

HRSA Health Information Technology and Quality Webinar

**“Privacy and Security – What Questions
Should You Ask Your Vendor?”**

Date: 8/19/2011

US Department of Health and Human Services
Health Resources and Services Administration

Office of Health Information Technology and Quality

Additional HRSA Health IT and Quality Toolboxes and Resources including past webinars can be found at:

<http://www.hrsa.gov/healthit>

<http://www.hrsa.gov/quality>

Additional questions can sent to the following e-mail address:

HealthIT@hrsa.gov

- US Department of Health and Human Services
- Health Resources and Services Administration

Upcoming HRSA Health IT and Quality Announcements

- New Items to the HRSA Health IT Site:
 - New Quality Improvement Grantee Spotlight Firsthealth Home Services
 - HRSA Celebrates National Health IT Week from September 12-16, please check out the HRSA Health IT website for information on HRSA's outreach initiatives for that week.
- Next HRSA HIT and Quality webinar, "Impact of ICD-10 on Safety Net Providers" Friday September 23rd, 2pm EST
- Last month's webinar "Tips For Generating and Utilizing Quality Data Reports Using Health IT" now available online
- HRSA "Call for Papers: **Evidence for Informing the Next Generation of Quality Improvement Initiatives: Models, Methods, Measures and Outcomes**" for Journal of Health Care for the Poor and Underserved.

Abstracts Due September 1st. Questions? Please contact OHITQPapers@hrsa.gov or see the HRSA Quality Improvement website for more information

Introduction

Presenters:

- Laura Rosas-Office of the National Coordinator for Health Information Technology
- Richard Sanders-The Sander's Law Firm and General Counsel Georgia PCA
- Holly Schlenvogt-Wisconsin Health Information Technology Extension Center

HIPAA Security and Contracting with EMR Vendors

HRSA Webinar

August 19, 2011

Richard D. Sanders

**General Counsel, Georgia Association for
Primary Health Care**

The Sanders Law Firm, P.C.

**3525 Piedmont Road
7 Piedmont Center, Suite 300
Atlanta, Georgia 30305
(404) 364-1819**

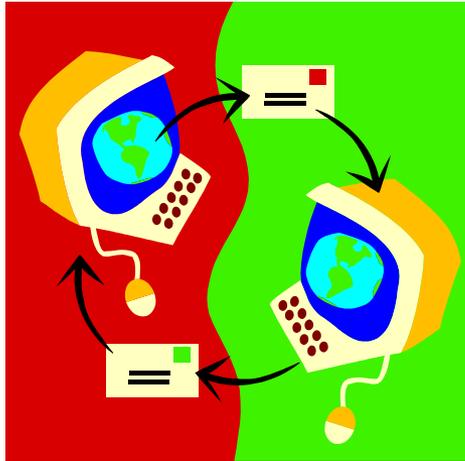
rsanders@southernhealthlawyers.com

www.southernhealthlawyers.com

Overview of the Privacy Rule

- The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) established, for the first time, a set of national standards for the protection of certain health information.
- The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule, effective April 14, 2003, to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Congress was concerned about the impact of technology on the protection of patient information.
- The Privacy Rule standards address the use and disclosure of individuals’ health information (“PHI”).
- A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information through technology to provide and promote high quality health care and to protect the public's health and well being.

Purpose of the Security Rule

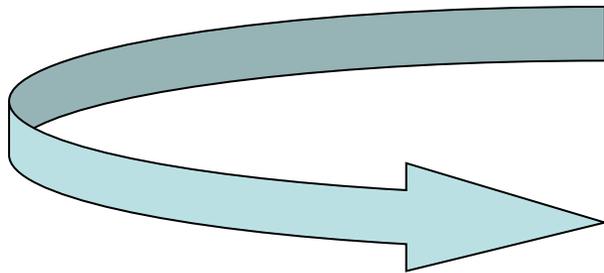


➤ To safeguard PHI that is maintained or transmitted in electronic form

➤ To protect the confidentiality, integrity, and availability of PHI with standards that apply to both a covered entity's internal and external activities

What are the Requirements of the Security Standards?

3 Safeguard Categories:



Administrative

Physical

Technical

Security and Privacy

Administrative Safeguards require the development of P&P's addressing:

- the security management process;
- assigned security responsibility;
- workforce security;
- information access management;
- security incident procedures;
- security awareness and training;

Security and Privacy Administrative Safeguards (Cont'd)

- contingency plans
- evaluation of the effectiveness of compliance measures for technical and non-technical measures; and
- business associate contracts and other arrangements

Physical Safeguards require the development of Policies and Procedures addressing:



➤ facility access controls

relates to interior & exterior of a building

➤ workstation use & security



includes portable devices and device and media controls

Sample of Various State Privacy Laws Impacting Privacy and Security through Information Technology

- In California, a health care provider may prepare a summary of the record for inspection rather than allowing access to the entire record, as long as the summary of the record is available to the patient within 10 working days from the date of the patient's request. (*Ca. Health & Safety Code 123130(a)*)
- In Florida, medical records may not be furnished to, and the medical condition of a patient may not be discussed with, any person other than the patient or the patient's legal representative or other health care practitioners and providers involved in the care or treatment of the patient, except upon written authorization of the patient." (*Fla. Stat. 456.057(7)(a)*).

Security and Privacy

Technical Safeguards require the development of policies and procedures addressing:

- access control
- audit controls
- integrity
- transmission security
- personal/entity authentication



Financial Considerations

- Estimated total start up costs (purchasing, installing, training, hiring support staff) to be \$32,000 per physician
- Studies estimate net benefits from EHR use of \$86,000 per physician over a 5 year period
- Some experts feel benefits on this scale are only recognized in hospitals and large health systems rather than small clinics

EHR Vendor Considerations

- There are over 80 private vendors of EHRs
 - Variety of target markets based on both clinic specialty and clinic size
- Contract negotiation is key to Privacy and Security
 - Items of negotiation
 - Software price
 - Hardware installation
 - Implementation and consulting services
 - Hours of support
 - Response and resolution time
 - System upgrades

Contract Terms

- Contract Terms affecting Privacy and Security Compliance include:
 1. Term and Termination
 2. Compensation
 3. Indemnification
 4. Duties and Obligations
 5. Mutual Confidentiality Obligations
 6. Limits on use of PHI
- The terms in a contract are limited by state and federal law

Term

- Contracts with long terms (5-10 years)
 - Probationary period
- Contracts with short terms (1-3 years)
 - Automatic renewal
 - Cancellation notice

Scope of Service

- Describes the services the vendor will provide
- Describes the specialty of the company
- Lists all locations where the company will be required to work



Termination

- For Cause
 - *“Practice may terminate this agreement for the following reasons. . .”*
- Without Cause
 - *“Practice may terminate this Agreement for any reason or not reason at all, upon thirty days notice”*
- For Cause with Cure Period
 - *“Practice may terminate this Agreement upon Vendor’s breach of this Agreement upon notice of such breach and failure of Vendor to cure such breach within 30 days.”*

Termination

- Immediate Termination
 - *“Practice may terminate this Agreement, effective immediately, if (1) Vendor fails to perform the Services in a timely manner, (2) Vendor is excluded or prohibited from doing business with the federal government; or (3) Vendor violates the privacy or security of patients of the Practice.”*
- Notice
 - *“Vendor must give one hundred eighty (180) days notice”*
- Satisfaction Clause
 - *“The Practice may terminate this Agreement if the Vendor’s services do not meet the Practice’s satisfaction.”*

Duties of Vendor that Impact Providers

- Quality/ effectiveness
- Guaranteed “up-time”
- HIPAA Privacy and Security Compliance
- Record Keeping
- Transferability/ exchange
- Assistance upon termination

Representations and Warranties

- Vendor must represent and warrant the functionality of the system
- Vendor must also represent that the system meets the requirements of various standards required under HIPAA

Non-Compete and Non-Solicitation

- In many states, non-compete and non-solicitation clauses must be “reasonable” in length of time, geographic area, and scope in order to be enforceable
- Non-solicitation clauses usually cover 3 items:
(1) Employees; (2) Business Relationships; and
(3) Patients.
- Generally a restriction of two (2) years or less is considered reasonable.

Compensation

- Types of Compensation
 - Project fee
 - License (per user or per seat)
 - Hourly
 - Hybrids
 - Performance bonus

Arbitration/Mediation

- Arbitration is essentially an agreement between parties to try to resolve a dispute outside of the court system.
- The parties agree upon a third party as an arbitrator who will act as a judge and jury.
- Arbitration and Mediation provisions are viewed as good for employers because the process is faster and avoids a jury trial.

THANK YOU!!!

Richard D. Sanders

**The Sanders Law Firm, P.C.
3525 Piedmont Road
7 Piedmont Center, Suite 300
Atlanta, Georgia 30305**

(404) 364-1819

rsanders@rdslawfirm.com



The Office of the National Coordinator for
Health Information Technology



Privacy and Security: Questions to Ask When Choosing an EHR

August 19, 2011

Laura E. Rosas, JD, MPH
Office of the Chief Privacy Officer

Putting the **I** in **HealthIT**
www.HealthIT.gov



Patient and Practice Information – The Castle



Encryption
Back Up/Recovery
Network Security
Audits

Access Controls

Physical Security

Policies and Procedures and Training

Start with Assessing Your Organization



- Where is your Health Center/CAH located? Urban or Rural? Do you have broadband or similarly fast and reliable internet service?
- Will you be using mobile devices? Tablets? Laptops? I Pads? Smartphones?
- How computer savvy is your staff? Do you have IT staff or do you outsource that function?
- Are you planning on joining an HIE?

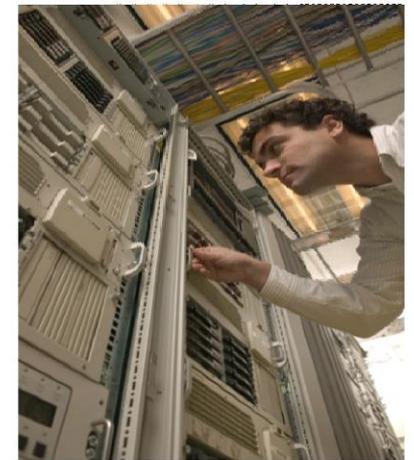
Assessing Your Organization



Are you part of a Health Center Controlled Network or a Regional Extension Center? If so, do they have specific vendors they work with at a reduced cost or for additional services?



Are you planning on giving your patients access to their own PHI? Through a portal? HIE? Interface with an EHR – does your vendor have experience with this?



Software Demonstrations



- Whenever possible, ask to see a live demonstration rather than a canned one.
- Have the right people in the room; whether for an RFP process or the mapping of workflow; include representatives of providers, nurses, medical assistants, IT/security, front desk, billing etc. The feedback they will provide from their unique perspectives will be invaluable, and well worth the upfront investment of their time.



Software Demonstrations



Ask for a demonstration on how to set up each of the security features, especially those features that you will want to be global:

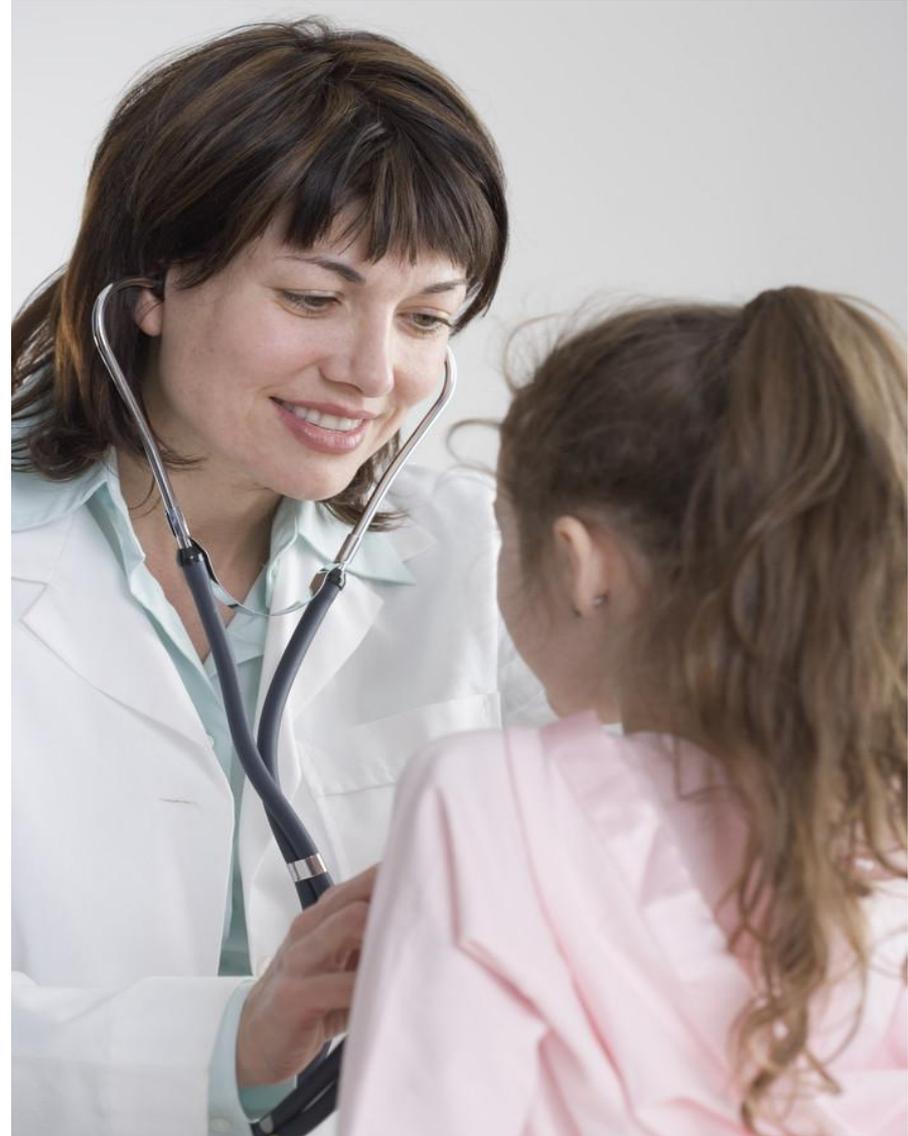
- password difficulty, ie alpha-numeric, 8 characters or more difficult (ie passphrase)
- software time-outs after periods of inactivity
- lock-outs after specified number of wrong passwords

In some EHR software, setting up role or user based access can take hours. In others, the level of granularity may be inadequate for the needs of your organization.

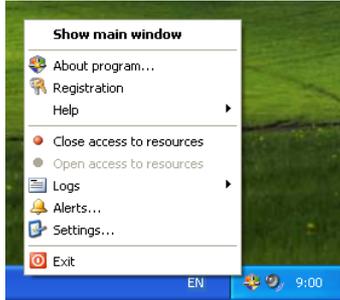
Software Demonstrations



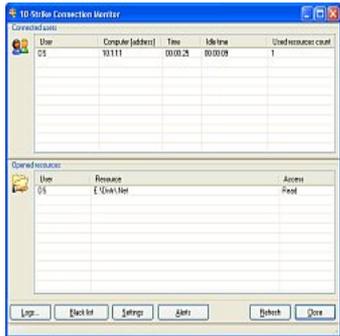
- How does the EHR restrict bills from being sent to patients homes in the case of minor patients consenting to own treatment?
- How does the EHR restrict billing to health plans in accordance with patient requests and new HITECH HIPAA requirements?
- What functions does your EHR have to specially protect (i.e. restrict access) certain patient data? (ie substance abuse, mental health, minor consented health information)



Choosing a Vendor: Demonstrations and Documentation



After starting, the program hides into the system tray displaying the program icon with the context menu. With its help, you can stop or start again the *Server* service which provides the network access to your shared folders



With Our Shared Folder Access Monitoring Program, You Can:
Constantly monitor access to your shared folders, files, printers, and the registry in a real-time

- Ask to see the auditing functions. Are they understandable? Who has access to these features? Is this limited?
- Ask to see how difficult it is to
1) provide electronic copy of patient data
2) paper copy of patient data and how access to those features are configured
- What training and documentation does the vendor provide for these features?

HIPAA's Interaction with Other Federal Laws



- May require permission before sharing certain patient health information: Remain in effect

Federal Statute	Consent/disclosure requirement
42 CFR Pt. 2: The Confidentiality of Alcohol and Drug Abuse	Requires federally assisted treatment centers to obtain individual consent prior to sharing information, even for treatment
Title X of the Public Health Service Act	Requires federal funded family planning clinics to maintain confidentiality of family planning services provided to patients, including minors
Genetic Information Nondiscrimination Act (GINA) of 2008	Requires patient consent for disclosure of genetic information to health plans for underwriting purposes to be incorporated into HIPAA Privacy Rule
The Family Education Rights and Privacy Act (FERPA)	Governs the protection of education records which include student health records



“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”

The End

HIPAA/HITECH Resources



- **Privacy and Security Section of HealthIT.gov:** <http://healthit.hhs.gov>
- **Are you a Covered Entity?:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>
- **HHS Health IT Privacy and Security Toolkit – OCR Guidance:**
http://healthit.hhs.gov/portal/server.pt?open=512&objID=1174&parentname=CommunityPage&parentid=26&mode=2&in_hi_userid=10732&cached=true
- **OCR HIPAA Privacy Rule Training Materials:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html>
- **OCR Guidance on Significant Aspects of the HIPAA Privacy Rule:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/privacyguidance.html>
- **Fast Facts about the HIPAA Privacy Rule:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/cefastfacts.html>
- **The HHS Office of Civil Rights, HIPAA FAQs:** <http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>
- **Guidance materials for Small Providers, Small Health Plans, and other Small Businesses:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/smallbusiness.html>
- **OCR's Sample Business Associate Contract Provisions:**
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>



Other Federal Law Resources



- **42 CFR Pt. 2:** <http://www.samhsa.gov/healthPrivacy/>
- **Title X Confidentiality:** 42 C.F.R. § 59.11: <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ce18bb9053f3b026e8983fd8ac27170c&rgn=div8&view=text&node=42:1.0.1.4.43.1.19.11&idno=42>
- **GINA deferring to HIPAA:** 29 C.F.R. §§ 1635.9(c) and 1635.11(d):
<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&node=29:4.1.4.1.21.0.26.9&idno=29> and <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ecbc0d928c8f11dbab0c20532d0101c9&rgn=div8&view=text&node=29:4.1.4.1.21.0.26.11&idno=29>
 - **GINA:** http://www.ornl.gov/sci/techresources/Human_Genome/publicat/GINAMay2008.pdf
- **HIPAA deferring to FERPA;** exceptions to “protected health information” under (2)(i) and (2)(ii) in 45 C.F.R. § 160.103: <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=35aa826589279b8cff00d53c641a609f&rgn=div8&view=text&node=45:1.0.1.3.74.1.27.3&idno=45>
 - **FERPA/HIPAA Guidance:** <http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf>

State Privacy Law Resources



- For state privacy laws, see the **National Conference of State Legislators (NCSL)**: <http://www.ncsl.org/?tabid=17173>
- For **state privacy law information**:
<http://ihcrp.georgetown.edu/privacy/records.html>
- **National Governor's Association (NAG) Report** on state laws and HIE:
<http://www.nga.org/Files/pdf/1103HIECONSENTLAWSREPORT.PDF>
- **Health Information Security and Privacy Collaboration (HISPC)** reports on state laws:
http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_hispc/1240
- **OCR's Sample Business Associate Contract Provisions**:
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>

Security Questions You Should Ask Your Vendor

Holly Schlenvogt, MSH, CPM

HIT Specialist and Privacy & Security Lead

WHITEC

August 19, 2011

Objectives

- Provide general considerations when selecting a system
- Provide key security-related questions to ask vendors
- Resources



General Considerations

- Is it client-server or hosted/ASP (web-based)?
- What software and hardware is needed?
- Do you help set up the hardware and wireless routers?
- What is the warranty for the software, servers, other hardware, etc.?
- How often are updates done?
- How often is the system down on average?
- What happens if the vendor sells to another company?



System Access

- Role (or user) based access
 - Does the system allow the organization to create & assign different access roles (to meet minimum necessary requirements)?
 - Does the vendor assign them?
- User modifications & terminations
 - Does the organization or the vendor do this?



System Access, continued

- Can access to certain types of records be locked so certain roles are not able to access them (i.e. sensitive records such as mental health, AODA, etc.)?
- Remote access
 - What methods of remote access to the EHR are recommended or set up for the users?
 - How is remote access secure?

Username: Login

Password: ●●●●

Submit

Authentication

- What type of authentication is used? User ID & Password, or other two-factor?
 - Does the system work with finger print or id badge sign-on applications?
 - Does the system work with single sign-on applications?
- Passwords
 - Strength: at least 8 characters, alpha numeric, and require a character?
 - Frequency to change? Is this forced by the application or something the organization can change?
 - Users may not utilize previous 6 passwords?
 - Users forced to change password after first log-in?
 - What are the default settings?
 - Can settings be changed by users and/or the organization, or only by the vendor?



Auto Log Off

- Can the system be set to automatically save and then log-off users after 10 minutes of inactivity?
- Does the vendor do this or the organization?

Encryption & Integrity



- Where is ePHI stored?
- Is data at rest & in transit encrypted?
 - What type of encryption is used?
- Is there a firewall?
- What anti-virus protection is used?
 - When & how is it updated & monitored?
- Any other integrity controls used?



Audit Trails

- User access
 - What details are included on the audit trail?
 - Is it easy to manipulate the data?
 - How long are audit reports maintained?
- Log-in monitoring
 - Are there system event logs
 - Who monitors them?
 - Can alerts be sent?
 - Does the system lock accounts after 3 unsuccessful access attempts?

Data Storage & Backups

- Source data:
 - Where is the source data stored?
- Backup data:
 - Where is it stored?
 - How is it backed up?
 - When is it backed up?
 - How often are backups tested?
- How long is data stored?





Contingency Plan

- Is there an emergency mode operation plan?
 - Will the vendor work with you to create one?
 - How is ePHI accessed during an emergency?
 - Are there redundant power supplies?
 - How often is the plan tested?
 - Where is the plan located?
- How is lost data restored?

Facility Security

- How is access restricted to those who do not need access?
- Is there a fire prevention system in place?



Vendor Access

- How many support staff are authorized to use this account?
- Do you have active Privacy & Security policies & procedures?
- Do you have a Privacy Officer & Security Officer?
- Do you have an active training program?
- Reminder: Obtain a HIPAA-compliant Business Associate Agreement (BAA)



General Security

- Are all of the security features “on” or is this controlled by the organization?
- Are there any interdependencies that will impact the confidentiality, integrity, and/or availability of ePHI?
- Have all the security features been tested for reliability? What did the tests show about performing the function correctly, accurately, and with integrity?
- What other types of security and system support do you provide?
- Will any of this security cost more or does it come with it? Including support?

Resources

- HIPAA Collaborative of Wisconsin
<http://hipaacow.org>
- American Health Information Management Association (AHIMA) <http://www.ahima.org/resources/>
- HCPRO HIPAA Update Blog
<http://blogs.hcpro.com/hipaa/>
- Healthcare Information and Management Systems Society www.himss.org
- National Institute of Standards & Technology – EHR Testing Requirements:
http://healthcare.nist.gov/use_testing/effective_requirements.html



Contact Information

- Holly Schlenvogt, MSH, CPM
HIT Specialist and Privacy & Security Lead
WHITEC
 - hschlenv@whitec.org
 - 608-729-2707

Thank you!

Office of Health Information Technology and Quality

Additional HRSA Health IT and Quality Toolboxes and Resources including past webinars can be found at:

<http://www.hrsa.gov/healthit>

<http://www.hrsa.gov/quality>

Additional questions can sent to the following e-mail address:

HealthIT@hrsa.gov

- US Department of Health and Human Services
- Health Resources and Services Administration