A State Policy Paper on
Health IT Security

Enhancing Privacy and Security of Protected Health Information In the State of Utah

Through
Education, Training, and Technical Assistance

Submitted to

David W. Patton, PhD
Executive Director
Utah Department of Health

With Recommendations for

Utah Governor Gary R. Herbert's Office

By
Utah Digital Health Service Commission

288 N. 1460 W.
Salt Lake City, Utah 84116
health.utah.gov/phi/

December 2012

CONTENTS

EXECUTIVE SUMMARY

The State of Utah is a national leader in Health Information Technology (HIT). We are consistently striving to achieve outcomes that result in improved quality and decreased costs of health care. Realization of the HIT investment must have constant vigilance over the security and privacy of our information systems. To this end, the Utah Digital Health Service Commission (DHSC) has developed this white paper, through a public process of reviewing current information technology practices and making recommendations to protect Utah healthcare providers and the health industry from breaches of Protected Health Information. This white paper discusses the current challenges of HIT security and privacy, including unsecure uses of mobile devices; identifies the weakest links in HIT security and health information exchange; and proposes solutions by identifying best practices, available resources, and provides questions with answers regarding privacy and security of electronic health systems for practitioners.

The Utah Digital Health Service Commission is a governor-appointed statutory policy advisory body (§26-9f). Its mission is to facilitate and promote the adoption of the secure, effective and efficient exchange of electronic health data and services, as a means to reduce health care costs, enhance quality, increase access, and improve medical and public health services.

INTRODUCTION

The healthcare system in the State of Utah has made, and continues to make, significant investments in Health Information Technology (HIT) systems. These investments have been made with both public and private dollars. These investments are being made with the expectation of a return on investment (ROI) in the form of improved quality outcomes and decreased costs (i.e., improved value). A recent Institute of Medicine (IOM) report reaffirmed potential cost reductions on the order of 30 percent based on system changes that leverage improved information flows from HIT investment. These cost reductions are realized due to outcomes such as reduced duplication of services, hospital admissions, emergency room visits and adverse drug reactions, as well as decreasing fraud[1]. However, any ROI will only be realized to the extent that these systems are secure and individual privacy is maintained.

More than 21 million individuals' Protected Health Information (PHI) have been breached in the 49 states and District of Columbia and reported to the Office for Civil Rights at the U.S. Department of Health and Human Services since 2009[2]. A survey of 72 health care organizations conducted by Ponemon Institute in Michigan, estimated that on average data breach incidents cost these benchmarked organizations more than $2.2 million per incident. According to the study, the cost of data breaches continues to rise[3].

In April 2012 the State of Utah detected a data breach on a computer server that stores personal health information. Information on the server included claims payment and eligibility inquiries. This could include sensitive, personal health information from individuals and health care providers such as Social Security numbers, names, and dates of birth, addresses, diagnosis codes, national provider identification numbers, provider taxpayer identification numbers, and billing codes. Approximately 780,000 individuals had personal information compromised as part of the breach, of those, approximately 280,000 had their Social Security numbers compromised. The State of Utah took immediate and on-going actions to restore data security and re-establish public trust. Still, the state of Utah incurred a significant negative impact on its national reputation as a leader in HIT systems due to this incident.

The Utah Digital Health Service Commission (DHSC) had identified the potential lack of adequate protection of sensitive health information for Utahns before the data breach was discovered. The data breach highlights the urgency for statewide actions. DHSC held five public meetings in 2012 and received public testimony from representatives of healthcare providers, higher education, professional colleges, IT

[1] Institute of Medicine, Best Care at Lower Cost, edited by Mark Smith, et al. National Academy of Science, 2012. Prepublication copy.

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html as of October 20, 2012

[3] http://www.healthcare-informatics.com/article/unsecured-mobile-devices-weak-link

professionals, federally-funded Regional Extension Center, and statewide health information exchange entities.

This white paper is developed through a public process. Its purposes are to help the Utah healthcare industry to identify current information technology practices that may increase risk of PHI security breaches and offer solutions for enhanced protection. DHSC provides recommendations in education, training, technical assistance on protecting PHI for Utah healthcare providers and health industry.

CHALLENGES

New Federal Requirements

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 requires Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities and their associates to adopt more stringent privacy and security provisions. The penalties for violations of privacy, security, and breach notification provisions are substantial. The Centers for Medicare & Medicaid Services (CMS) includes specific security criteria in their core measures of Meaningful Use of Electronic Health Records (EHR). Core measure #15 requires all eligible providers and hospitals to "protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities."[4] Providers and hospitals shall "conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process." [2]

[4] https://ehrincentives.cms.gov/hitech/

Unfortunately, many payers, providers, hospitals, clinical laboratories, and governments face enormous challenges in keeping PHI secure. The biggest weakness identified nationally involves a lack of adequate security measures and the use of unsecured mobile devices.[5]

Potential Weakest Links in Health IT Security

While large providers, systems, and payers are implementing the CMS Meaningful Use requirements, the Utah Medical Association testified that the majority of small and independent clinics lack resources and capacity to update their security measures and are unable to treat IT security issues as a priority. The Utah Hospitals and Health Systems Association expressed similar concerns for independent rural and Critical Access Hospitals. These hospitals and independent clinics need extra technical assistance in assessing and improving IT security to meet the Meaningful Use requirements.

Network Security of the Statewide Health Information Exchange

UHIN which operates the statewide clinical Health Information Exchange (cHIE) utilizes a high degree of security. However, the purpose of the cHIE is to 'connect the dots'. As such, UHIN has connected 43 of the state's 56 hospitals, 305 clinics, and

[5] Leon Rodriguez, Director, Office for Civil Rights, speech at the ONC Annual Conference, December 12, 2012, Washington, D.C..

96 nursing homes as of October 29, 2012. About 200 participating providers, with patient permission, can access their patients' electronic records across health systems. These connections are projected to increase substantially over time. As with the section above, the primary concern of the cHIE is that a data breach at any independent clinic could present a security threat to other integrated health systems and potentially the entire statewide information exchange network. Independent clinics need technical assistance in assessing and improving IT security.

Unsecure Uses of Mobile Devices

Of the 502 data breaches on the OCR web site, 40 percent involved a mobile or portable device reported as stolen or lost[1]. Laptops, USB drives, smart phones, tablets, and iPads etc., are being increasingly used in healthcare practice. Protected health information may be stored on a mobile device unencrypted, and mobile devices may not be set up using a strong password or any password at all. A growing challenge is individuals being able to access facility PHI through personal devices that are not adequately controlled by their employers. DHCS identified unsecure use of mobile devices represents an increased security threat to PHI protection.

Mobile devices continue to be a security concern due to the nature of the devices: mobile, easy to carry, hence easy to lose or a target for theft. Because of the number of different platforms, there is little consistency in how the devices are managed and secured. Ownership of the device is also a concern. Who is responsible for the security of the device? The use of personally-owned devises which may store PHI from an employee's company may significantly increase the security risk window. Source repositories for applications are very questionable in some cases as to the source code vetting that takes place for the applications that are offered to the public. Because there is little or no vetting within some segments of the application markets that are available to the public, there is a possibility that malware can be inserted within source code, which would expose the device and all data that transit through the device to be compromised. Portability creates a problem in that mobile devices remove the ability to create secure perimeters within an organization. The loss of boundary between private and professional activity can present a problem in that data leakage occurs with sensitive data moving from a protected professional environment to the personal environment without the user being aware that data is leaking across that boundary.

Social Media Applications

The concern about social media applications are that there is no assurance of the level of protection that is afforded to users who participate in the social network. Social media sites exist to make money. If the end-users are not paying then some entity is paying the social media application to gain access to the sites users data. This creates issues regarding data integrity and data protection, which is the ability for assurance that the data are not exposed or release inappropriately. For example, if you are asked to include the name of your

employer in a social media application that information can be farmed to targeted phishing attacks.

The social media organizations have attempted to implement security within their applications, but as of yet, the security of the environment cannot be assured. As an example, banner ad companies sell space to whom-ever wants to pay. So if you are a user of the social media site, they can add you to the survey so that when you open up the banner, it is programmed to add software to your computer which may infect or allow data to be withdrawn from your computer. Healthcare professionals should be very cautious about what data are placed within a social media environment and how employees are interacting with social media while using company computers.

Cloud Computing

As IT costs increase, cloud computing is an area that offers significant potential for cost reduction. Cloud computer offers the ability for rapid provisioning and de-provisioning of resources and a high degree of scalability. This translates to the ability to offer a wide variety of low cost services, including the ability to reduce hardware and software replacement cost cycles.

Data within the cloud exist in a transient environment meaning that it is common for data to be rapidly shipped between various data centers by the cloud hosting company. Cloud computing vendors are constantly looking for inexpensive data hosting locations to effectively compete. Data can and will be transferred between these locations without the user's knowledge or consent and any conventional privacy agreements could be made invalid.

The security concern for cloud computing centers over the challenge of creating effective and enforceable service level agreements (SLA), operational level agreements (OLA), and/or contracts, which protect data and/or information that reside within the cloud environment. Cloud providers have been reluctant to alter specific SLA's due to the pressure to reduce administrative overhead and the growing number of customers that are moving to the cloud-computing environment.

Another concern is how the judicial system is viewing data which are stored in a cloud environment. Most recently, cloud environments are being viewed by the judiciary as public spaces. This raises privacy and security concerns as well as questions about protections of patented or copyrighted material.

EXAMPLES OF BEST PRACTICES

The DHSC invited several speakers to present their best security practices and improvement efforts, lessons learned, and to discuss statewide implications:

Risk Analysis of Clinical Practices

As mentioned above, the lack of adequate security practices in entities which hold PHI represent a significant risk. Central Utah Clinic hired an independent security consultant and has conducted a HIPAA security self-audit. This security audit produced eye-opening information for management to take immediate actions to set up additional

physical, technical, and administrative safeguards. All HIPAA covered entities, but most particularly, as discussed above, independent clinics would benefit from a HIPAA security self-audit. It would help them identify and address security risks.

Technical Assistance from HIT Regional Extension Center (REC)

As part of the funding agreement with the Office of National Coordinator for Health Information Technology (ONC), *HealthInsight* provides tools and resources to develop information security policies & procedures and to perform the risk analysis required for Meaningful Use. The tools and resources are available on their website at www.healthinsight.org. Additionally, for primary care providers and critical access and rural hospitals *HealthInsight* can provide direct technical assistance through 2013 – with over 1,000 Utah providers and hospitals already receiving support.

Security of the Statewide Clinical Health Information Network (cHIE)

UHIN, which operates the cHIE, takes privacy and security very seriously. As part of its commitment, UHIN undergoes a rigorous, independent third party accreditation every other year, the most recent being 2012. Because of this practice, UHIN keeps all of its privacy and security practices up to the continually evolving requirements. Sites connecting into the cHIE are required to comply with all HIPAA privacy and security requirements including HIPAA privacy and security training, disaster recovery planning, and security risk assessments and mitigation. All data is encrypted to federal standards both at rest and in motion.
As a testament to the rigor of this bi-annual accreditation, UHIN recently underwent a privacy and security audit conducted by the U.S. Office of Civil Rights (OCR) and passed with no findings. In contrast, of the 112 audits conducted by OCR nationally to date, nearly all have failed.

Telehealth's Privacy and Security

The Utah Telehealth Network (UTN) connects hospitals, clinics, and health departments in support of telehealth and telemedicine, the exchange of health information, and collaboration among health care providers. Sites connecting into UTN's high-speed broadband network are required to comply with their Network & Information Security Policy. Business Associates Agreements and Third Party Network Connection Agreements are signed when appropriate. UTN's telemedicine privacy and security recommendations include: annual training in HIPAA security and patient confidentiality; telemedicine room privacy considerations; use of patient consent forms; and the use of security tools such as encryption, enterprise firewall traversal systems, gatekeepers, Virtual Private Networks (VPNs), and secure email when sharing patient information. UTN works closely with the University of Utah Information Security and Privacy Office and follows their Security and Patient Confidentiality Policy.

Workforce Training on Cyber Crime

The University of Utah requires all employees with access to PHI to pass a role-based, on-line privacy and security HIPAA training course

annually; one component is to improve the awareness of cyber-attacks via email or web based threats and to be prepared for social engineering attacks.

Training is a must, but it can't be the final defense. Testing of the training impact with audits or simulations can help engrain the end-user to react automatically to these threats.

Healthcare Workforce Training and HIT Certificate Program

Salt Lake Community College (SLCC) received HITECH HIT professional training funds in 2010-2011. One important component of that grant was to upgrade the skills of existing employees. SLCC has trained about 300 health professionals in the state of Utah. With new funding from the U.S. Department of Labor in 2012, SLCC will be launching a new Health Information Technology Certificate Program in spring 2013. The program's focus will be to train entry level personnel in health record management, health information security and protocols, health data management and other similar topics.

Professional or career colleges are important training forces for front-line health and IT workers. For example, LDS Business College has produced many certified IT professionals for the health industry. Recently they decided to significantly increase their technology program offerings, including a security curriculum to address increased industry needs.

Privacy and Security Education in Higher Education

Commissioners from University of Utah and Southern Utah University reported that computer science and health professional educational programs in universities provide courses on patient privacy and information security, as well as ongoing training and certification required by regulatory and accrediting agencies. However, privacy and security education in specialties of Management, Marketing, Economics, Finance and Public Administration need improvement in some universities.

Executive management's understanding of security risks and IT compliance are crucial for protecting patient privacy. Policies developed by leaders dictate how the technical systems are adopted, implemented, how training occurs and how the systems are monitored. When management controls are in place, technical expertise can be available and trained front line staffers have the ability to be compliant. Higher education institutions need to provide adequate training for future managers and leaders to understand challenges and requirements on protecting privacy and security of patients' sensitive information.

PROPOSED SOLUTIONS

Health care is beginning the same security evolution the banking industry has undergone[6]. Coordination and collaboration among health systems, public and privacy entities and sectors are

[6] Michael McMillan, National Chair, HIMSS Privacy and Security Policy Task Force, speech at the Utah HIMSS meeting on August 16, 2012

crucial. The Utah Digital Health Service Commission recommends the following possible solutions:

Technical Assistance for Small Practices

Utah relies upon the federal privacy and security requirements and standards. *Like with the government's role in transforming financial systems, the state can help to ensure that patient health information is protected in all health care practices.* With the growing emphasis on exchanging health information between healthcare entities, independent clinics and small rural and critical access hospitals especially could greatly benefit from technical assistance to comply with these security requirements. To this end, the DHSC has compiled a list of questions and answers for understanding privacy and security issues with electronic health record systems (Appendix A).

Coordination of Existing and New Resources to Include Training or Technical Assistance for Targeted Providers

Utah complies with HIPAA regulations. *At this time, the DHSC is recommending that no additional regulations be added at the state level.*

However, the federal standards are fairly broad and can be challenging to understand and implement. The DHSC recommends that Utah adopt specific statewide training modules for covered entities doing business in Utah (see useful links in the section of Resources).

The Utah Medical Association (UMA) and *HealthInsight* REC have begun a discussion to leverage the UMA's existing medical continuing education mechanism and REC's Meaningful Use technical assistance for physicians and office managers through the development of this white paper. DHSC supports inter-organizational collaboration to provide security training and technical assistance to healthcare workforce in Utah.

Training Needs Assessment for Rural Utah

DHSC also recommends that a statewide assessment be conducted to determine if appropriate HIT training is available through rural Utah – either on-site or via distance education. The state of Utah needs training capacity that serves to upgrade the skills of current HIT staff through a certificate program as well as to provide entry level training for those desiring to enter the workforce.

Statewide Training Coordination

DHSC hopes that this white paper can be used to communicate key messages statewide to enhance awareness of these HIT security issues.

DHSC also encourages educational institutions to consider minimal core requirements of IT security education or training for our future health workforce.

Security Management of Mobile Device

The DHSC consulted with experts in the field on mobile device protection and security, and recommends the following:

Host

For devices accessing PHI, enable secure socket layer (i.e., protocol management encryption software) protection when available; register the device with manufacturer, provider, or employer; allow remote wipe of user's device if misplaced, lost, or stolen, and create secure logins for user and device access to databases with PHI.

Users

For devices used to access PHI, the DHSC recommends that companies enable device auto-lock and use of complex passwords, avoid using auto-completes and password caching, connections to unsecure or unknown Wi-Fi networks (i.e., set Bluetooth to non-discoverable), keep operating system updated (i.e., no rooting). Utilizing a two factor authentication may help minimize the risk on non-authorized access.

Special Consideration of Privacy and Security When Using Cloud Computing Services

As mentioned in the previous section, cloud computing - the storage of data on physical hard drives maintained through outside cloud computing vendors, can result in data being stored essentially anywhere; in many cases including outside U.S. jurisdiction; where ever the lowest cost is available. Data can be shipped between many different sites, all unknown to the purchaser of the service.

DHSC encourages healthcare providers, as the end-users, to ask questions on privacy and security when purchasing software services that involve any form of data storage. For example, does the application use cloud computing services? Where does my data physically reside? It is swapped between different sites?
How many copies of my data will be made? To be security-conscious users of cloud computing may influence the practice of securely using cloud technology for all Utahns.

The use of cloud computing is exploding. There is little evidence on best privacy and security practice in using cloud computing services. The DHSC recommends that the state of Utah supports studies of appropriate use cloud computing services as it relates to the security of the healthcare data of Utahns.

RESOURCES

Publicly available resources for education and training on health information privacy and security include:

A. ONC Provider HIPAA training games

http://www.healthit.gov/providers-professionals/privacy-security-training-games

B. ONC Mobile Device Privacy and Security on YouTube
http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

C. HIMSS provider security tool kit
http://www.himss.org/ASP/topics_pstoolkit.asp

D. Utah Regional Extension Center at *HealthInsight*
http://www.healthinsight.org/Internal/REC.html

E. Health Information Technology Certificate of Completion Program at Salt Lake Community College
http://www.slcc.edu/hit/index.aspx

F. Course Era:
Free online courses in Information Security, Information Systems/ Computer science, and healthcare.
https://www.coursera.org/

G. Cyber Security Awareness Video:
Amazing mind reader reveals his 'gift'
http://youtu.be/F7pYHN9iC9I

H. The DHSC developed the following check list of points for consideration of a HIT security assessment:

a. Vendor
- i. Vendor contract should include clauses on confidentiality according to HIPAA privacy regulation
- ii. A regulation should be in place to provide a capability to toggle vendor access on and off, providing access only when required
- iii. Must have procedures covering the monitoring of vendor access through audit logs.
- iv. Database should be encrypted and all data transfers are made with bank-level security. (https, ssl, encryption)

b. Server Plan and Execution of Privilege Separation of Powers (System Administrator from Database Administrator)

i. Physical Recommendations:
1. Security
2. Disaster Recovery Plans
3. Network Connection Backup
4. Redundant Power
5. Storage Media Transport and Disposal Protocols

ii. Security of Operating System:
1. User Authentication
2. Patching
3. Resource Controls
4. Additional Security Controls
5. Security Testing of Operating System
6. Ongoing Configuring, Protection, and Analysis of Log Files
7. Recovery

iii. Security Management Practices:
1. System Wide Security System Policies
2. Configuration/Change Control/Management
3. Risk Assessment and Management
4. Security Awareness and Training
5. Certification and Accreditation

c. Mobile Devices
i. Host
1. Enable SSL protection where available
2. Enable registration of device
3. Enable remote wipe of user's device
4. Enable logging user access and device access to database

ii. User
1. Enable device auto-lock
2. Enable passwords, require complex passwords

3. Avoid using auto-completes and password caching
4. Avoid unknown Wi-Fi networks, set Bluetooth to non-discoverable
5. Keep OS updated, no rooting of devices
6. Use anti-virus as it becomes available for device
7. Use data encryption for device and its memory storage
8. Know what you are downloading. Make sure you download apps from reputable developers
9. Remove ALL extraneous applications from every machine with access to PHI (including email)

iii. Physical

1. Education of users on storage of Confidential data
2. User caution-unknown email and text messaging
3. Never leave mobile device unattended
4. Immediately report loss or theft of device

ACKNOWLEDGEMENTS

This state policy white paper was initiated and developed by the Utah Digital Health Service Commission (DHSC) with broad public input. The DHSC chair, vice chair and its members are listed below with their representativeness and affiliation:

Mark Munger, Chair, Non-physician health care provider, College of Pharmacy University of Utah
Doug Hasbrouck, Vice Chair, Physician Involved in Telehealth, *HealthInsight*
Scott Barlow, Telehealth consumer advocate, Central Utah Clinic
Henry Gardner, Telehealth Advocate, Zions Bankcorp
Deb LaMarche, Member uses telehealth, Utah Telehealth Network, U of U
Brad LeBaron, Representative for licensed health care facilities, Uintah Basin Medical Center
Chet Loftis, Representative for the health insurance industry, Public Employee Health Program
Marc Probst, Member uses telehealth in serving medically underserved population, Intermountain Healthcare
Dennis Moser, Rural health consultant, Utah Center for Rural Health, Southern Utah University
Jan Root, IT professional involved in telehealth, Utah Health Information Network
Wesley Smith, Representative for Public Interests, Salt Lake Chamber of Commerce
Nancy Staggers, Nursing Representative, College of Nursing and Department of Biomedical Informatics, University of Utah

Partners Who Contributed to the White Paper

Patricia Carroll, Utah Telehealth Network
Scott Horne, Utah Hospitals & Health System Association
Felix Littlefield, Salt Lake Community College
Gary Mackelprang, PrimeCare Direct
Michelle McOmber, Utah Medical Association
Craig Nelson, LDS Business College
Wyatt Packer, *HealthInsight*
Jerry Smith, University of Utah Health Care Information Security Office
Jamie Steck, Central Utah Clinic
Weston Tolman, College of Pharmacy, University of Utah

Utah Department of Health's Contributors

Robert T. Rolfs, Deputy Director, UDOH
Tom Hudachko, Public Information Officer
Esther Munene, CDC /APHI Fellow
Barry Nangle, Center for Health Data
Humaira, Shah, Office of Health Information & Data Security (OHIDS)
Wu Xu, OHIDS

APPENDIX A: EHR SECURITY

There are two basic implementation methodologies for electronic health record systems: local hosting (the EHR software, server and all records reside in the clinician's office) and Software as a Service (SaaS) or cloud-based (the EHR application and records reside off-site and are accessed via the Internet or a VPN connection). Security concerns will vary subtly according to implementation method. Regardless of the method, however, the following general questions can serve as a guideline with EHR vendors: (Question: *Answer*)

1. Vendor contract should contain explicit guarantees and assurances about security. Inquire about the specific threat and vulnerability technology used by the system. Some specific questions you might want to ask:

a. How does the vendor identify threat vectors and test for new vulnerabilities? *The vendor's ability to safeguard your data depends on the answer to this question. In short, the vendor should understand all common attack methodologies and countermeasures. Because the field evolves very quickly, it is imperative that the vendor have in-house expertise that subscribes to and carefully studies IT security forums, lists, news groups and blogs. Networks that contain PHI must be on the 'cutting edge' of computer security.*

b. Is all PHI encrypted when transmitted over the Internet? How is it encrypted? *All transmissions should be encrypted over a secure socket layer/virtual private network. Encryption protocols vary; 256 bit is a good industry standard as of 2013.*

c. How are patches and updates administered? *Updates are released daily, many of them address important security issues. The vendor should subscribe to a management service or at the very least run auto-updates.*

d. Describe the network topology: are production servers hardened and firewalled with intrusion detection? *They should be; multiple tiers of firewalls are better than a single tier and various types of intrusion detection are better than a single type. Hardened servers are servers that have been stripped of any and all extraneous applications and attachments*.

e. Is the system stateless? *There should not be any data left on local work stations when the Internet connection is terminated or when the local machine is turned off at the end of the day*.

f. Does the vendor maintain comprehensive audit logs so that every user's actions are accounted for? How are these audit logs

stored? Who has access to them? *Every keystroke of every user should be tracked and stored in an audit log. The logs should be read-only and access issues should be left to clinic management*).

g. How does the vendor authenticate users? Does it employ two-part authentication? Does the system require complex passwords? Does it support bio-authentication? *A user ID and password are relatively easy to compromise and don't provide very good security. A second form of authentication; something external to the system and in possession of the authorized user increases the likelihood that the user is legitimate. Complex passwords--a combination of numbers, letters and special characters with good password control (requiring regular changes-- is optimal. Bio authentication is good, but not fool-proof on consumer grade machines (it shouldn't be used as a replacement for other security measures).*

h. Are users granted role-based access? How granular is the definition of roles? *They should be; Office of National Coordinator for Health Information (ONC) requires it and common sense dictates it. Administrative, clinical, prescribing, scheduling and billing should have separate privileges.*

i. Does the vendor's software appropriately filter malicious user input and extraneous error conditions (a frequent cause of security shortcomings such as SQL injection or forced browsing)? *This, like Q/A a and c above, require considerable in-house expertise to regulate. Malicious attacks that exploit user input fields can be sophisticated and require great expertise to identify and disable.*

j. Describe physical security at the data center. Where is the data center located? Is the data redundant (stored in two geographically distributed locations)? How are backups handled? *The ideal data center should be located in a limited access, highly secure facility. At a minimum, it should boast redundant power, redundant telecom, and redundant application servers. Ideally, it should be certified. The old SAS 70 standards are dated and largely irrelevant; rather, look for SSAE 16 and SOC2 / SOC3 certifications. Multiple, redundant data centers in diverse locations are preferable to a single data center.*

k. Describe disaster recovery plans. *The vendor should have a written disaster recovery protocol that will ensure that there is no data loss and minimum down-time in the event of a catastrophe.*

l. How does the vendor dispose of end-of-cycle equipment? Are hard drives degaussed and properly disposed of? *Hard drives and other magnetic storage media should be thoroughly degaussed and preferably destroyed at end-of-life*.

2. Does the vendor submit to a regular (at least annually) third-party security audit by an accredited auditing firm to ensure it is in compliance with the

HIPAA privacy and security rules? The results of this audit (and past audits) should be available for review. *Vendor should submit to such audits and the results should be available for inspection. The third-party auditor should be of national prominence.*

3. What kinds of third-party connections does the vendor allow? How are third parties vetted for security compliance? *Third-party connections (with labs, radiography facilities, health exchanges, etc.) are inevitable. Does the vendor require connections to adhere to the same security requirements observed by the vendor?*

4. How does your vendor announce product updates and upgrades? How do you validate legitimate vendor communications? *Such announcements should be through authorized, well-established channels (not email). Ideally, such announcements / updates should be delivered centrally in the case of SaaS systems or via registered mail in the case of locally hosted EHRs.*

5. Is the vendor's corporate computing environment segregated from its EHR production environment? *It should be. In other words, the vendor's email servers, development servers, test environment, etc. should be completely segregated and firewalled from the production servers.*

6. Inquire about the vendor's workforce education. Are the vendor's employees conversant with HIPAA and knowledgeable about security of PHI? *The workforce should receive formal training from a certified body.*

7. Does the vendor assist with local security implementation (e.g., wireless network setup, anti-virus, spyware and malware protection, suggested workforce IT policies and procedures, etc.)? *They should.*

8. Has the vendor experienced any data breaches? *Hopefully no, but if yes, ask for details.*

9. Does the vendor offer remote support? If so, will that entail access to your computing environment? How will the vendor gain that access and protect the session?

10. Will the data be stored in an HL7-compliant format? How will you obtain and protect your data if the vendor fails or is acquired by another company? *Data should be stored in an HL7 compliant format so that it can be retrieved from the vendor's system in a usable format should you decide to leave the vendor. Make sure you understand what is entailed in getting your data (ALL your data) from the vendor—some charge exorbitant fees to give you your own data! A description of your rights to your data (and attendant costs) should be contractually stipulated.*