Roanoke Valley Media Public Safety Co-Op

Minutes 05/08/03

Members Present:

Shelly Alley	Roanoke Police
Jennifer Faulkner	Roanoke Fire-EMS
P.J. Patrone	Roanoke County Police
Amanda DeHaven	Roanoke Regional Airport Commission
Rich Martin	Roanoke Times
Mike Crockett	City of Roanoke 911
Scott Smith	Roanoke County Police
Huck Ewers	Roanoke County Police
Gary D. Huffman	Roanoke County Fire and Rescue
Jeff Sturgeon	Roanoke Times
Lindsey Nair	Roanoke Times
Dwayne Yancey	Roanoke Times
Tad Dickens	Roanoke Times
Shawna Morrison	Roanoke Times
Jenny Kincaid	Roanoke Times
Bonnie Naumann	Roanoke Times
Mike Stater	Virginia Department of Health
Sgt. Bob Ross	VSP
Jennifer Conley Sexton	Roanoke Co Fire and Rescue
Melissa Preas	WSLS-10
Scott Meadows	Roanoke City Schools
Joe McKean	WDBJ-7

I. Shelly Alley welcomed everyone to the meeting and asked everyone to introduce him or herself.

II. Shelly introduced Eric Earnhart with Carilion who in turn introduced the guest speakers, Judie Snipes, Corporate Privacy Officer and Tom Newtown, Information Security Officer. They gave an in-depth presentation (see end of the minutes) on HIPAA and what it means to all of us.

Some additional discussion included –

- HIPAA does not change how law enforcement officers do their job.
- Hospital will continue to release one word conditions through Eric or his designee if the reporter has the patient's name.
- Fire-EMS/ Rescue are healthcare providers.

- When law enforcement is seeking information about a no news patient, hospital staff can clarify with the patient. (Often times the patient indicates no news to keep a particular family member of ex-family member from learning about their condition.)
- Eric mentioned that the state of Washington, hospital and press agencies published a guide to address such issues. See www.wsha.org.
- Law enforcement agencies will report back about what they learn from their city attorney's about how HIPAA is being addressed.

III. Additional Discussions

- Discussions were held about some of the recent major incidents that have occurred (Madison Avenue shooting, missing person cases, etc.)

- Everyone agreed that the paging system seems to be working well. AEP has become a new user of the system.

- Mike Stater recently joined the Virginia Department of Health as their new Public Information Officer for this region.

IV. Next Meeting

Tentatively scheduled for July 17th, WVTF-FM had expressed interest in hosting us at their new studio. Shelly will follow-up and let everyone know.

HIPAA Training Overview

What Is HIPAA?

Among the multiple priorities and constraints facing the healthcare industry is a new wave of change brought on by the Health Insurance Portability and Accountability Act (HIPAA). President Clinton signed HIPAA into law in August 1996. The intent of the legislation is to:

- Improve the portability of health benefits.
- Ensure greater accountability in the area of healthcare fraud.
- Simplify the administration of health insurance.

Title II of the Act, in a subsection entitled Administrative Simplification, mandates compliance with a wide range of health information management, security and privacy standards such as:

1. Improve efficiency by standardizing information interchange, and
2. Protecting health information through setting and enforcing standards.

More specifically, HIPAA calls for:

1. Standardization of electronic transactions and code set data
2. Unique health identifiers for individuals, employers, health plans and healthcare providers
3. Privacy standards protecting the use and disclosure of confidentiality and integrity of "individually identifiable health information," past, present and future.
4. Security standards to address how information is to be protected.

The bottom line: sweeping changes for healthcare transaction and administrative information systems.

Who Is Affected?

Most healthcare organizations. This includes healthcare providers, health plans, clearinghouses (organizations that process claims), billing agencies, information systems vendors and other vendors/agencies contracted to work on behalf of a healthcare organization.

Penalties

Any member of Carilion's workforce who uses or disclosures protected health information, without proper authorization may be subject to criminal penalties of up to:

- $ 25,000 and one (1) year in prison for knowingly disclosing information.
- $ 100,000 and five (5) years in prison if done under false pretense.
- $ 250,000 and ten (10) years in prison for intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm.

Compliance Deadlines

- Privacy – April 14, 2003
- Transaction and Code Sets Rule – October 16, 2003
- Security – tentative October 2004
- National Identifiers – varies with publication date

What Is the Effect?

Broad and deep - compliance will not be the same for each organization because organizations are not standard. Therefore what is right for one organization may not be right for another organization. An organization must look at what is reasonable and right for them and their patients when addressing HIPAA requirements.

A variety of issues were considered when analyzing the impact of HIPAA at Carilion including:

- ✓ Improving the efficiency and cost-effectiveness of our healthcare system.
- ✓ Using resources effectively, both in terms of dollars, staffing, and time -- which are necessary to implement these regulations.
- ✓ Analyzing electronic health strategies and HIPAA objectives, which are clearly connected in the areas of standardization and technical security measures.
- ✓ Upgrading legacy systems, which adds to cost of compliance as well as ongoing dependency on vendors

HIPAA will have a profound impact on Carilion's electronic communications and transactions. Implementation of the information security and privacy features in HIPAA will pave the way for electronic health and other healthcare commerce — as well as for new uses of evolving technologies, such as hand-held devices and wireless access. To realize these potential benefits — and to ensure that official compliance deadlines are met — we assessed our current information environment and developed strategies to meet these challenges.

Glossary of Terms

Access and Confidentiality Agreement – An agreement, signed by each Carilion employee and vendor personnel working at a Carilion facility, stating that they will comply with the laws and Carilion policies relating to confidential information.

Authorization – A customized document that gives Carilion permission to use specified protected health information for specified purposes, which are generally other than treatment, payment and healthcare operations, or to disclose protected health information to a third party specified by the individual

Business Associate Agreement – A business associate is a person or entity who performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

Consent – A general document that gives Carilion, which has a direct treatment relationship with the patient, permission to use and disclose protected health information for treatment, payment and healthcare operations.

Covered Entity – A Provider, Payer or Clearinghouse that is covered by the HIPAA regulation.

HIPAA – Health Insurance Portability and Accountability Act of 1996.

Minimum Necessary – When using or disclosing protected health information or when requesting protected health information from another covered entity, Carilion must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

NPP – Notice of Privacy Practices. A notice of privacy practices within Carilion that must be made available to each patient each time they register at or are admitted to a facility for treatment or healthcare services as an inpatient or outpatient.

PHI – Protected Health Information.

TPO – Treatment, Payment and Healthcare Operation.

Administrative Simplification within HIPAA

The Administrative Simplification section is to standardize specific electronic transactions and identifiers used in healthcare business processes such as billing, claims, and other interactions between providers, clearinghouses and health plans. By making business practices more uniform, costs due to duplication of effort, modifications of procedures, errors and delays should be substantially reduced. The framers of HIPAA anticipated that these improvements would encourage the use of electronic data interchange (EDI) in healthcare, and result in the eventual replacement of paper-based transactions. They also recognized that healtcare's growing reliance on EDI calls for the use of strong protections to ensure patient privacy and the security, integrity, and authenticity of health information. Central to this concern was the concept of protecting "patient identifiable health information" — any information, including demographic information, that refers to an individual's past, present or future health, and identifies an individual, or that could be useful in identifying an individual.

The Administrative Simplification section of HIPAA mandates the following:

I. ELECTRONIC HEALTH TRANSACTIONS STANDARDS

Today, health providers and plans use many different formats. Implementing a national standard means everyone will use one format, thereby "simplifying" and improving transaction efficiency nationwide. The rule requires specific formats developed by American National Standards Institute (ANSI).

The following transactions will require the use of HIPAA defined standards: *(Healthcare organizations not conducting business via electronic transactions nor having someone to transmit electronically for them are exempt from use of these standards)*

1.	Health claims or equivalent encounter information	837
2.	Enrollment and disenrollment	834
3.	Eligibility for a health plan	270 and 271
4.	Payment and remittance advice	835
5.	Health plan premium payments	820
6.	Health claims status	276 and 277
7.	Referral certification and authentication	278

Virtually all health plans will have to adopt these standards. Providers using non-electronic transactions are not required to adopt the standards; although if they don't, they may be required, by a health plan, to contract with a clearinghouse to provide translation services.

Health organizations also must adopt standard Code Sets to be used in health transactions. For example, coding systems that describe diseases, injuries, and other health problems, as well as their causes, symptoms and actions taken must become uniform. Parties to any transaction will have to use and accept the same coding. Again, this is intended to reduce mistakes, duplication of effort and costs. Fortunately, the code sets proposed as HIPAA standards are already used by many health plans and providers, which should ease the transition.

II. UNIQUE IDENTIFIERS FOR PROVIDERS, EMPLOYERS, HEALTH PLANS and PATIENTS

HIPAA requires the adoption of standards that would provide for unique, national identifiers for providers, employers, health plans and individuals to be used within the healthcare system.

The current system allows multiple ID numbers when dealing with each other, which is seen as confusing, conducive to error and costly. It is expected that standard identifiers will reduce these problems.

The first identifier regulation was issued May 31, 2002 for Employer Number.

III. SECURITY OF HEALTH INFORMATION

Security refers to the means by which organizations and people ensure the privacy and confidentiality of healthcare information. Security addresses "how" information is to be protected from inappropriate use. It applies to individually identifiable health information that is maintained or transmitted electronically, oral or written, by healthcare entities.

The security proposal is presented in four categories:

1. Administrative procedures – Formal practices to manage the selection and execution of security measures to protect information, and to manage the conduct of personnel in relation to the protection of information.

2. Physical safety guidelines – Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.

3. Technical security services – Processes that protect information and to control individual access to information.

4. Technical security mechanisms – Processes that guard against unauthorized access to information that is transmitted over a communications network.

The Security regulation is focused on outcomes rather than specific technologies or methodologies. The regulation expects organizations to assess their individual security risks, and implement programs appropriate for their organization to meet the security requirements.

IV. PRIVACY AND CONFIDENTIALITY

The purpose of the Privacy Rule is to protect the rights of individuals with respect to use and disclosure of their individually identifiable health information. The Privacy Rule will, at a minimum:

- Limit the non-consensual use and release of private health information.
- Give patients rights to access their medical records and to know who else has accessed them.
- Restrict disclosure of health information to the minimum needed for the intended purpose.
- Establish policies and procedures on use and disclosure of protected health information.
- Establish new criminal and civil sanctions for improper use or disclosure.
- Establish new requirements for access to records by researchers and others.

The new regulation reflects five basic principles:

- Consumer Control: Consumers have new rights to control the release of their medical information.
- Boundaries: With few exceptions, an individual's healthcare information should be used for health purposes only, including treatment and payment.
- Accountability: There will be specific federal penalties if a patient's right to privacy is violated.
- Public Responsibility: The standards reflect the need to balance privacy protections with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting healthcare fraud and abuse.
- Security: Organizations that are entrusted with health information must protect it against deliberate or inadvertent misuse or disclosure.

Relationship to State Laws

HIPAA preempts state law except:

- ✓ where the state law is necessary to prevent fraud and abuse,
- ✓ to ensure state insurance or health plan regulation,
- ✓ to address controlled substances or for certain other purposes, and
- ✓ when state law is more stringent than HIPAA requirements.

VIRGINIA CODE – Patient Health Records Privacy

It recognizes a patient's right of privacy in the content of a patient's medical record. Patient records are the property of the provider maintaining them, and, except when permitted by this section or by another provision of the State or Federal Law, no provider, or other person working in a healthcare setting may disclose the records of a patient.

Policies and Procedures

The *Corporate Information Security and Privacy Policy* outlines our organization's philosophy regarding the protection, use and disclosure of all information, regardless of the media in which it is published.

The *Confidentiality of Protected Health Information Policy*, details how patient records are to be handled.

Reference Information

For a complete set of the HIPAA regulations: http://aspe.hhs.gov/admnsimp

Informational site: www.hipaadvisory.com

Corporate Privacy Officer	Judie Snipes	540-224-5801
Information Security Officer	Tom Newton	540-224-4246

1. The resources and time necessary to read and understand the regulations (some facilities must use consultants)

   - Original regulation was 143 pages with 1368 pages of explanation (preamble) issued in December 2000.
   - August 14, 2002 465 pages of changes.
   - December 3, 2002 - 121 Guidance information from DHHS.
   - 309 pages in comparing HIPAA to Va law.

2. The adjustments needed for being complaint with Transaction and Code Sets. Many offices and hospitals use Clearinghouses and will continue to do so and must depend on them to be ready to transmit in the proper format. The result of not being compliant may negatively impact revenue. But even Medicare struggled to get there in time and thus extensions were allowed and encouraged.

3. Writing or enhancing policies and procedures and doing gap analyses to make sure you have met the intent of the regulation.

4. Educating the "workforce" which included doctors, staff, volunteers, Ministers / Chaplains and students (for CHS this was 11,000 people) and we needed to track attendance and make it mandatory for all. We soon learned that training on HIPAA is one thing. Applying it to real situations is where the problems come in.

5. Evaluating all of your electronic systems, doing a gap analysis to determine how they actively track access.

6. Working with vendors to make sure that any systems not currently compliant can be made complaint in a reasonable amount of time. (Note a lot of vendors MUST adapt or hospitals and doctors will need other software or mechanisms to track access) THIS IS WHERE THERE WILL BE NEED FOR A SIGNIFICANT AMOUNT OF INVESTMENT IN TECHNOLOGY AND FOR SOME HOSPITALS THIS MAY MEAN A BURDEN THEY MIGHT NOT BE ABLE TO AFFORD!

7. Someone in each organization must serve as Privacy Officer and Security Officer. Can be in addition to other duties, a separate function or combined into one role. Depends on the size of the organization or facility.

8. The Privacy Officer and Security Officer will have an initial HUGE responsibility of answering hundreds of questions from patients, staff, MDs etc, because everyone wants to do the right thing and the regs are so lengthy that most do not understand. We have seen a number of consultants make money recommending things that are NOT necessary or appropriate and may in fact harm patients by delaying care or treatment. We expect that this will settle down after the first year. Currently we are getting about 10-20 emails and calls a day just to answer simple questions because everyone is more aware.

9. Each covered entity (and especially providers) must give out a Notice of Privacy Practices (NPP). These cost money to print and distribute and create lots of questions from the public. There are several things you are required to say and getting it right is harder than most expected. Our notice is three (3) pages and a local Ophthalmologist's is seven (7). We must also make an effort to get the patient to sign that they received the NPP. This has to be tracked in our systems. There will be expense, time and effort to get them in different languages.

10. We are obligated to track all access NOT related to Treatment, Payment and Operations. There will be few but having patients know that they can ask will generate requests. When patients ask we must do an evaluation in all cases. (read that as time and money when most have shown nothing but we owe it to patients to check). They can ask for 6 years back, but not BEFORE April 14, 2003. We think each request may take 2-3 hours based on our testing of the process. This will get easier as vendors get more compliant systems for us. Question is will our vendors be compliant or will providers and others be required to replace software at their expense?

11. Business Associate Agreement that must be entered into with all business, vendors and servicers that we provide patient information to in order for them to do a service for us. This process is time consuming and in some cases requires legal assistance.

12. Now for the kicker. These and all other changes required for HIPAA will be at the cost of the organization's cost. This is yet another example of a federally unfunded mandate for healthcare! We will save money and be more efficient because of Transaction and Code Sets component, but we will spend more to track access and change computers or modify computer systems to meet the other privacy and security pieces of these regulations. For some providers, this will be millions of dollars. We at Carilion are trying to take a reasonable and common sense approach to keep costs down.

13. There is hope! With all regulations there are periods just after the implementation where facilities and others impacted will ask a lot of questions and the Feds will evaluate the full impact of the regulations (like unfounded requests). Once this information is collected, expect to see more guidelines and help with the regulations coming down to providers and others.

The item number 12... this is the smoking gun we hear about across the country... where do facilities that are currently struggling to meet budget get the money to pay for all of this labor and systems costs?