Cyber Insurance. Vendor shall maintain in force during the term of this Agreement Information technology and cyber errors and omissions liability insurance with a combined single limit of not less than \$ 10,000,000.00 in the aggregate. Such coverage shall include but not be limited to, third party liability coverage for loss or disclosure of data, including electronic data, network security failure, unauthorized access and/or use or other intrusions, infringement of any intellectual property rights (except patent infringement and trade secret misappropriation) unintentional breach of contract, negligence or breach of duty to use reasonable care, breach of any duty of confidentiality, invasion of privacy, or violation of any other legal protections for personal information, defamation, libel, slander, commercial disparagement, negligent transmission of computer virus, worm, logic bomb, or Trojan horse or negligence in connection with denial of service attacks, or negligent misrepresentation.



**SCHEDULE 1**

**EXHIBIT XX**

**INSURANCE REQUIREMENTS**

<b>Type of Insurance</b>	<b>Coverage</b>
General Liability	\$1,000,000 each occurrence \$2,000,000 in the aggregate
Professional Liability	\$5,000,000 each claim \$10,000,000 in the aggregate
Crime Insurance	\$5,000,000 each event
Umbrella Coverage	\$5,000,000 occurrence and in the aggregate for excess for General Liability Insurance
Data Breach Insurance (including the coverage for the following: (1) contingent bodily injury for technology products; (2) notification expenses to warn customers or patients of security breaches; (3) loss including fines and penalties arising out of HIPAA and other privacy or consumer protection laws; (4) enterprise data privacy; (5) errors and omissions coverage for delivery of technology professional services; (6) network security protection and unauthorized access, including rouge employee coverage; (7) breach of an insured's privacy statement; and (8) malicious code, cyber-attacks, and inadvertent transmission of viruses.)	Included within Professional Liability Insurance listed above

SCHEDULE 2

# IT VENDOR RISK

## Insurance Requirements

Willis

## WHAT INSURANCE TO REQUIRE<sup>1</sup>

### VENDORS PROVIDING SOFTWARE, SOFTWARE OR SYSTEMS DEVELOPMENT, OR HARDWARE AND CONSULTING SERVICES.

- **Technology Professional Services and Products Coverage.** Vendors should be required to purchase Technology Errors and Omissions covering liabilities arising from errors, omission etc in rendering computer or information technology services. The best coverage is for “all products and services of the Insured” and is specific with its inclusion for both products as well as services. Very few markets are now following this approach with most defining professional services for each company. The vendor needs to incorporate coverage for “bodily injury and property damage that results from the failure of your products or your work provided or performed for others; and is caused by an errors and omissions wrongful act...”.
- **Privacy Coverage.** If the Vendor has access to confidential information whether it be personal or commercial in nature, the policy should cover liability arising from the disclosure of confidential information. The vendor should have coverage for the “Failure to prevent unauthorized access to, or use of, electronic data containing private or confidential information of others.”
- **Media and Content Coverage** If the services provided by the vendor involve publishing or creating of content, Media Liability coverage should be a component of the coverage and may include: cover for unauthorized use of advertising material, slogan or title or infringement of copyright, title, slogan, trademark, trade name, trade dress, service mark, or service name or plagiarism or unauthorized use of a literary or artistic format, character, or performance in your covered material. Some limited coverage may be provided under the General Liability policy for these types of exposures but these are now mostly excluded through professional liability exclusion.
- **Software Copyright Coverage.** If the vendor is creating code for the client or integrating code with client’s code, the policy should have coverage for software copyright which will provide protection in the event that any code that is provided is the subject of a claim that the vendor did not have the license to use it. This coverage will also protect against the claims arising from open source software copyright infringements from code that infringes public licenses.
- **Network Security Coverage** If the vendor has access to its client’s network or is connected to its client’s network or has employees working inside the client’s facility, coverage for network security and failures should also be requested to cover liability for unauthorized access or use of those systems.
- **An example request for coverage might read:** Vendor shall purchase and evidence (listing our organization as an Additional Insured) Technology Errors & Omissions (or technology professional liability coverage) insurance, including cover for loss or disclosure of electronic data, media and content

---

<sup>1</sup> These are examples only. Specific description of services may need to be inserted where the services are out of the ordinary. Contract language must for reviewed by lawyers for suitability in the circumstances of each particular vendor contract.

rights infringement and liability, network security failure, software copyright infringement and bodily injury and property damage due to the failure of your products or services with limits of \_\_\_\_\_ (limits vary depending on size of vendor and criticality of application).

## INTERNET/APPLICATION SERVICE PROVIDERS (VENDOR TO WHOM CLIENT HAS OUTSOURCED FUNCTIONS SUCH AS WEB HOSTING)

- Technology Professional Services and Products Coverage Exposures are likely to be required as described in the previous section
- Privacy Liability Coverage. Exposures are likely to be required as described in the previous section
- Media and Content Coverage Exposures are likely to be required as described in the previous section
- Software Copyright Coverage. If the vendor is creating code for the client the policy should have coverage for software copyright which will provide protection in the event that any code that is provided is the subject of a claim that the vendor did not have the license to use it. This coverage will also protect against the claims arising from open source software copyright. It is less likely that software copyright is required for ASPS than for other technology vendors but it may be prudent to include the coverage in a request.
- Network Security Coverage If the vendor has access to its client's network or is connected to its client's network or has employees working inside the client's facility, coverage for network security and failures should also be requested to cover liability for unauthorized access or use of those systems..
- **An example request for coverage might read:** Vendor shall purchase and evidence (listing our organization as an Additional Insured) Technology Errors & Omissions (or technology professional liability coverage) insurance, including cover for loss or disclosure of electronic data, media and content rights infringement and liability, network security failure and software copyright infringement liability and bodily injury and property damage due to the failure of your products or services with limits of \_\_\_\_\_ (limits vary depending on size of vendor and criticality of application).

## COMPANIES PROVIDING CONTENT

- Media and Content Coverage Companies providing content should be required to purchase Media Liability coverage which includes cover “for Unauthorized use of any advertising material, or any slogan or title... infringement of copyright, title, slogan, trademark, trade name, trade dress, service mark, or service name... plagiarism or unauthorized use of a literary or artistic format, character, or performance in your covered material. Some limited coverage may be provided under the General Liability policy for these types of exposures but these are now mostly excluded through professional liability exclusion.
- Privacy Liability Coverage. In the event a content provider has access to confidential information of the client whether it is personal or commercial in nature, the policy should cover the disclosure of confidential information. The vendor's policy should provide coverage for the “Failure to prevent

unauthorized access to, or use of, electronic data containing private or confidential information of others.” Broader coverage for non-electronic data is also covered.

- Network Security Coverage If the content provider has access to its client’s network or is connected to its client’s network or has employees working inside the client’s facility, coverage for network security and failures should also be requested to cover liability for unauthorized access or use of those systems.
- Broader Media Coverage can be obtained for the following on a standalone basis or as part of a professional policy.
  1. defamation including libel, slander, product disparagement or trade libel;
  2. negligent or intentional infliction of emotional distress, outrage or outrageous conduct;
  3. piracy and misappropriation of ideas under implied contract or other misappropriation of ideas or information;
  4. unfair competition, but usually only when alleged with other claims
  5. deceptive trade practices or fraud, but usually when alleged with other claims
  6. conspiracy, but usually only when alleged with other claims;
  7. breach of an indemnification or hold harmless agreement, but usually only when alleged with other claims such as those referred to above;
  8. negligent supervision of an employee, but usually only when alleged with other claims
  9. errors or omission in content or material.
- **An example request for coverage might read:** Vendor shall purchase and evidence (listing our organization as an Additional Insured) Media Errors & Omissions (or Media Liability) insurance, including cover for loss or disclosure of electronic data, media and content rights infringement and liability, with limits of \_\_\_\_\_ (limits vary depending on size of vendor and criticality of application).

## PARTNERS, OR AFFILIATES CONNECTED TO YOUR NETWORK

- Network Security Liability. If Customers, Partners, affiliates or anyone else has a connection to or access to the companies coverage for privacy and network security liability can be requested. Their policy should provide coverage for the “Failure to prevent unauthorized access to, or use of, electronic data containing private or confidential information of others.” Broader coverage for non-electronic data is also covered.
- Privacy Liability Coverage. In the event Customers, Partners, affiliates or anyone else has access to has access to confidential information whether it be personal or commercial in nature, the policy should cover the disclosure of confidential information. The vendor policy should provide coverage for the “Failure to prevent unauthorized access to, or use of, electronic data containing private or confidential information of others.” Broader coverage for non-electronic data is available under other specialized forms if required.

- **An example request for coverage might read:** Vendor shall purchase and evidence (listing our organization as an Additional Insured) Privacy and Network Security (sometimes otherwise known as Cyber Liability) coverage providing protection against liability for (1) systems attacks (2) denial or loss of Service attacks (3) spread of malicious software code (4) unauthorized access and use of computer systems and (5) liability arising from the loss or disclosure of confidential electronic data with coverage with limits of \_\_\_\_\_. [Limits will vary based on company size]

DM\_US 35880426-6.009900.0171

# **AHLA In-House Counsel Meeting 2012**

## **DOING GOOD AVOIDING EVIL**

Cynthia F. Wisner

1

### **Scenario 1 - Stolen Laptop**

Joe Jackson takes his laptop everywhere. His laptop is encrypted and he is careful to save on his laptop only the info he needs for this travels and to back up the laptop on the shared drive. Sadly Joe's apartment was broken into last week and the laptop was stolen.

2

### Scenario 2 – Billing/Coding Error

An audit revealed that the Hospital and its physicians complied with Medicare requirements for 15 of the 100 Evaluation and Management (E&M) services. However, the Hospital incorrectly billed for the remaining 85 services, resulting in overpayments totaling \$8,100. According to the audit overpayments occurred because the Hospital had inadequate billing system controls over billing E&M services related to outpatient eye injection procedures, and the Hospital's physicians, who performed the eye injection procedures, did not fully understand the Medicare requirements for separately billable E&M services.

3

### Scenario 3 – Stolen Patient Information

The billing activities for the employed physicians of Mercy Hospital are outsourced to ABC billing company. After investigating several patient complaints Mercy Hospital has discovered that hundreds of credit cards have been obtained in the names of its patients. Mercy Hospital notified ABC billing company and ABC suspects an employee with authorized access to the patient information misused his access to open up credit cards.

4



#### Scenario 4 – CDSP Error With Alert Fatigue

Jenny Blum has been working on 6E for the past three years. This week the new EHR called for her to give the patient 6 mg of a medication that she has always in the past limited to 2 mg. Jenny questioned the dosage and her supervisor agreed that she could call the physician to verify the order. Following the incident the investigation determined that the medication and dose were triggered by a standing order based on the clinical decision support program. However, the CDSP triggered an alert to the physician to check the dosage. The alert had been disabled. The physician changed the order when called and acknowledged that he had asked for the alert to be turned off. Further investigation revealed a flaw in the formula that doubled the patient's weight because the program ran twice.

5

#### Scenario 5 – Lost Flash Drive

Susan Smith travels from site to site to train users on data mining and She has her presentation on a flash drive. The presentation uses a test data set, but at her last session she downloaded production data to work with the site in the application because the application had not yet been installed. She forgot to delete the production data. The flash drive is not encrypted or password protected and she cannot find the flash drive. She has called the site's privacy officer and security officer to report the loss.

6

### Scenario 6 - HIE Disclosures

An IT vendor proposes a new coordination service that is intended both to facilitate the exchange of information between health care practitioners, providers, and suppliers (collectively, "Health Professionals", and to help them keep track of patients receiving services from other Health Professionals.

7

### Scenario 7 – Stolen Smart Phone

Jill Langster has a smart phone and was able to link her work email to her phone. She works in the coding and billing area and receives a lot of email with patient information.

She has added a password to her phone, but the email icon, when touched, displays all of her email. She left her smart phone plugged in to the charger in the hotel. The hotel staff called her and let her know that they have the phone and that she can pick it up.

8

### Scenario 8 – Payor Audit

An external audit revealed overpayments from incorrect billing of Medicare claims. The setup of the billing system caused a charge to be submitted when the lab service was ordered, and did not delete the charge when the service was not provided (e.g. due to an order change, patient discharge).

9

### Scenario 9 – Professional Liability Claim

Dr. Tim Johnson has been sued. He is concerned about whether the critical pathway can be introduced into evidence regarding the standard of care. The EHR in which the patient's vital signs were recorded includes a CDSP and critical pathway for chest pain. However, Dr. Johnson has been treating Ms. Dotson for the past 4 years and he decided to exercise his medical judgment and not to follow the prompts. In fact, he had his office manager turn off the prompts so that he could enter data more efficiently.

10

### Scenario 10 – Copy of Medical Record

Cynthia Thomas has asked for a copy of her medical record. She has shared a copy with her brother who is a physician. Her brother has contacted the hospital's medical records department to ask for more pages from the electronic record advising that it appears to him that the record is incomplete.

## OUTLINE

AHLA 2012

Doing Good and Avoiding Evil in Electronic Health Records (EHRs)

Cynthia F. Wisner

### **Brief Overview of the Functionality and Services Presenting the Highest Risks**

An Electronic Health Record (EHR) is an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR automates access to information and has the potential to streamline the clinician's workflow. <http://www.cms.gov/Medicare/E-Health/EHealthRecords>

### **Interoperable EHRs**

Interoperability is the ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively, and consistently, and to use the information that has been exchanged.

[www.nahit.org](http://www.nahit.org).

[http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_028957.hcs?p?dDocName=bok1\\_028957-02#02](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_028957.hcs?p?dDocName=bok1_028957-02#02)

### **Privacy Risks**

Most technology does not assure unauthorized viewers do not access patient information and many breaches occur as a result of misuse of access.

The office of the national coordinator for health information technology recently published a guide to privacy and security of health information (2/23/2012) for use by physician practices, noting "Adopting an EHR and electronically sharing patient health information with other providers creates both new risks and new ways to secure information.

<http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

The guide further states, "Your practice, not your EHR vendor, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR and comply with HIPAA Rules and CMS<sup>3</sup> Meaningful Use requirements."

**Latest re Privacy Regulations and Audits:** The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) said that a rule updating Health Insurance Portability and Accountability Act (HIPAA) regulations has been

sent to the White House Office of Management and Budget (OMB), signaling the rule will be released publicly in the near future. OMB received the final omnibus rule on March 24. Regulatory review is expected to take a full 90 days.

Audits mandated by the HITECH Act began in November 2011. OCR (Office of Civil Rights) contracted with KPMG in July 2011 to conduct 150 privacy and security compliance audits.

### **Security Risks**

Downloads, printed PHI, portable media all increase the risk of a wrongful disclosure.

Large amounts of data are accessible quickly

Significant number of losses involve stolen laptops

#### **Examples from May 2012 of stolen laptops:**

Stolen laptop risks data of 2,100 Boston Children's patients

May 25, 2012 Stolen laptop risks data of 2,100 Boston Children's patients - FierceHealthcare

<http://www.fiercehealthcare.com/story/stolen-laptop-risks-data-2100-boston-childrens-patients/2012-05-25#ixzz1wCh008KN>

Our Lady of the Lake Regional Medical Center has determined that a laptop computer containing limited health information for former Intensive Care Unit patients was discovered to be missing from a local physician office sometime between March 16 and 20, 2012. An extensive search was initiated as soon as the incident was discovered. Investigation of the incident continues and we have reported this occurrence to law enforcement. We will continue to share updated information. We are sorry this incident occurred and assure our patients and the community that we are committed to protecting patients' personal information. <http://www.nbc33tv.com/news/local-news/missing-laptop-from-olol-contains-patient-information>

### **Sadly, many breaches are caused by persons authorized to access PHI**

#### **Examples from misuse of access:**

**Ochsner Medical Center:** On March 3, 2009, Washington brought the stolen patient information sheets to the residence of his girlfriend, Blair, who then created online accounts with companies such as Kohl's, Target, American Eagle, Old Navy, Citizen's Bank, and Best Buy, in the names of the hospital patients contained on the information sheets. According to court documents, Washington was employed by Ochsner Medical Center as a janitor from November 2008 until June 3, 2009. In his capacity as janitor, he stole printouts containing confidential patient information such as names, social security numbers, and dates of birth, phone numbers, home addresses and other personal information that was intended to be shredded. Blair was sentenced to twenty-seven months in prison followed by three years of

supervised release, and Washington was sentenced to three years probation, with the special condition of six months of community confinement followed by six months of home incarceration.

**Howard University:** Six weeks after Howard University Hospital told more than 34,000 patients that a contractor's laptop containing their personal health information had been stolen; federal authorities have filed criminal charges against a hospital worker accused of selling people's medical records. Charging documents filed in federal court in Washington this week say Laurie Napper, a technician in the surgery department, sold patients' names, addresses, and dates of birth and Medicare numbers from August 2010 until December 2011. Charging documents state that Ms. Napper was employed by Howard University Hospital, but officials said she was employed in the offices of surgical physicians located on the Howard University campus but not in the hospital itself.

#### **And lost data also is costly:**

The issue is the ability of the covered entity to prove that the lost data has been destroyed or returned. On May 25, 2012 HealthData Management reported that South Shore Hospital in Weymouth, Mass., has agreed to a \$750,000 settlement with the state Office of Attorney General following a breach of protected health information that affected about 800,000 patients in 2010.

Under the agreement, the fined amount is \$750,000 but the hospital will be credited \$275,000 as recognition of investments it has made in improving information security. The hospital will pay a \$250,000 regulatory enforcement payment and make a \$225,000 contribution to a data security education fund.

The hospital sent hundreds of back-up computer tapes in three boxes to a contractor for destruction in February 2010, but the contractor only received one box. The contractor did not notify South Shore until June 2010. The boxes were never found and following an investigation South Shore said it believed but could not prove that the boxes were disposed of in a secure landfill.

<http://www.healthdatamanagement.com/news/breach-notification-hipaa-privacy-security-ocr-44516-1.html>

#### **Is the information security infrastructure ready for EHRs?**

An HHS Report concludes that Electronic records are vulnerable (reported by Associated Press May 17, 2011)

HHS report concludes hosp-doctor links are being layered on system that already has glaring privacy/security problems. HHS examined computer security at seven large hospitals and found 151 security vulnerabilities. The report classified 4 out of 5 flaws as "high impact," meaning they could result in costly losses, even injury and death. Among the flaws were inadequate passwords; computers that

did not automatically log off inactive users; unencrypted laptops that contained pt. data. HHS also criticized agencies' lax enforcement HIPAA security rules.

And the GAO also has identified the vulnerabilities of EHRs. Homeland Security (DHS) also has been criticized by the GAO for security vulnerabilities in the nation's infrastructure. According to the GAO DHS faces challenges in meeting its responsibilities to protect the nation's vast critical infrastructure—18 broad ranging sectors including banking and finance, chemicals, communications, energy, public health and health care, transportation, and defense. Given that these sectors are largely owned and operated by the private sector or state and local governments, numerous parties have responsibility for securing and maintaining these networks. Key challenges include the following:

Highlights of [GAO-08-212](#) (PDF), Highlights of [GAO-08-588](#) (PDF), Highlights of [GAO-08-825](#) (PDF), and Highlights of [GAO-08-1157T](#) (PDF)

**Authentication and identity-proofing schemes are needed** for providers, including individuals and systems, such as doctors, practices and hospitals, as well as for consumers, HHS panelists discussing a National Health Information Network said in 2010. <http://fcw.com/articles/2010/01/07/nhin-authentication-hhs-electronic-health-records.aspx>

### **Electronic and Digital Signatures**

While federal and accreditation requirements including the Conditions of Participation (COPs) have been updated to require authentication and not a physical signature some state agencies continue to require physical or digitized signatures. Accreditation standards and COPs permit state law to require physical signatures. Whether the federal E-Sign law preempts state law and regulations is not tested, especially because the E-Sign law was focused on consumer transactions. The Electronic Signatures Act (Public Law No: 106-229) went into effect on October 1, 2000 and gives electronic contracts the same weight as those executed on paper.

**Digital signature:** a cryptographic signature (a digital key) that authenticates the user, provides nonrepudiation, and ensures message integrity. This is the strongest signature because it protects the signature by a type of “tamper-proof seal” that breaks if the message content were to be altered.

**Digitized signature:** an electronic representation of a handwritten signature. The image of a handwritten signature may be created and saved using various methods, such as using a signature pad, scanning a wet signature, or digital photography. The signature may be “captured” in real time (at the time the user applies the signature), or a saved image captured at the point of normal business operations may be imported. The digitized signature is useful for patient signatures that must



be collected for admission consent, surgical consent, authorizations, discharge instructions, advance directives, and generally any other type of electronic form requiring patient signature.

**Electronic signature:** a generic, technology-neutral term for the various ways that an electronic record can be signed, including a digitized image of a signature, a name typed at the end of an email message by the sender, a biometric identifier, a secret code or PIN, or a digital signature.

### **Sensitive diagnoses**

Federal laws protect alcohol treatment records, drug abuse treatment records, mental health treatment records, HIV/Acquired Immune Deficiency Syndrome (AIDS) records, hepatitis B or C testing records and genetic testing records

Every state has consent requirements for disclosure for treatment of sensitive diagnoses

Sample state laws: ILLINOIS PUBLIC HEALTH (410 ILCS 513/) Genetic Information Privacy Act.

Sec. 15. Confidentiality of genetic information.

(a) Except as otherwise provided in this Act, genetic testing and information derived from genetic testing is confidential and privileged and may be released only to the individual tested and to persons specifically authorized, in writing in accordance with Section 30, by that individual to receive the information.

Sec. 30. Disclosure of person tested and test results.

(a) No person may disclose or be compelled to disclose the identity of any person upon whom a genetic test is performed or the results of a genetic test in a manner that permits identification of the subject of the test, except to the following persons:

(1) The subject of the test or the subject's legally authorized representative. This paragraph does not create a duty or obligation under which a health care provider must notify the subject's spouse or legal guardian of the test results, and no such duty or obligation shall be implied. No civil liability or criminal sanction under this Act shall be imposed for any disclosure or nondisclosure of a test result to a spouse by a physician acting in good faith under this paragraph. For the purpose of any proceedings, civil or criminal, the good faith of any physician acting under this paragraph shall be presumed.

(2) Any person designated in a specific written legally effective release of the test results executed by the subject of the test or the subject's legally authorized representative.

(3) An authorized agent or employee of a health facility or health care provider if the health facility or health care provider itself is authorized to obtain the test results, the agent or employee provides patient care, and the agent or employee has a need to know the information in order to conduct the tests or provide care or treatment.

**Sample consent form:**

**FOR SENSITIVE DIAGNOSIS ONLY**

**AUTHORIZATION FOR RELEASE OF INFORMATION**

ANY USE AS AN AUTHORIZATION TO USE OR DISCLOSE PSYCHOTHERAPY NOTES MAY NOT BE COMBINED WITH ANOTHER AUTHORIZATION EXCEPT ONE TO USE OR DISCLOSE PSYCHOTHERAPY NOTES.

**If signed by legal representative, please provide representative documentation as required by state law, i.e. Power of Attorney, Health Care Surrogate, Living Will or Guardianship papers. HMHS WILL NOT PROCESS INVALID FORMS.**

**FM.18.02.001-Authorization Release PHI-12/10/2008**

Beneficiary name Sponsor ID Number

Beneficiary street, city, state, zip: Beneficiary S.S. number

I authorize the use or disclosure of the above-name beneficiary personal health information by Humana Military Healthcare Services ("HMHS") and/or TRICARE Health Plan, as describe below: **(ONLY ONE CHECK BOX BELOW IS ALLOWABLE, PER FORM)**

Pregnancy & Birth Control Records

Abortion Records

AIDS & STDS Records

Mental Health Records

(Nature of Information, as limited as possible: \_\_\_\_\_)

Alcohol & Drug Abuse Records

(Nature of Information, as limited as possible: \_\_\_\_\_)

This information may be disclosed to, and used by, the following individual or organization:

Name:

Address:

The information is being disclosed for the following purpose(s)::

Personal Use  Continued Medical Care  School

Other \_\_\_\_\_

Insurance Claims  Retirement/Separation  Legal (Purpose of disclosure, as specific as possible)

**By signing below, the beneficiary or the beneficiary's representative agrees to the following statements:**

1. I understand that my health care and the payment for my health care will not be affected if I do not sign this form.
2. I understand that I may see and copy the information described on this form if I ask for it, and that I get a copy of this form after I sign it.
3. I understand that I may revoke this authorization at any time. I understand that in order to revoke this authorization, I must do so in writing and send my written revocation to HMHS' Privacy Office to the address below. I understand that the revocation will not apply to information that has already been released in response to the authorization.
4. I understand that once the information is disclosed pursuant to this authorization, it may be re-disclosed by the recipient and the information may not be protected by federal privacy regulations
5. I understand that my records are protected under the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, and cannot be disclosed without my written consent unless otherwise provided for in the Regulations.

I understand that I may refuse to sign this authorization and that HMHS may not condition treatment or payment on whether I sign this authorization. If no expiration date is specified then this authorization will expire one year from the date of signature.

**Expiration Date**

\_\_\_\_ / \_\_\_\_ / \_\_\_\_

**(MM) (DD) (YR)**

Signature of beneficiary or beneficiary's representative Representative relation to beneficiary  
//

Signature of parent, guardian or authorized representative, when required Date (MM/DD/YR)  
*(The MCSC Operations Manual and state/federal law commonly state that information related to alcohol/drug treatment, abortion, venereal disease, and/or AIDS cannot be disclosed without written consent of the patient/beneficiary. In some instances, information related to mental health and pregnancy/birth control may also require written consent of the patient/beneficiary.)* HMHS will follow all Federal and state laws and regulations that are more stringent.

Return completed form (select best option): Humana Military Healthcare Services  
HMHS Privacy Office

P.O. Box 740062

Louisville, Kentucky 40201-7462

**Or fax to: 877-298-3407**

**FOR SENSITIVE DIAGNOSIS ONLY**

**AUTHORIZATION FOR RELEASE OF INFORMATION**

ANY USE AS AN AUTHORIZATION TO USE OR DISCLOSE PSYCHOTHERAPY NOTES MAY NOT BE COMBINED WITH ANOTHER AUTHORIZATION EXCEPT ONE TO USE OR DISCLOSE PSYCHOTHERAPY NOTES.

**If signed by legal representative, please provide representative documentation as required by state law, i.e. Power of Attorney, Health Care Surrogate, Living Will or Guardianship papers. HMHS WILL NOT PROCESS INVALID FORMS.**

<http://www.humana-military.com/library/pdf/auth-release-sensitive-diagnosis.pdf>

**Exceptions exist for emergencies**

Definition of emergency varies by state and type of data

**For example**, in Michigan HIV-related information is confidential and cannot be released unless the patient authorizes disclosure, or a statutory exception applies.

This confidentiality statute applies to all reports, records, and data pertaining to testing, care, treatment, reporting and research, and information pertaining to partner counseling and referral services (formerly known as partner notification) under section 5114a, that are associated with the serious communicable diseases or infections of HIV and AIDS.

Michigan law provides that information pertaining to an individual who is HIV infected or has been diagnosed as having acquired immunodeficiency syndrome, may be disclosed to a health care provider for 1 or more of the following purposes:

- (i) To protect the health of an individual.
- (ii) To prevent further transmission of HIV.
- (iii) To diagnose and care for a patient.

**Health Information Exchanges (HIEs) create major privacy and security risks**

Most HIEs started as treatment only

Most HIEs rely on security schemes in use by participants

Similar risks to those of Business Associates

Largest number of breaches

**Transmission issues:** In other industries attacks are causing many breaches. See report of attacks and breaches from Symantec

[http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-](http://www.symantec.com/content/en/us/enterprise/other_resources/b-)

istr\_main\_report\_2011\_21239364.en-us.pdf and the 2012 Verizon report [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

### **Biggest integrity issue in the EHR is over-writing**

Over-writing the initial entry, even though the information is incorrect, could be construed as improper alteration of the historical medical record.

As a general matter, states require that electronic records be maintained “to the same standards” as paper copies.

The amended entry in the EHR should be flagged to indicate that it has been corrected, and the original entry should be retained and easily accessed. A comment field in the amended record may be the solution. As in a paper record, a narrative entry indicating that an error has been made, and is being corrected by the new entry, is the best procedure.

### **Examples of State laws on altering medical records:**

In Michigan the intentional alteration of medical records is a felony: Michigan Compiled Laws Section **750.492a Placing misleading or inaccurate information in medical records or charts; alteration or destruction of medical records or charts; penalties**

In Maryland § **4-403**. Alteration of medical records is a misdemeanor. **A provider may not knowingly or willfully destroy, damage, alter, obliterate, or otherwise obscure a medical record, hospital report, laboratory report, X-ray report, or other information about a patient in an effort to conceal the information from use as evidence in an administrative, civil, or criminal proceeding.**

Alteration of records historically has been considered spoliation subject to penalties and often loss of insurance coverage, and in some cases punitive damages. Punitive damages were awarded for fraudulently altering medical records in *Moskovitz v. Mt. Sinai Med. Ctr.*, 69 Ohio St.3d 638, 635 N.E.2d 331 (Ohio 1994) [http://biotech.law.lsu.edu/cases/medrec/moskovitz\\_v\\_mt\\_sinai.htm](http://biotech.law.lsu.edu/cases/medrec/moskovitz_v_mt_sinai.htm)

### **Second biggest integrity issue in the EHR is cut and paste**

Dimick, Chris. "Documentation Bad Habits: Shortcuts in Electronic Records Pose Risk." *Journal of AHIMA* 79, no.6 (June 2008): 40-43. For more about appropriate uses of copy and paste or carry forward. [Journal.ahima.org](http://www.journal.ahima.org).

### **Patient Portals and Personal Health Records**

The Personal Health Record (PHR) is an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual. [healthit.hhs.gov/defining\\_key\\_hit\\_terms](http://healthit.hhs.gov/defining_key_hit_terms)

The Federal Trade Commission (FTC) regulates personal health records offered by non-HIPAA covered entities. PHRs offered by HIPAA covered entities are covered by HIPAA.

### **Minors' records**

Most states provide for confidentiality of minors records in connection with those health care services that can be obtained by the minor without a parent/guardian's consent.

### **Meaningful Use Security**

CMS takes Privacy and Security very seriously: *“Do not register and attest for an EHR Incentive program until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis. Document these changes/corrections. Providers participating in the [EHR Incentive Program](#) can be audited. When you attest to meaningful use, it is a legal statement that you have met specific standards, including that you protect ePHI.”*  
<http://www.everythinghitech.com/everything-hitech/attestation/>

### **Meaningful Use Stage 2**

In Stage 2 of meaningful use CMS proposes to formally require patient portals.

**EPs:** The requirement for eligible professionals that patients have electronic access to their information is proposed to become that patients have used the capability to access and download their information and have communication preferences stated, as well as a requirement that 10% patients get reminders for preventive, follow-up care. Patients will have the right to view and download (on demand) relevant information contained in the longitudinal record, which has been updated within 4 days of the information being available to the practice.

**EHs:** For Eligible Hospitals (EH)s the requirement is that 80% of patients are offered the ability to view and download via a web-based portal, within 36 hours of discharge, relevant information contained in the record about EH inpatient encounters, and must provide 10% of patients seen during the EHR reporting period timely electronic access to their health information, which can be achieved through an EHR patient portal or personal health record. (A web portal as defined as online access to health information. Therefore all patient portals defined as such are subject to HIPPA rules and regulations.)

<http://www.hitechanswers.net/patient-portals-a-necessity-for-stage-2-meaningful-use/> and

[http://www.fhwnlaw.com/docs/bush\\_-\\_meaningful\\_use\\_stage\\_2.pdf](http://www.fhwnlaw.com/docs/bush_-_meaningful_use_stage_2.pdf)

### **Telemedicine and other Social Media**

A recent study concluded that the use of mobile, robotic telemedicine technology is in fact feasible for the NICU. The system used enabled remote neonatologists to accurately identify and assess the patients through the use of the mobile robot in the NICU without incident and the audio and video quality was noted as

acceptable.<http://www.imedicalapps.com/2012/03/researchers-study-the-feasibility-of-mobile-robotic-telemedicine-in-the-nicu/>

The Department of Health and Human Services defines a **mobile health device** as:

"[A] handheld transmitting device with multi-functional capabilities used to store, transmit and receive health information and has user control over the access to the health information. Mobile devices combine elements of computing, telephone/fax, Internet and networking functions. This generally includes laptop computers, personal digital assistants (PDA), smartphones, and tablet computers. Mobile transmitting devices generally do not include storage devices such as USB drives."

Both mobile devices and telemedicine are “new” challenges for application of existing laws and regulations.

A good summary of the devices, advancements and current concerns can be found in the overview of the 17th Annual International Meeting and Exposition brought together telemedicine vendors, entrepreneurs, engineers, government employees, representatives of healthcare systems, and medical and academic institutions, healthcare administrators, and a variety of healthcare professionals from around the world, totaling about 5,000 attendees. Only a handful of lawyers were in attendance.

<http://www.healthlawyers.org/News/Health%20Lawyers%20Weekly/Pages/2012/May%202012/May%2018%202012/AvoidingLegalPitfallsWhenImplementingTelemedicinePracticesInsightsFromTheATAAnnualInternationalMeetingAndExposition.aspx>

New research from HealthGrades concludes that hospitals with better patient-provider communication have better patient safety and satisfaction rates. The data point to a link between provider communication and patient safety.

"We have reached a point where Americans must acknowledge the connection between communicating with their healthcare provider and their own safety and satisfaction as patients," study author Kristin Reed, HealthGrades vice president of clinical quality programs, said in a statement.

[http://www.healthgrades.com/business/news/press-releases/2012\\_Patient\\_Safety\\_Experience.aspx](http://www.healthgrades.com/business/news/press-releases/2012_Patient_Safety_Experience.aspx)

Mobile devices may facilitate more patient interaction. Clinical diagnostic decision support software vendor Isabel Healthcare has introduced a mobile version for use with iPhone, iPad and iPod touch devices. It is the first mobile app for the 12-year-old firm and will enable quick access to diagnostic support during hospital rounds or any other type of patient encounter. Weekly, monthly and annual pricing options are available. The app gives access to information on more than 6,000 diseases and supports sharing results with colleagues or including them in medical notes.

[http://www.healthdatamanagement.com/news/health-information-technology-](http://www.healthdatamanagement.com/news/health-information-technology-vendor-news-44501-)

[1.html?ET=healthdatamanagement:e2584:190069a:&st=email&utm\\_source=editorial&utm\\_medium=email&utm\\_campaign=HDM\\_Daily\\_0523](http://www.healthdatamanagement.com/news/health-information-technology-vendor-news-44501-1.html?ET=healthdatamanagement:e2584:190069a:&st=email&utm_source=editorial&utm_medium=email&utm_campaign=HDM_Daily_0523)

### **OIG Advisory Opinions re stroke network and connectivity**

Recent OIG advisory opinions illustrate the flexibility of OIG in reviewing proposals for improving patient care through shared EHRs and health information. In Adv Op 11-12 the OIG determined that arrangements to provide neuro emergency clinical protocols and immediate consultations with stroke neurologists via telemedicine technology to certain community hospitals (the “Proposed Arrangement”) could potentially generate prohibited remuneration under the anti-kickback statute if the requisite intent to induce or reward referrals of Federal health care program business were present, but the Office of Inspector General (“OIG”) would not impose administrative sanctions. In Adv Op 11-06 the OIG concluded that “per-click” payments for transmission of referral information as part of integrated electronic health record and physician office support services also could potentially generate prohibited remuneration under the anti-kickback statute if the requisite intent to induce or reward referrals of Federal health care program business were present, but the OIG would not impose administrative sanctions. <http://oig.hhs.gov/reports-and-publications/archives/advisory-opinions/index.asp#2011>

### **EHR Donation Stark Exception, AKS Safe Harbor and IRS guidance**

The EHR donation permissions are scheduled to expire December 31, 2013. In a letter to Inspector General Daniel Levinson the HIMSS Board of Directors and members strongly recommend removing the sunset provision and making the EHR donation rules a permanent safe harbor. HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare.

<http://www.himss.org/policy/d/HIMSSCommentsToOIGSafeHarbor.pdf>

### **Legal Responses to Highest Risks**

Evolving Standards of Care Delivery and Documentation

Potential for efficiency and savings depends heavily on improving physicians and other providers’ documentation. However, electronic documentation in its current incarnation is time-consuming and can degrade diagnostic thinking — by distracting physicians from the patient, discouraging independent data gathering and assessment, and perpetuating errors.

<http://www.nejm.org/doi/full/10.1056/NEJMp0911734>

### **Potential for Harm Concerns with EHRs**

Physicians are concerned about the impact of EHRs on the delivery of health care. Gordon D. Schiff, M.D., and David W. Bates, M.D. provided their Perspective in the N Engl J Med 2010; 362:1066-1069 March 25, 2010 identifying the need for reconceptualize documentation workflow as part of the next generation of EHRs. They also lament that billing codes dictate evaluation and management and providers are forced to focus on ticking boxes rather than on thoughtfully documenting their clinical thinking.

The following are the National Institute of Standards and Technology's (**NIST**) **Top 3 Potential For Harm concerns** with EHRs:

**1. Patient identification errors**

For example, if EMR displays don't have headers with two patient identifiers, lock out or control multiple accesses to records, or fail to provide full patient identification with integrated apps like imaging, the wrong actions could be performed on the wrong patient.

**2. Data accuracy errors.**

There's lots of ways EMR design foster data errors, the report notes, including when information is truncated on the display, when accurate information isn't displayed unless users refresh the data, when discontinued meds aren't eliminated and when changes in status aren't displayed accurately.

**3. Medication Errors.**

Medication errors in hospital discharge summaries have the potential to cause serious harm to patients. These errors are generally associated with manual transcription of medications between medication charts and discharge summaries. Studies also show junior doctors are more likely to contribute to discharge medication error rates. Electronic discharge summaries have the potential to reduce discharge medication errors to ensure the safe handover of care to the primary care provider.

[http://www.ijmijournal.com/article/S1386-5056\(09\)00134-8/abstract](http://www.ijmijournal.com/article/S1386-5056(09)00134-8/abstract) and [http://www.tara.tcd.ie/bitstream/2262/41594/1/PEER\\_stage2\\_10.1007%252Fs00228-009-0680-1.pdf](http://www.tara.tcd.ie/bitstream/2262/41594/1/PEER_stage2_10.1007%252Fs00228-009-0680-1.pdf)

**4. Data availability errors.**

Clinicians can easily make mistakes if they can't easily see all the information they need to understand doses without additional navigation; if complex doses aren't easily understandable without extra navigation; and if information accurately updated in one place shows up accurately and efficiently within other areas or integrated software.

**DO they or DON'T they? Do EHRs improve Quality?**

CMS notes that the EHR can improve patient care by:



- Reducing the incidence and extent of medical error by improving the accuracy and clarity of medical records.
- Making the health information available, reducing duplication of tests, reducing delays in treatment, and patients well informed to take better decisions.

<http://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html?redirect=/EHealthRecords/>

And more studies are being conducted about the details of the EHR

For example, in a recent study Boston researchers found that Doctors' documentation may affect care quality. Primary care doctors who used structured EHR documentation or free text notes provided better quality care to patients with diabetes and coronary artery disease than those who dictated their notes, Boston researchers reported in the *Journal of the American Medical Informatics Association*. [BeckersHospitalReview.com](http://BeckersHospitalReview.com) (5/25).

While a 2011 study (and past studies) show that EHRs reduce errors, the AMA still is concerned about substituting process for judgment.

### **Studies Show that EHRs Reduce Medical Errors**

In a 2005 article entitled **Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs** the authors reported that e-prescribing has the potential to eliminate 200,000 adverse drug events annually. <http://content.healthaffairs.org/content/24/5/1103.full>

In a study published in the March 2011 issue of *Journal of Psychiatric Practice*, findings show that the rate of medication errors was reduced 87 percent after "computerized provider order-entry and error-reporting systems were implemented." The study was conducted at an 88-bed psychiatric unit at Johns Hopkins Hospital, and data was randomly selected from 2003 to 2007. <http://chartlogicnews.com/newsrelease-cid-1-id-141.html>

### **Both NIST and AMA linked EMRs to patient harm in 2012**

The NIST report released in March 2012 analyzed which EMR design factors have an impact on usability (PDF), including one subset which seems likely to cause patient harm. NIST is the National Institute of Standards and Technology in the Department of Commerce. According to the report it is estimated that one in three patients will potentially be harmed during hospitalization, the potential for using EHRs to improve patient safety may be significant. On the other hand, a prior study found that patient mortality unexpectedly increased following the introduction of an EHR in a pediatric hospital.

Info Week reported in January 2012 that an AMA report found that EHRs are linked to errors, harm. The report cites a litany of broad-based problems that have accompanied the emergence of EHR systems, including these: poorly designed systems with software that is far from user friendly; a data-entry process that encourages copying and pasting data and that contributes to what researchers call "automatic behavior" rather than meaningful analysis; and assorted problems that result in "generating new types of errors." In fact, says Dr. David Classen, a consultant on the AMA report, "There is still very limited evidence that EHRs improve the safety of care in the average doctor's office."

[www.informationweek.com/news/healthcare/EMR/232400325](http://www.informationweek.com/news/healthcare/EMR/232400325)

In addition, studies are mixed about how EMRs will impact liability for physicians. A 2010 survey by Conning Research and Consulting, an insurance industry research firm, found that most insurers believe medical claims will rise during the move from paper to electronic records. Lawsuits probably will decrease after an adjustment period, the study said. <http://www.ama-assn.org/amednews/2012/03/05/prsa0305.htm>. The consensus conclusion, as reflected in the Institute of Medicine report, is that additional research is needed to better understand how EHR usability can impact patient outcomes.

### **The confidentiality and error reporting controversy.**

Sen. Chuck Grassley (R-Iowa) sent letters in 2010 to 31 hospitals seeking more information about their experiences and concerns with health IT systems.

<http://www.ihealthbeat.org/articles/2010/1/21/sen-grassley-asks-hospitals-to-detail-health-itrelated-errors.aspx#ixzz1wCMkRdnZ>

There's also no mechanism for publicizing problems with EHR interfaces, unlike the FDA's process for issues with medical devices. Shneiderman describes a case where a physician found a bug in an EHR that created a danger to patients. "He contacted the supplier because he thought it was something other users should know about, and the response was, 'Oh, we know-we're working on it,'" Shneiderman says. "The physician said, 'What? You know about it and you haven't notified everyone?' Contrast that with the Federal Aviation Administration, where problems with airplanes are publicized within hours."

The IOM report calls for substantial loosening of those contractual restrictions. "The committee views prohibition of the free exchange of information to be the most critical barrier to patient safety and transparency," the report says. "The committee urges the [HHS] Secretary to take vigorous steps to restrict contractual language that impedes public sharing of patient safety-related details. Contracts should be developed to allow explicitly for sharing of health I.T. issues related to patient safety." The report also says there should be a central place to report and publicize known issues with EHR software.

<http://www.informationweek.com/news/healthcare/EMR/232400325>

Poor EHR design might be a patient safety issue. The Institute of Medicine's (IOM) November 2011 report, "Health IT and Patient Safety: Building Safer Systems for Better Care," cited lack of usability as one potential cause of errors in using EHRs: "Poor interface design that detracts from clinician efficiency and affinity for the system will likely lead to underuse or misuse of the system." [http://www.healthdatamanagement.com/issues/20\\_2/user-unfriendly-43946-1.html?zkPrintable=true](http://www.healthdatamanagement.com/issues/20_2/user-unfriendly-43946-1.html?zkPrintable=true) and <http://www.iom.edu/~media/Files/Report%20Files/2011/Health-IT/Commissioned-paper-Roadmap-for-Provision-of-Safer-HIS.pdf>

### **Standing Orders or Protocols – what can and cannot be used to provide care?**

What is a standing order?

A standing order is a written document containing rules, policies, procedures, regulations, and orders for the conduct of patient care in various stipulated clinical situations. The standing orders are usually formulated collectively by the professional members of a department in a hospital or other health care facility. Standing orders usually name the condition and prescribe the action to be taken in caring for the patient, including the dosage and route of administration for a drug or the schedule for the administration of a therapeutic procedure. Standing orders are commonly used in intensive care units, coronary care units, and emergency departments. <http://medical-dictionary.thefreedictionary.com/standing+orders>

Proposed changes to the Medicare Conditions of Participation (COPs) would allow hospitals to use standing orders when certain requirements are met. The proposed rule would allow for the preparation and administration of drugs and biologicals on the orders contained within pre-printed and electronic standing orders, order sets, and protocols for patient orders, if the orders meet the proposed requirements in the medical record services COP.

<http://www.cms.gov/Regulations-and-Guidance/Legislation/CFCsAndCoPs/Hospitals.html> and <http://www.gpo.gov/fdsys/pkg/FR-2012-05-16/pdf/2012-11548.pdf>

*Standing Orders:* We have allowed hospitals the flexibility to use standing orders and have added a requirement for medical staff, nursing, and pharmacy to approve written and electronic standing orders, order sets, and protocols. We have required that orders and protocols must be based on nationally recognized and evidence-based guidelines and recommendations.

**§ 482.24 Condition of participation:  
Medical record services.**

\*\*\*\*\*

(c) \*\*\*

(2) All orders, including verbal orders, must be **dated, timed, and authenticated promptly by the ordering practitioner or by another practitioner who is**

**responsible for the care of the patient** only if such a practitioner is acting in accordance with State law, including scope-of-practice laws, hospital policies, and medical staff bylaws, rules, and regulations.

(3) Hospitals may use pre-printed **and electronic standing orders, order sets, and protocols for patient orders only if the hospital:**

- (i) Establishes that such orders and protocols have been reviewed and approved by the medical staff and the hospital's nursing and pharmacy leadership;
- (ii) Demonstrates that such orders and protocols are consistent with nationally recognized and evidence-based guidelines;
- (iii) Ensures that the periodic and regular review of such orders and protocols is conducted by the medical staff and the hospital's nursing and pharmacy leadership to determine the continuing usefulness and safety of the orders and protocols; and
- (iv) Ensures that such orders and protocols are dated, timed, and authenticated promptly in the patient's medical record by the ordering practitioner or by another practitioner responsible for the care of the patient only if such a practitioner is acting in accordance with State law, including scope-of-practice laws, hospital policies, and medical staff bylaws, rules, and regulations.

\* \* \* \* \*

In contrast to a standing order, an order set, protocol, critical pathway or clinical practice guideline can be incorporated into the EHR and can interface with decision support systems.

The Agency for Health Care Research and Quality offers the following definitions:

**Clinical Practice Guidelines:** Defined as "systematically developed statements to assist practitioner and patient decisions about appropriate healthcare for specific clinical conditions,"<sup>1</sup> guidelines may affect both the process and the outcome of care.

**Critical Pathways:** Although closely related to clinical practice guidelines, pathways more directly target the specific process and sequence of care, frequently plotting out the expected course of an illness or procedure with associated prompts for appropriate interventions. Also known as clinical pathways and care maps, pathways are generally multidisciplinary by design and may incorporate the responsibilities of physicians and nurses with those of ancillary medical providers including pharmacists, physical therapists and social workers.

**Protocol and Order Set:** The terms protocol and order set often are used to describe care paths and processes initiated and following based on symptoms and diagnoses.

The potential of clinical practice guidelines and critical pathways is illustrated by the 2007 study in which several physicians determined a favorable impact of standardized order sets on quality and financial outcomes for patients at Baylor Health Care System (BHCS).

[http://www.ahrq.gov/downloads/pub/advances2/vol2/Advances-Ballard\\_12.pdf](http://www.ahrq.gov/downloads/pub/advances2/vol2/Advances-Ballard_12.pdf)

## **Mobile Devices and Medical Apps**

**Be sure to attend the PG Luncheon for Health Information and Technology at the 2012 Annual Meeting is about Google, Medical Apps and the FDA  
Eric D. Hargan, Esquire**

The Food and Drug Administration (FDA) announced in 2011 that it would begin overseeing certain medical applications for mobile devices that could present a risk to patients if the apps do not work as intended. In July 2011, FDA published proposed guidelines on how it intends to regulate "mobile medical apps." But does such oversight appear to be necessary and sufficiently targeted, and can it be exercised in a way that does not stifle innovation?

This is an area of breaking news:

**Example: FCC approves allocation of wireless spectrum for medical devices**

The Federal Communications Commission has agreed to allocate 40 MHz of broadband spectrum for medical devices. The move is expected to eliminate transmission interference from consumers' devices and allow for easier monitoring of patients by eliminating the cables that keep them tethered to hospital beds. Healthcare IT News (5/24).

**Copyright issues-**

**CPT codes** are licensed by the AMA. The AMA is committed to making *CPT* widely available at low cost. The AMA holds copyright in *CPT* and use or reprinting of *CPT* in any product or publication requires a license. <http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/cpt/cpt-products-services/licensing.page>

**Patient evaluations and copyrighted scales**

Care is needed to ensure that copyrighted materials are not incorporated into the EHR without authorization from the owner

**Example:** In December 2011, developers of the Sweet 16 permanently removed the cognitive impairment examination from the Internet, saying it no longer could be distributed. The move stems from a copyright infringement accusation by Psychological Assessment Resources (PAR), a corporation that manages the copyright license to another cognitive screening test, the Mini-Mental State Examination. <http://www.ama-assn.org/amednews/2012/01/30/prsa0130.htm#s1>

**Billing and Coding Errors and Associated Enforcement Consequences – coping with systemic errors and avoiding false claims**

Overpayments occurred primarily because the Hospital did not have adequate controls to prevent incorrect billing of Medicare claims. Medicare Compliance Reviews for Calendar Years 2009 and 2010: Piedmont Hospital (A-04-11-00081), Regional Medical Center at Memphis (A-04-11-00082), and South

Miami Hospital (A-04-11-07023)  
<http://oig.hhs.gov/oas/reports/region4/41107023.pdf>

**Fletcher Allen Health Care Did Not Always Bill Correctly for Evaluation and Management Services Related to Eye Injection Procedures (A-01-11-00515)**  
<http://go.usa.gov/pH1>

Fletcher Allen Health Care (the Hospital), located in Burlington, Vermont, and its physicians complied with Medicare requirements for 15 of the 100 Evaluation and Management (E&M) services that we sampled. However, the Hospital incorrectly billed for the remaining 85 services, resulting in overpayments totaling \$8,100. Based on these sample results, we estimated that the Hospital and its physicians received overpayments totaling \$211,000 for calendar years 2008 through 2010. Overpayments occurred because the Hospital had inadequate billing system controls over billing E&M services related to outpatient eye injection procedures, and the Hospital’s physicians, who performed the eye injection procedures, did not fully understand the Medicare requirements for separately billable E&M services.

**Policies and Procedures**

**Administrative Safeguards**

Sample security policies table of contents:

1	<a href="#">Information Security Management</a>
1.1	<a href="#">Information Security Roles &amp; Responsibilities</a>
1.2	<a href="#">Information Classification</a>
1.3	<a href="#">Information Handling</a>
2	<a href="#">Domain Name and SSL</a>
3	<a href="#">Information Security Risk Management</a>
3.1	<a href="#">Information Security Risk Assessment</a>
1	<a href="#">Acceptable Use</a>
2	<a href="#">Network Communication Services (Email, Internet and other Social Media)</a>
3	<a href="#">Workstation Use and Security</a>
1	<a href="#">Unified Communications</a>
2	<a href="#">Workstation Use &amp; Security - Information Services</a>
3	<a href="#">Physical Security</a>
3.1	<a href="#">Building Security</a>
3.2	<a href="#">Equipment Security</a>
3.2	<a href="#">Environmental Security</a>

4	<a href="#">Operations Management</a>
4.1	<a href="#">Change Management and Approval Process</a>
4.2	<a href="#">Anti-Virus Security</a>
4.3	<a href="#">Backups</a>
4.4	<a href="#">Application and System Archival &amp; Storage</a>
4.5	<a href="#">Software Licensing &amp; Media Management</a>
5	<a href="#">Security Monitoring &amp; Vulnerability Management</a>
5.1	<a href="#">Security Compliance: Evaluation &amp; Accreditation</a>
5.2	<a href="#">Information Access Monitoring</a>
5.3	<a href="#">Performance / Availability Monitoring</a>
6	<a href="#">Access Management</a>
6.1	<a href="#">Identification &amp; Authentication</a>
6.2	<a href="#">Eligibility for Access to the Electronic Information Systems</a>
6.3	<a href="#">Management of Access to Trinity Health Systems and Applications</a>
6.4	<a href="#">Vendor Access</a>
6.5	<a href="#">Revoking Access</a>
6.6	<a href="#">Portal Identification &amp; Authentication</a>
7	<a href="#">Network Communications Security</a>
7.1	<a href="#">Secure Network Connections</a>
7.2	<a href="#">UnSecure Network Connections</a>
7.3	<a href="#">Wireless Access Point Security</a>
7.4	<a href="#">User Remote Access</a>
7.5	<a href="#">Dial Out Modem Connections</a>
8	<a href="#">Information Security Incident Management</a>
9	<a href="#">Business Continuity Management</a>
9.1	<a href="#">Continuity Plan Risk Assessment</a>
9.2	<a href="#">Business Impact Analysis</a>
9.3	<a href="#">Recovery Alternatives</a>
9.4	<a href="#">Continuity Plan Development</a>
9.5	<a href="#">Continuity Plan Testing</a>
9.6	<a href="#">Continuity Plan Updates</a>

**Disclaimers** esp re CDSP

Samples:

Licensee acknowledges and agrees that the Licensed Software and System furnished by Vendor are information management tools only and that they contemplate and require the involvement of Licensee's learned intermediaries. Licensee further acknowledges and agrees

that Vendor has not represented its System as having the ability to diagnose disease, prescribe treatment, or perform any other tasks that constitute the practice of medicine or of other professional or academic disciplines. In addition, all clinical content (“Content”) has been developed and reviewed by Vendor based upon published data and the experiences of qualified professionals whenever possible; however, it is Licensee’s responsibility to validate all Content against its standard operating procedures, and all federal, state and local regulations.

Licensee acknowledges that Vendor: (a) has no control of or responsibility for the Licensee’s use of the Content, (b) has no knowledge of the specific or unique circumstances under which the Content provided may be used by the Licensee, and (c) has no liability to any person or entity for any change made to or data or information added to the Content by the Licensee or any party other than Vendor.

Clinical Content. Purchaser understands that the Clinical Content is an information management and diagnostic tool only and that the Clinical Content does not have the ability to diagnose disease, prescribe treatment, or perform any other tasks that constitute the practice of medicine. Clinical Content reflects clinical interpretations and analyses and cannot alone either (a) resolve medical ambiguities of particular situations; or (b) provide the sole basis for definitive decisions. All ultimate care decisions are strictly and solely the obligation and responsibility of the health care provider.

### **Test Data and Tests**

Whenever possible production data should not be used. In the event that training or tests must occur with production data the data should be de-identified as much as possible to meet the minimum necessary test.

Visitors should be trained and consideration should be given to requiring a confidentiality agreement from visitors.

Sample Site Visit Confidentiality Agreement:

#### **TRINITY HEALTH SITE VISIT CONFIDENTIALITY AGREEMENT**

I understand that as part of a site visit at \_\_\_\_\_(Site Name) \_\_\_\_\_ (“Site”), I may come in contact with Confidential Information (as defined below). As such all site visitors are required to read, sign and abide by the terms and conditions of this Trinity Health Site Visit Confidentiality Agreement before participating in the site visit. This requirement includes site visitors who are participating via phone or electronic communication media.

Confidential Information shall mean all non-public information, whether verbal, visual or written, related to the Site, its patients, vendors, employees, and affiliates, including, but not limited to, information relating to:

- Patients’ Protected Health Information (PHI) such as patient medical records, charts, diagnoses, treatment, demographic data, identifying numbers, insurance data, financial information, etc.
- Employment records; and
- Business records.

THEREFORE, in exchange for my participation in the site visit, I hereby acknowledge and agree to the following:



1. I understand that I have no right or privilege to access or view any Confidential Information and the Site has the right to deny me access to any and all information.
2. I understand and agree that I will only observe Confidential Information in the context of the site visit and will not record, capture or duplicate any or all information.
3. I agree not to disclose any Confidential Information obtained during the site visit and to use the Confidential Information only for my education regarding the functions demonstrated at the site visit.
4. I agree to immediately notify the Site of any use or disclosure of Confidential Information not permitted by this Agreement of which I become aware.
5. In the event that I take a guided tour of the Site, I agree not to stray outside of the area permitted by the Site's tour guide.

Date: \_\_\_\_\_

Visitor's Signature: \_\_\_\_\_

### **Monitoring**

Several monitoring reports are useful in assuring the privacy and security of PHI:

VIP

Same last name

Unusual activity

### **Sample Contract Clauses**

Meaningful Use. Supplier shall ensure that the Products provided under this Agreement are compliant with and provided in conformance with the criteria for meaningful use for an electronic health record, including the privacy and security criteria. Supplier also shall ensure that the Products are compliant with regulations applicable to Payment Card Industry compliance, data breach reporting, patient rights and federal and state electronic records regulations. Supplier shall comply with Trinity Health's interpretation of state and federal regulations of which Supplier has been informed in writing by Trinity Health.

### **ASP-HOSTING TERMS AND CONDITIONS**

ASP Services.

Host Computer System.

Interfaces.

Industry Standards.

Technical Assessment.

Documentation and Controls.

Security Policies.

- Identity Authentication & Access.
- Information Access Policies.
- End-user password security.
- Secure Access.
- Unique Identification.
- Authentication.
- Data Access Controls.
  - Auditing and Monitoring.
- Access Logs.
- Incident Reports
- Right to Audit.
  - System Administrators.
- Minimum Number.
- Background Checks.
  - Physical Security of Data and Remote Connectivity Centers.
- Location.
- Access.
  - Data in Transit.
  - Service Level Agreements.
- Availability of Services.
- Downtime.
  - ASP Services Minimum Warranties.

## **TERMS**

ASP Services. Supplier agrees to provide the ASP Services set forth in the ASP Services Exhibit (“Services”). Supplier grants Trinity Health, including its Authorized Users, a non-exclusive right to remotely access and use the ASP Services and any related Software set forth in the ASP Services Exhibit. ASP Services shall meet, at a minimum, the requirements in this Agreement and the ASP Services Exhibit.

Supplier’s Host Computer System.

Interfaces.

Industry and Security Standards. Supplier shall maintain the security and integrity of the Host Computer System and ASP Services consistent with industry standards for comparable services, including but not limited to maintaining access controls, firewalls, wireless and mobile device and storage security, virus scanning/protection software, anti-malware software, encryption of data in transport and storage (including backup data), and network security intrusion protection systems. Supplier shall not take any action that could jeopardize the confidentiality, integrity, availability or security of Trinity Health or patient data. To the best of Supplier’s efforts and in accordance with industry standards, the ASP Services will not contain any malware or programming devices (e.g. viruses,

back doors, timers or other disabling devices, etc.) which would (i) disrupt the use of the services to which Trinity Health's network is interfaced or connected; or (ii) destroy or damage data or make data inaccessible or delayed.

**Technical Assessment.** Trinity Health has conducted a technical assessment of the ASP Services. Supplier shall take all actions identified in the technical assessment as required to ensure compliance with Trinity Health's standards for privacy and security. Supplier shall maintain the ASP Services in accordance with the descriptions provided in the technical assessment of Supplier's compliance with the ASP Hosting procedures and notify Trinity Health of any deviations from the functionality reviewed in the assessment. To the extent of a conflict between the requirements of this Agreement and the descriptions of Supplier's ASP Services in the technical assessment the requirements of this Agreement control.

**Documentation and Controls.** Supplier shall maintain a security program with an identified security official responsible for the operations and performance of the program and notify Trinity Health of the name, title and security certifications and any changes. Annually, Supplier must provide documentation of the controls and currency of the controls for website security, assurance of uptime and compliance with service level agreements and timely response times, physical security of the host computer location and equipment, timely responses to and notification of security incidents/issues, database and transmission encryption, data quality/corruption prevention, timely return/destruction of data, compliant use of copyright & logos, and restrictions and security of use of portable media.

**Security Policies.** Supplier shall maintain information security policies that specifically address the confidentiality, integrity, and availability of its facilities, systems, and the information in its possession and control. Supplier's security policies must be made available to Trinity Health upon request.

**Identity Authentication & Access.**

**Auditing and Monitoring.**

**Access Logs.** Supplier shall ensure that its security procedures include review and examination of system access and event logs, and/or activities to evaluate the utilization levels, efficiency and technical capabilities of the host computer network and each user's compliance with this Agreement. Supplier agrees to monitor and audit all access to and use of the host computer network. Access event activity logs will be maintained for 60 days. The access log will show, at a minimum, date, time, data accessed, source IP address, and the identity of the user as to each event of access to data on the host computer. The access log will be sortable, using commonly available means, by date, user, and/or by the name of individual(s). Supplier will make the access log available promptly to Trinity Health for auditing or monitoring.

Incident Reports. Supplier will (i) promptly report to Trinity Health any access, use or disclosure of Trinity Health data not permitted by this Agreement; (ii) any successful security incident of which Supplier becomes aware; and (iii) in summary form, upon request of Trinity Health, any unsuccessful security incident of which Supplier becomes aware.

Right to Audit. Supplier shall permit Trinity Health (or its contracted agents) to conduct periodic audits of including without limitation, the Supplier's facility, security controls, security vulnerabilities, adherence to Trinity Health policy, including security requirements, reports, documentation necessary to test the existence of information security controls, orders, invoices, volume reports, discounts, and performance under this agreement. The audits shall be conducted upon reasonable advance notice during regular business hours and in such a manner as not to unduly interfere with Supplier's operations. Trinity Health reserves the right to review the audit results and discuss and mutually determine audit items that may need resolution and/or mutually develop plans and procedures to address any changes based on the findings from the audit.

Availability of Audits. Supplier will provide Trinity Health with any current-year, independently conducted, third-party audit or assessment report that includes testing of general and technology-based controls for the specific scope of work to ensure that the Supplier is compliant with policies, procedures, standards and applicable regulatory requirements.

System Administrators.

Physical Security of Data and Remote Connectivity Centers.

Data in Transit.

Service Level Agreements.

Availability of Services. The ASP Services shall be available seven (7) days a week, twenty-four (24) hours a day ("Hosted Application Hours"). The ASP Services will be fully operational and accessible using Internet access methods commonly in use within the industry, including transmission security. Supplier will provide customer service support by phone during standard business hours for each Trinity Health location to resolve any issues that may arise with respect to the ASP Services. Services response times and corrective actions shall be specified in a Support Exhibit.

Downtime. Supplier reserves the right to schedule reasonable downtime during non-standard business hours. Unscheduled downtime shall not include downtime attributable to Trinity Health's hardware or systems. Reliable access and use of

the services is of the essence and Trinity Health shall be entitled to appropriate credits or termination for any excessive downtime.

**AGREEMENT BETWEEN TRINITY HEALTH AND VENDOR WHEN THERE IS NO PHI USED OR DISCLOSED**

The parties agree that Vendor’s services and functions do not require the use or access to protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act 1996, as amended (HIPAA).

Members of vendor’s workforce may perform services on site at a health facility. They may have the opportunity to access or see PHI that is being used by the facility for treatment, payment or operations. Vendor agrees that it shall instruct its workforce regarding the confidentiality of PHI and shall not permit members of its workforce to access, view, obtain, copy, review or use PHI. Vendor agrees to instruct its workforce to decline to view PHI and to promptly return or destroy any PHI that is erroneously shared or delivered to Vendor. Vendor agrees to maintain strict performance standards, including disciplinary actions, with respect to wrongful access to, copying, viewing, misuse or disclosure of PHI.

\_\_\_\_\_  
Vendor Date

\_\_\_\_\_  
MO representative Date

*(person that signed contract with vendor)*

Due Diligence Checklist for Vendor Evaluation

**Electronic Data Interchange**

**The questions below should be answered with respect to data exchange with Trinity Health’s external business partners. These are utilities providing secure, automated data transmissions between Trinity application servers and authorized, external vendors / trading partners. In addition, secure batch file transfers (between Trinity Health applications/systems) are considered EDI.**

Describe the requirements for EDI. Be specific and include a diagram..  
Describe the method of internal data movement utilized with the software/application (e.g. NFS, FTP)?

Does the solution contain customized code or utilize any 3rd party software utilities to process in part or in total EDI files or reports? If so, is Trinity Health required to use the provided solution or will you support other solutions? Describe how your technical teams work with Trinity Health to develop, integrate or automate EDI transmissions as required by the software/application?

**Authorization:**

How does the solution allow for data access controls?

**Communication Control:**

Does the solution store or transmit Protected Health Information (PHI)? Does the solution provide data encryption in transit? If so, describe the type, level, & strength of the encryption. Does the solution provide data encryption in storage? If so, describe the type, level, and strength of the encryption.

**Auditing/Reporting:**

Is there the ability to report on the status of user IDs, including inactive IDs? Is the solution able to capture system log data? Specify available logging. Describe the solution's security logs, and/or audit trails and audit reporting capabilities. What data is captured? Describe the solution's capabilities for archiving and/or purging log files.

**System Security:**

What is the session timeout setting for your application? Does the system require that Virus protection be disabled for specific files/folders for the system to function properly? If so, please specify the requirement. Has this solution been security tested? If so, please specify who completed the testing. Has the hosting facility undergone industry recognized security certification, such as SAS70? Describe and provide the resulting documentation. Does this solution have documented best-practice security configurations and processes? Describe. Does this solution require or encourage the use of shared user accounts? Outside of the operating system, are user credentials cached anywhere in the system? If so, how are they protected from unauthorized use? Are users required to be granted direct access to systems, environments, or partitions outside of the applications? Who owns the security responsibilities in your organization (Name & Title)? Include security organizational chart. Describe the solution's interoperability requirements, capabilities and limitations with various network security environments, including but not limited to Network-based "stateful" firewalls, VPN's, Network-based Admission Controls (NAC), and Intrusion Detection/Protection Systems.

Another resource to review to facilitate selection of an EHR system with safeguards to reduce the likelihood of falsification is from AHIMA. See Appendix C: Steps to Prevent Fraud in EHR Documentation [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_033095.hcsp?dDocName=bok1\\_033095](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_033095.hcsp?dDocName=bok1_033095)

## **Cyber Insurance**

**Cyber-Insurance.** Supplier shall provide, at Supplier's sole cost and expense, throughout the Term of this Agreement the following insurance types and limits issued by an insurance company authorized to do business in the applicable states:

Privacy and Network Liability insurance in a minimum amount of Five Million Dollars (\$5,000,000) per incident and annual aggregate.

**Security Background Checks.** Supplier shall require acceptable results from security background checks on all system administrator users of the host computer system.

## **Sample Notice letters**

### **Letter to Former Employee**

Date

Former Employee Address

**RE:** Warning – Alleged HIPAA Violation by Former Employee

Dear \_\_\_\_\_:

#### **This letter is to serve as your first and final warning letter:**

Recently, (Hospital name) received a complaint from a patient alleging that you unlawfully disclosed patient information to an unauthorized third party.

As you know, even though you are no longer employed by (Hospital Name), we are obligated to thoroughly investigate this important matter and report any confirmed violations to the DHHS's Secretary and the Office of Civil Rights. You should be aware that if our investigation results in confirming that a violation did in fact occur, that this behavior will subject you to direct federal and state criminal exposure (e.g., effective 02/17/09 under the HITECH Act), civil penalties, along with a direct violation of the Iowa's Board of Nursing Administrative code regarding the confidentiality and privacy rights of patients (IA ADC 655-4.6(4)(i)).

As such, if you are disclosing information about patients that you obtained during your employment with (Hospital name), we strongly advise you to stop violating the law and cease and desist from disclosing any of our patients' PHI to any third party, which is a violation of both federal and state law. We will take any and all necessary legal action to protect the privacy, confidentiality, and rights of our patients.

Signature

Hospital Privacy Officer

### **Letter to Patient**

Date

Dear Ms. Patient:

#### **This letter is to serve as your first and final warning letter:**

Recently, you notified us that you had in your possession a list containing the names and other identifying information about certain Hospital patients. While we appreciate that you brought this concern to our attention, we remain concerned that you have not cooperated with our efforts to bring resolution to this matter.

In furtherance of our obligations to investigate privacy concerns, and implement necessary corrective measures, we requested that you return the list on two different occasions. In each instance, you refused to do so.

Hospital is obligated by law to keep patient information private. Hospital is also obligated by law to implement corrective measures in the event of any inadvertent breach of patient information. You wrongfully obtained Hospital's patient information and you are inhibiting Hospital's ability to comply with the law.

Hospital is obligated to report certain privacy violations to the U.S. Department of Health and Human Services' Secretary and the Office for Civil Rights. You should be aware that if you do not return the list by May 25, 2012, your behavior may subject you to direct federal and state criminal exposure (e.g., effective 02/17/09 under the HITECH Act), and/or civil penalties triggered by Hospital's reporting of events.

Importantly, your disclosure of the information you have in your possession to any third party is a violation of both federal and state law. We will take any and



all necessary legal action to protect the privacy, confidentiality, and rights of our patients.

It is our hope that we receive your cooperation. We strongly advise you to return the list as soon as possible.

Sincerely,

Privacy Officer