



Letter from the President

Dear Members:

For those that missed it, I wish you had been able to attend the annual Conference in Myrtle Beach! We had a wonderful time. The Columbia Chapter tied the Lexington Chapter for second place for the most attendees at the meeting with 22 attendees. Spartanburg came in first with 29 attendees. We had wonderful speakers and the location was wonderful! The beach bash was a lot of fun. There are hopes that it will be there again next year. Mark your calendars.

As we approach the last quarter of the year there are many things coming up! There will be a planning retreat in November and a joint Christmas party with the Lexington Chapter in December.

We hope that all of the programs have brought you good information! If you have any suggestions of topics for next year, please do not hesitate to let any one on the board know of them. If you would like to help on the board please let us know. We would be glad to have your help.

The new committee of Insurance and Legislative Issues for the State Board level has been a wonderful new committee and I believe will be very beneficial to all of our practices. If you have any questions about the Cigna or BCBS lawsuits please ask our representative, Karen McGrady.

We look forward to seeing you at the next meetings!

Harriet Oster, President

The Medical Manager

Newsletter of the Columbia Chapter
South Carolina Healthcare Managers Association
3rd Quarter 2004

UPCOMING EVENTS:

October 19, 2004 – Monthly Meeting

Location: Providence Education Building

Topic: Innovations in Practice Efficiency

Speaker: Ann Humphries

October 22-23-2004 – Columbia Board Planning Retreat (2004 and 2005 board members to attend)

Location: To be announced

November 16, 2004 – Monthly Meeting

Location: Two Medical Park

Topic: "Your Internet Presence: The good, the bad and the ugly"

Speaker: Glenn Oster

December 2, 2004 – Annual Holiday Celebration- joint venture with the Lexington Chapter

Location: To be announced

The 2004 conference in Myrtle Beach was a huge success!!

Many thanks to those that sponsored and attended. If you were unable to attend, please consider attending next year. The speakers were excellent, the topics timely and useful, and who can forget the Beach Bash? Watch your newsletter for upcoming information on Conference 2005!!

\$



Welcome new members!!



Margaret "Meg" Pearce – Palmetto
Neurosurgery and Spine

Julie Dunn – Resource One, LLC

Todd Lewis – Companion Employment Services

J. Reed Folline – Ellison Kibler & Assoc. of
Merrill Lynch



Congratulations to the Manager of the Year
and the Member of the Year!!

At our July Medical Managers
Celebration, Carra Jackson-Holton of
Professional Pathology Services was
honored by her peers by being voted
Manger of the Year. Likewise, Jessica
Turner of ImageCare, LLC, was honored by
being voted Member of the Year. Both of
these ladies have worked hard to make our
organization a success. Congratulations!



**It's almost that time again!! In the
next few weeks, you will be receiving
your dues notice for the 2005 year.**

**Please complete a new application
and return it with your dues payment.
Anyone who joined the organization
prior to September 2004 will need to
renew their membership for the 2005
year.**

\$

**Please send dues and application to
PO Box 7122 Columbia, SC 29202**

**Overtime rules change affects RNs,
PAs, athletic trainers, certified
medical technologists and dental
hygienists**

Many salaried medical professionals working in
medical group practices that required an
advanced degree to fulfill their position
requirements are exempt from overtime pay
under a revised labor regulation. Effective Aug.
23, the regulations modify the categories of
salaried professionals who are ineligible for
overtime compensation. For medical
professionals to qualify under the regulations,
they must meet the following requirements of
the learned professional employee exemption:

- The employee must be salaried at a rate of \$455 or more per week;
- The employee's primary duty must be the performance of work requiring advanced knowledge, defined as work that is predominantly intellectual in character and that includes work requiring the consistent exercise of discretion and judgment;
- The advanced knowledge must be in a field of science or learning; and
- The advanced knowledge must be customarily acquired by a prolonged course of specialized intellectual instruction.

The new exemption will affect the following salaried medical professionals:

- Registered nurses (RNs) licensed with the state;
- Physician assistants (PAs) certified by the National Commission on Certification of Physician Assistants who successfully completed four years of academic study by an accredited program;
- Athletic trainers certified by the Board of Certification of the National Athletic Trainers Association who successfully completed four years of academic study by an accredited program;
- Certified medical technologists who successfully completed three years of academic study by an accredited program; and

- Dental hygienists who successfully completed four years of academic study by an accredited program.

Licensed practical nurses, lab technicians and other similar salaried health care professionals generally do not qualify. These employees rarely require an advanced academic degree for entry into their occupations and therefore do not fall under the learned professional employee exemption.

For additional information on the Fair Pay Overtime Initiative, please log on to:

<http://www.dol.gov/esa/regs/compliance/whd/fairpay/main.htm>

Reprinted with permission from the Medical Group Management Association, 104 Inverness Terrace East, Englewood, CO 80112-5306; 303.799.1111. www.mgma.com. Copyright 2004.

HIPAA Security rule analysis

Compliance

Date Medical practices will have 26 months — until **April 21, 2005** — to comply. It is important to note, however, that several of the Security provisions will require implementation as part of the Privacy rule. In the Privacy regulation, the government calls on covered entities, including all medical groups, to implement "appropriate administrative, technical and physical safeguards" for protected health information (PHI) in all forms, nonelectronic and electronic. These "security" provisions of the Privacy rule go into effect as of April 14, 2003.

Overview of the Final Security Rule

The Department of Health and Human Services (HHS) states in the Security rule, "we have focused more on what needs to be done and less on how it should be accomplished." The Security rule offers a high-level description of principles which each covered entity must evaluate and apply, based on the entity's specific situation. Different from the Privacy rule, which covers health information in written, oral, and electronic form, the new Security rules' scope is narrowed to (PHI) in electronic form only.

In general, practices are required to:

- (1) Ensure the confidentiality, integrity, and availability of all electronic PHI which the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of PHI.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.

- (4) Ensure compliance by its workforce.

This rule allows for a flexible approach to be adopted: "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." The government is thus allowing practices to factor in cost, size, complexity, technical infrastructure, other capabilities, and the possibility and seriousness ("criticality") of potential security risks.

One area of vast improvement from the proposed rule is the final Security rules' explicit recognition that the cost of implementation is a factor in security decision-making. Small and rural providers in particular should benefit from this recognition. Despite this recognition, the government cautions that cost considerations do not justify ineffective security. The rule states "[T]here is a clear requirement that adequate security measures be implemented . . . Cost is not meant to free covered entities from this responsibility."

According to the rule, a covered entity can take into account the following factors in deciding which security measures to use:

1. The size, complexity, and capabilities of the covered entity.
2. The covered entity's technical infrastructure, hardware, and software security capabilities.
3. The costs of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

The rule also clarifies some common concerns regarding the types of communications that are covered:

- Paper-to-paper faxes are not considered electronic and thus are not covered under the rule. However, computer-generated faxes are electronic and are thus covered. Should you print out a paper copy of a computer-generated fax, that information is covered.
- Voice telephone communications are not considered electronic PHI under the rule.
- There is no distinction in the rule between PHI that moves internally within a practice or PHI that is sent outside the practice.

- Computer workstation protection is now much more flexible in concept. As an example, computer workstations are not required to utilize an automatic log-off system.
- The use of electronic file encryption is an acceptable method of denying access to information in that file. Encryption provides confidentiality, thus qualifying as a form of access control. The use of encryption, for the purpose of access control of data at rest, should be based upon each entity's risk analysis. Therefore, encryption has been adopted as an **addressable** (see next section) implementation specification in the final rule.

Required and Addressable Implementation Requirements

The Security rule has both "standards" and "implementation specifications." Implementation specifications can be either "required" ("R") or "addressable" ("A"). HHS has included an appendix to the rule--a "Security Standards Matrix" that lists each standard and its associated implementation specifications. The Matrix (see attached) indicates with an "R" or "A" whether the particular implementation specification is required or addressable, and lists the section of the Security rule where the standard and implementation specification is found.

In simple terms, a standard explains what must be done, and implementation specifications explain how to do it. HHS labels an implementation specification "addressable" if it is one of several options, none of which by itself is essential. Essential implementation specifications are labeled "required".

Physical Security Measures The Security rule sets out a number of physical security requirements a practice will need to consider:

Standards

1. **Facility access controls** - Practices must implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
2. **Workstation security** - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
3. **Workstation use** - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of

4. workstation that can access electronic protected health information.
5. **Device and media controls** - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Required Implementation Specifications

1. **Disposal** - Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
2. **Media re-use** - Implement procedures for removal of electronic protected health information

Addressable Implementation Specifications

1. **Contingency operations** - Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
2. **Facility security plan** - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
3. **Access control and validation procedures** - Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
4. **Maintenance records** - Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
5. **Accountability** - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
6. **Data backup and storage** - Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Technical safeguards

A practice must consider the following technical safeguards:

Standards

1. **Access control** - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
2. **Audit controls** - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
3. **Integrity** - Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
4. **Person or entity authentication** - Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
5. **Transmission security** - Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Required Implementation Specifications

1. **Unique user identification** - Assign a unique name and/or number for identifying and tracking user identity.
2. **Emergency access procedure** - Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Addressable Implementation Specifications

1. **Automatic logoff** - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
2. **Encryption and decryption** - Implement a mechanism to encrypt and decrypt electronic protected health information.
3. **Mechanism to authenticate electronic protected health information** - Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

4. **Integrity controls** - Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
5. **Encryption** - Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Security Management Measures

The rule requires medical practices and their business associates to manage their security processes. Practices must have the ability to detect an intrusion (such as a computer hacker attack) and respond quickly and effectively with countermeasures. HHS uses the term "incident response" to describe this process. Another aspect of security management is personnel training. The rule states that security training must be given to a practice's entire workforce, not just that part of the workforce that comes in contact with PHI. Keep in mind that volunteer workers, students, and temporary workers also are considered your employees, and must be trained. As with all aspects of the security management process, training must keep up with changes in threats and countermeasures.

Risk Assessment and Risk Management

The Security rule explains that: "The administrative, physical, and technical safeguards a covered entity employs must be reasonable and appropriate to accomplish the tasks outlined in paragraphs (1) through (4) of § 164.306(a)." The way a group practice knows what measures are reasonable and appropriate to complete each of the listed tasks is through a two-step process outlined in the new rules.

A practice must first assess the security risks it faces, then implement countermeasures proportional to those risks. The effectiveness of ensuring the confidentiality, integrity, and availability of PHI, and in protecting PHI against

"any reasonably anticipated threat or hazard" will be the measure of success. The rule discusses risk assessment and risk management but does not

prescribe any particular technology solution to achieve compliance.

Business Associate Contracts

HHS has abandoned the proposed rule's requirement for a comprehensive and complex security "chain-of-trust agreement".

Rather, they have substituted a requirement for practices to have agreements with all business associates who create, receive, maintain or transmit electronic protected health information on the practice's behalf. These contracts must contain assurances from the business associate that it will appropriately safeguard the information. This security component should be an extension of the Business Associate Contracts, which practices are obligated to develop as part of the Privacy rule.

The contract between a group practice and a business associate must provide that the business associate will:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the practice
2. Ensure that any agent, including any business associate subcontractors to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it
3. Report to the covered entity any security incident of which it becomes aware
4. Authorize termination of the contract by the covered entity, if the practice determines that the business associate has violated a material term of the contract

Documentation Requirements

Practices must institute the following documentation policies and procedures:

1. Maintain a record of the policies and procedures implemented to comply with this rule in written (which may be electronic) form
2. If an action, activity or assessment is required by this rule to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment
3. Retain the documentation required by this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later
4. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains
5. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information

Intersection Between the Security and Privacy Rules

Despite the fact that the mandated compliance date for the final Security rule is April 21, 2005, practices are required to comply with several of the Security provisions in order to meet the requirements of the Privacy regulation. The deadline for Privacy compliance is April 14, 2003. Practices have an additional year to modify existing business associate contracts.

The physical security requirements contained in the Security rule include several issues that intersect directly with the Privacy regulation. For example, the Security rule discusses the issue of disposing of computer hard drives with patient information on them. Should patient information be disclosed from someone accessing a discarded or reused computer floppy disk or hard drive, it could potentially be a violation of the Privacy rule. In addition, the Privacy rule expressly states that a practice must protect against intentional or accidental disclosure of protected health information. This includes physical security measures such as locked cabinets and doors, protecting computers against access from unauthorized individuals, and the development of a employee termination policy that would include ensuring receipt of keys and the changing of passwords.

Conclusion

The HIPAA Security rule, while allowing for considerable implementation flexibility, continues to mandate a comprehensive set of administrative and technical obligations. The rule provides high-level guidance on what practices are required to do in order to maintain the security of their patient's information, but wisely leaves it up to the practice itself to decide the specific measures are most appropriate. It will be a significant challenge for practices to undertake the required "risk analysis" and "risk mitigation" outlined in the regulation. MGMA educational and implementation resources will continue to provide assistance to practice administrators as they meet this HIPAA challenge and comply with this new federal mandate.

Reprinted with permission from the Medical Group Management Association, 104 Inverness Terrace East, Englewood, CO 80112-5306; 303.799.1111. www.mgma.com. Copyright 2004.