Physicians Insurance
A Mutual Company

HIPAA – Revised to Implement the HITECH Act

HIPAA
The Health Insurance Portability and Accountability Act of 1996, or HIPAA, as it has become widely known, was enacted by the federal government to help workers maintain their health insurance coverage during a time of job change, to establish privacy and security rules for protected health information, to set standards for electronic billing of health care services, and to develop a national provider identifier system.

The HIPAA Privacy Rule established standards to protect individuals' personal health information and requires appropriate safeguards to protect the privacy of personal health information, sets limits and conditions on the uses and disclosures of personal health information without patient authorization, and gives patients certain rights over their personal health information. The Privacy Rule compliance date was April 14, 2003.

The HIPAA Security Rule established standards to protect individuals' electronic personal health information that is created, received, used, or maintained by covered entities. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality and security of electronic protected health information. The Security Rule compliance date was April 21, 2005.

The HIPAA Enforcement Rule contains provisions related to ascertaining compliance with and enforcement of the Privacy, Security, and Breach Notification Rules, and sets forth the civil money penalties that may be imposed for violations of the Rules. The Enforcement Rule also establishes procedures for hearings related to enforcement actions. The Final Enforcement Rule was effective on March 16, 2006.

The HITECH Act and the Breach Notification Rule
On February 17, 2009, the American Recovery and Reinvestment Act (ARRA) was signed into law. The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of ARRA to promote the adoption and meaningful use of health information technology, to strengthen the civil and criminal enforcement of the HIPAA rules, and to add breach notification requirements to HIPAA. The breach notification requirements, known as the Breach Notification Rule, established standards for providing notification of breaches of unsecured protected health information. The Breach Notification Rule was implemented through interim final regulations that were effective on September 23, 2009.

Final Regulations
On January 25, 2013, the U.S. Department of Health and Human Services (HHS) issued final regulations to modify the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules for the purpose of implementing the requirements of the HITECH Act. The final regulations also modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing the Genetic Information Nondiscrimination Act of 2008 ("GINA"). Collectively, the regulations are referred to as the Final Rule and were effective on March 26, 2013; however, in general, covered entities and business associates have until September 23, 2013, to comply.

This Final Rule will require you to review and revise your current practices relating to the use and disclosure of protected health information. To this end, this article is intended to provide you with a summary of the

regulatory changes contained in the Final Rule and a checklist of items that you should use to achieve compliance with the Final Rule by the September 23, 2013, compliance date.

Physicians Insurance has updated our HIPAA-related sample policies and procedures, forms, and training materials to address these new federal requirements. In addition, we have identified a number of helpful resources to assist you in meeting these new regulations. This information is available to all policyholders and their staff on our Web site at www.phyins.com.

Final Rule Changes to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules:

Breach Notification Rule. Covered Entities will need to revise policies and procedures to incorporate the revised definition of a breach of PHI, the replacement of the "significant risk of harm standard" with the use of an objective risk assessment to demonstrate a low probability that PHI has been compromised, and changes to the regulatory exceptions to what constitutes a breach.

1. What Is A Breach? The Final Breach Notification Rule revises the definition of a breach and also revises when notice of a breach must be given. Specifically, an acquisition, access, use, or disclosure of protected health information ("PHI") in a manner not permitted under the Privacy Rule is presumed to compromise the security or privacy of the PHI and is therefore a "breach" unless the Covered Entity ("CE") or Business Associate ("BA"), as applicable, demonstrates that there is a low probability that the PHI has been compromised. As a result, breach notification is necessary in all situations except those in which the CE or BA demonstrates that there is a low probability that the PHI has been compromised using an objective risk assessment, based upon at least the following four factors, unless one of the regulatory exclusions in paragraph 2 below applies:

a) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification,
b) the unauthorized person who used the PHI or to whom the disclosure was made,
c) whether the PHI was actually acquired or viewed, and
d) the extent to which the risk to the PHI has been mitigated.

In addition, based upon the circumstances of the impermissible use or disclosure, additional factors may need to be considered to appropriately assess the risk that PHI has been compromised. The risk assessment should be documented and retained by the CE or BA as applicable.

2. What Is Not A Breach? The Final Rule adopted previously published exclusions from the definition of "breach"; consequently the following actions are not considered breaches of PHI and are not subject to the breach notification requirements:

a) any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or BA made in good faith and within the person's scope of authority and which does not result in further use or disclosure in a manner not permitted under the Privacy Rule;

b) any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement (OHCA) in which the CE participates, and the PHI received is not further used or disclosed in manner not permitted under the Privacy Rule; and

c) a disclosure of PHI where the CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

The CE or BA has the burden to demonstrate, using documentation, why an impermissible use or disclosure fits within one of these three exceptions.

3. Exception to Breach Eliminated. The Final Rule does not retain the previously existing exception for use or disclosure of a limited data set that does not include any dates of birth and zip codes. An improper acquisition, access, use, or disclosure of any limited data set is presumed to be a breach, whether or not the limited data set includes dates of birth and zip codes, and the CE or BA, as applicable, should conduct the 4 factor risk assessment to determine whether breach notification is required.

4. Notification. CEs continue to be responsible to notify (i) individuals, (ii) if applicable, the media, and (iii) HHS following discovery of a breach of unsecured PHI. The Final Rule incorporates a change to the requirements for notice to HHS. For breaches affecting less than 500 individuals, CEs are required to maintain a log or other documentation of the breaches, and submit the log annually to HHS within 60 days after the end of the calendar year for breaches that were *discovered* during the immediately preceding calendar year. Prior to the Final Rule, the log was to be submitted within 60 days after the end of the calendar year for breaches that *occurred* during the immediately preceding calendar year.

5. HHS Clarifications. Several clarifications to the breach notification requirements should be incorporated into the CEs' processes.

a) CEs retain the ultimate responsibility to accomplish the notifications required under the Final Rule, even when the breach of the CE's unsecured PHI occurs at or by a BA, or at or by a CE that is acting as a BA, such as when a CE contracts with another CE to perform the functions of a BA, for example, billing services. The obligation to disclose rests with the CE whose PHI is compromised. BAs in turn are responsible to report breaches to CEs.

b) Notices to individuals that are returned as undeliverable do not fulfill the notice requirements—they are deemed *not* to have been given. Either direct written notice using updated contact information or substitute notice, consistent with the regulatory requirements, must be given within the original 60-day time limit.

c) CEs are not obligated to bear the cost of media print or broadcasts regarding a breach, and media outlets are not obligated to print or broadcast information received from CEs concerning a breach. To fulfill the breach notification requirements, CEs must deliver notice, such as a press release, directly to the prominent media outlets being notified. Posting a general press release on the CE's Web site is not sufficient.

Privacy, Security, and Enforcement Rules.

1. Business Associates. The Final Rule expands the types of organizations included in the definition of a Business Associate and makes all BAs directly liable for violations of applicable provisions of the Privacy, Security, and Breach Notification Rules. Therefore, CEs need to formalize Business Associate Agreements with all BAs, and include the requirement that BAs formalize Business Associate Agreements with their

subcontractors that include the same restrictions and conditions that apply to the BA. CEs are not required to enter into Business Associate Agreements with subcontractors; the BA is required to meet this requirement and has direct liability for failing to do so.

a) Definition. First, the Final Rule revises the definition of Business Associate to include a person or entity who, other than a member of the CE's workforce, creates, receives, maintains, or transmits PHI on behalf of the CE. The addition of "maintains" means that an entity that maintains PHI on behalf of a CE is a BA even if the entity does not actually view the PHI or does so only on a random or infrequent basis. For example, a storage service provider is a business associate, even if that service provider does not access the PHI, or accesses PHI only on random or incidental basis.

b) Specific Organizations. The Final Rule also adds the following to the definition of Business Associate:

    (1) Health Information Organizations,
    (2) E-prescribing Gateways and similar organizations that provide data transmission services with respect to PHI to a CE and that require routine access to PHI,
    (3) Patient Safety Organizations that analyze data that includes PHI on behalf of a CE,
    (4) Vendors of personal health records that provide services on behalf of a CE, and
    (5) Subcontractors, defined as persons to whom a BA delegates a function, activity, or service that the BA has agreed to perform for a CE or BA, other than in the capacity as a member of the delegating BA's workforce. Subcontractors are BA's where that function, activity, or service involves the creation, receipt, maintenance, or transmission of PHI. Subcontractors include any agent or other person who acts on behalf of the BA, even if the BA has failed to enter into a Business Associate Agreement with the person.

All of these persons and entities are required to comply with the applicable Privacy, Security, and Breach Notification Rule provisions to the extent they create, receive, maintain, or transmit PHI on behalf of a CE; or with respect to subcontractors, on behalf of a BA.

c) Conduits. Entities that provide data transmission services but are mere "conduits" are not BAs. A conduit, whether of paper or electronic PHI, transports information, and may also store the information temporarily incident to the transportation, but does not access it other than on a random or infrequent basis as necessary to perform the transportation services or as required by law.

d) Direct Liability. BAs are now directly responsible to the Secretary of HHS for compliance with, and are directly subject to enforcement actions related to, applicable provisions of the Privacy, Security, Enforcement, and Breach Notification Rules. BAs are subject to the same civil and criminal penalties that CEs are exposed to, and when they are found noncompliant, HHS may impose civil monetary penalties directly on the BA, and the Department of Justice may enforce criminal penalties directly on the BA. Specifically, BAs are directly responsible to perform the following activities, and will be directly liable for failure to do so:

    (1) Maintain records and submit compliance reports to HHS when required by HHS to determine compliance with HIPAA, cooperate with complaint investigations and compliance reviews, and permit access by HHS to the BA's facilities, books, and records.

(2) Comply with the Security Rule, and implement administrative, physical, and technical safeguards for electronic PHI in accordance with the Security Rule. BAs will also be required to implement written policies and procedures for compliance with these requirements.

(3) Notify CEs of a breach of unsecured PHI.

(4) Use or disclose PHI only as permitted in the Business Associate Agreement or as required by law.

(5) Disclose PHI to HHS when required by HHS to investigate or determine compliance with HIPAA.

(6) Provide access to a copy of electronic PHI to either a CE, the individual, or the individual's designee when necessary to comply with an individual's request for an electronic copy of his or her PHI.

(7) Make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Until HHS provides additional guidance on the minimum necessary standard, this means BAs must limit the use, disclosure or request for PHI, to the extent practicable, to a limited data set, or if needed, to the minimum necessary to accomplish the intended purpose.

(8) Enter into Business Associate Agreements with subcontractors that are going to create, receive, maintain, or transmit PHI on the BA's behalf. The Business Associate Agreement must meet the applicable HIPAA requirements.

(9) BAs are responsible to provide an accounting of disclosures in accordance with the provisions of their Business Associate Agreements.

2. Business Associate Agreements. The Final Rule adds some new requirements to the content of Business Associate Agreements, and Business Associate Agreements entered into on and after March 26, 2013, must comply with the new requirements. If the Business Associate Agreement you were using before publication of the Final Rule on January 25, 2013, was HIPAA-compliant under the previous rules, and is not modified or renewed after March 26, 2013, then you have until September 23, 2014, to either amend the existing Agreement or terminate the existing Agreement and enter into a new Agreement, to achieve compliance with the Final Rule. An automatic renewal of a previously existing Business Associate Agreement is eligible for the extension of the compliance date, so long as the Agreement was HIPAA-compliant before January 25, 2013.

3. Minimum Necessary. The Final Rule adopts the application of the minimum necessary standard directly to BAs, but does not adopt regulations that further define "minimum necessary." Therefore, under the HITECH Act, CEs and BAs must limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. In the case of disclosure, the CE or BA disclosing the PHI is responsible to determine what constitutes the minimum necessary. HHS intends to issue future guidance on the minimum necessary standard.

4. Individual Access to PHI. The Final Rule strengthens the right of individuals to obtain electronic access to PHI.

a) One Readable Electronic Form Must Be Provided. CEs that maintain PHI electronically in Designated Record Sets must provide individuals with access to the electronic information in the electronic form and format requested, if it is readily producible, or if not readily producible then in a readable electronic form and format that is mutually agreeable to the CE and the individual. Previously, if the electronic form and format was not readily producible, then CEs were required to provide a hard copy. Now, CEs must offer at least one electronic form, even if doing so requires the CE to invest in additional technology to meet the basic requirement of providing some kind of readable electronic copy. If the individual declines the electronic format that is readily producible by the CE, the CE must provide a hard copy.

b) Content. The electronic copy must include all PHI electronically maintained at the time the request is fulfilled unless the individual requests only a portion of the PHI.

c) Transmission. CEs are not required to use external portable media furnished by the requesting individual if the CE has security concerns about doing so. The CE may send the electronic copy via unencrypted e-mail if the individual has requested it, provided the CE has advised the individual of the risk that the e-mail may not be secure, and the individual continues to request the unencrypted e-mail. The CE is not responsible for unauthorized access of PHI while in transmission based on the individual's request.

d) Third Parties. If requested by an individual, a CE must transmit the copy of PHI directly to another person designated by the individual. CEs must obtain written direction from the individual clearly designating the third party recipient and where to send the copy of PHI, and the written direction must be signed by the individual. CEs may rely on the information given by the requesting individual when providing PHI to a third party, but the CE is responsible to implement reasonable policies and procedures to verify the identity of any person who requests PHI and to implement reasonable safeguards to protect the information that is used or disclosed.

e) Timeliness. The Final Rule shortens the time within which CEs must provide individuals with access to PHI. CEs must now provide access within thirty (30) days, but may take an additional one-time extension of thirty (30) days when necessary, so long as the CE notifies the individual of the reasons for the delay. The CE's response time is further reduced by Washington law, which requires a response within 15 working days, or in the case of delay, not later than 21 working days.

f) Fees. CEs may continue to charge a reasonable cost-based fee when providing the required access to PHI, but the fee may include only labor costs for copying PHI, not any cost of retrieval, plus costs of supplies for paper copies or electronic media requested by the individual, such as flash drives and compact discs, plus postage costs where the individual requests that the CE provide the copy through the mail or by courier. Maintenance and capital costs may not be included in the fees charged. The fees permitted by the Final Rule are subject to the limits imposed by Washington law. Effective July 1, 2013, through June 30, 2015, WAC 246-08-400 limits copying charges to $1.09 per page for the first 30 pages plus $0.82 per page for all other pages, plus a $24 clerical fee for searching and handling records.

5. Right to Restrict Disclosures. Under the prior HIPAA rules, individuals may request special privacy protections for the use and disclosure of PHI for treatment, payment, and health care operations; however, CEs are not required to grant those requests, although the individual's request is retained in the record.

The Final Rule requires a CE to honor an individual's request to restrict disclosure of PHI to a health plan for payment or health care operations if the PHI relates solely to health care items or services for which the individual or another person has paid in full out of pocket, unless the disclosure is otherwise required by law.

6. Accounting of Disclosures. The Final Rule does not adopt final regulations related to the HITECH Act requirements for accounting of disclosures. Therefore, CEs should continue to comply with the previously existing regulations, and include in Business Associate Agreements, the requirements for BAs to maintain the needed documentation and respond to a CE's request for an accounting in a manner that permits CEs to meet the requirements of 45 CFR § 164.528, as it may be amended.

7. Fund-raising Communications. The Final Rule expands the types of information that CEs may use or disclose in fund-raising communications and the opt-out methods that CEs may provide to individuals. CEs will need to revise policies and forms to incorporate these revisions.

a) Scope of PHI. In making fund-raising communications, CEs may use, or disclose to institutionally related foundations or BAs, the following PHI in connection with fund-raising activities: demographic information of an individual (name, address, other contact information, date of birth, age, and gender), health insurance status, dates of health care services, department of service, treating physician, and—for the purpose of screening out individuals who had suboptimal outcomes—outcome information.

b) Form and Scope of Opt-Out. Notices of Privacy Practices must inform individuals that the CE may contact them to raise funds and that the individual has a right to opt out of receiving future fund-raising communications. Each fund-raising communication must also inform the individual that he or she has the same right to opt out. If the communication is oral, such as by telephone, the oral communication must clearly inform the individual of the ability to opt out. CEs must provide individuals with one or more simple, quick, and easy methods of opting out of future fund-raising communications. Examples of acceptable methods are preprinted, prepaid postcards, toll-free telephone numbers, and e-mail addresses; requiring an individual to write a letter is not acceptable. Note that CEs are free to decide the scope of the opt-out, which may provide individuals the choice to opt out of all future fund-raising communications or just campaign specific communications.

c) Prohibition on Contact. Once an individual opts out, CEs are prohibited from contacting the individual for fund-raising purposes. The previous rule required only that CEs make reasonable efforts not to send fund-raising communications to individuals who have opted out. CEs may, however, provide a method for the individual to opt back in.

d) Treatment Not Conditioned. CEs may not condition treatment on the individual's choice to receive or opt out of receiving fund-raising communications.

8. Marketing Communications. The Final Rule changes the definition of "marketing" to include any treatment or health care operations communication made to individuals about health-related products or

services that encourages recipients of the communication to purchase or use the product or service. If the CE or its BA receives direct or indirect payment from or on behalf of the third party whose product or service is being described, then CEs must obtain written authorization from the individual for the use or disclosure of PHI in a marketing communication, and the authorization must disclose that payment is involved and must clearly state that the individual may revoke the authorization at any time. In-kind benefits do not constitute payment. CEs may use or disclose PHI, without a valid authorization, in communications made for treatment or health care operations where the CE does not receive direct or indirect payment. In addition, face-to-face communications from CEs to individuals and promotional gifts of nominal value provided from CEs to individuals are permitted. CEs may also, without authorization, use or disclose PHI to make communications related to currently prescribed drugs, such as refill reminders, provided that any direct or indirect payment from the third party whose product is the subject of the communication is reasonably related to the CE's cost of making the communication.

9. Sale of PHI Prohibited. The Final Rule prohibits the sale of PHI unless a valid authorization is obtained, and valid authorizations must state that the disclosure will result in remuneration to the CE or BA. A sale occurs when the CE or BA discloses PHI in exchange for financial or in-kind (nonfinancial) remuneration, and a sale is not limited to a transfer of ownership of the PHI. The disclosure of PHI could be pursuant to a lease, license, or other access. A sale does not include a disclosure of PHI:

a) for certain public health activities;

b) for research, where the only remuneration received by the CE or BA is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI;

c) for treatment and payment;

d) for the sale, transfer, merger, or consolidation of all or part of the CE and related due diligence;

e) to or by a BA for activities that the BA performs on behalf of the CE, if the only remuneration is provided by the CE to the BA for its performance;

f) for providing an individual with access to his or her PHI, where the fees charged are consistent with the Privacy Rule;

g) for disclosures required by law; and

h) for any other purpose permitted by the Privacy Rule, where the only remuneration received by the CE or BA is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for that purpose or a fee otherwise expressly permitted by law.

10. Research Authorizations May Be Streamlined. The Final Rule streamlines the authorization process for use and disclosure of PHI in research. CEs may revise their authorization forms to incorporate the new rules.

a) Compound Authorizations. The Final Rule permits CEs to begin using single, compound authorizations that combine an authorization for the use or disclosure of PHI for a research study that conditions trial-related treatment on the authorization with an unconditioned authorization for the same or another research study, provided that the authorization clearly differentiates

between the two activities and clearly allows the individual to opt in to the unconditioned research activity. The single authorization must make clear that the individual has the choice not to opt in to the unconditioned activity and that the choice will not impact treatment, payment, or benefits.

b) Future Research May Be Included. Research authorizations no longer need to be study-specific; instead, authorizations may include an authorization to use or disclose PHI in future research studies that are unrelated to the present study, so long as the authorization adequately describes possible future research such that the individual has a reasonable expectation that his or her PHI could be used or disclosed for such future research.

c) Separate Authorizations for Psychotherapy Notes. Note that separate authorizations continue to be required for use or disclosure of psychotherapy notes in research, and an authorization related to psychotherapy notes may only be combined with another authorization for use or disclosure of psychotherapy notes.

11. PHI About Decedents. Individually identifiable health information of a person who has been deceased for more than 50 years is no longer considered PHI and is thus not protected under HIPAA. With respect to other deceased individuals, CEs may now disclose to family members, relatives, close personal friends, or others identified by the individual, any of whom were involved in the individual's care or payment for care prior to the individual's death, PHI about the individual that is relevant to the person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the CE. Consequently, CEs should refer to documentation of patients' expressed preferences before releasing PHI about decedents.

12. Disclosure of Student Immunization Records Permitted. The Final Rule permits CEs to send immunization records about a student or prospective student directly to a school without a written authorization provided that a) the PHI is limited to proof of immunization, b) the school is required by state or other law to have proof of immunization before admitting the student, and c) the CE obtains and documents agreement to the disclosure from either a parent or legal guardian. The parent or guardian's assent need not take the form of a valid HIPAA authorization—the Final Rule requires only that the CE obtain and document the assent. CEs should revise policies and procedures to implement a process for determining and documenting who the legal parent or guardian of the student is, and that person's assent to the disclosure. Washington law requires that all students attending licensed day care centers, and public and private schools from preschool through 12th grade, provide proof of immunization before or on the first day of attendance.

13. Notice of Privacy Practices.

a) Revise NPPs. CEs should revise their Notices of Privacy Practices ("NPPs") to add the following new requirements:

(1) a description of the types of uses and disclosures that require a written authorization, such as psychotherapy notes (if the CE records or maintains psychotherapy notes), marketing, and sale of PHI;

(2) a statement that all uses and disclosures not described in the NPP also require a written authorization;
(3) notice to the individual that the CE may contact the individual for fund-raising activities and that the individual has a right to opt out of receiving such communications;
(4) notice that the individual has the right to restrict disclosure of PHI by health care providers to a health plan where the PHI relates solely to health care items or services for which the individual has paid in full out of pocket; and
(5) a statement that the CE is required to notify the individual of a breach of unsecured PHI; no specific details of the CE's process are required to be included in the NPP.

Health plans, other than issuers of long term care policies, that use PHI for underwriting purposes must also include a statement that they are prohibited from using or disclosing PHI that is genetic information for these purposes.

b) Notify Individuals. HHS considers these changes to be material, which triggers a requirement for CEs to promptly revise and distribute the amended NPPs to individuals. Health care providers must make copies of their revised NPPs available to individuals to take with them upon request at their clinic locations and post them in a clear and prominent location. Providers are not required to hand out copies to all individuals seeking care, but must provide copies to and obtain acknowledgment of receipt from new patients.

Health plans that post their NPPs on Web sites must post their revised NPPs on their Web sites by September 23, 2013, and provide the revised NPP, or information about the changes and how to obtain the revised NPP, in their next annual mailings to the individuals then covered by the plan. Health plans that do not use Web sites must provide the revised NPP, or information about the changes and how to obtain the revised NPP, to covered individuals within 60 days after the revision to the NPP.

14. Genetic Information Nondiscrimination Act.

a) Genetic Information is Health Information. The Final Rule amended the definition of health information to include genetic information, which is information about (1) the individual's or a family member's genetic tests, (2) the manifestation of a disease or disorder in family members, and (3) the individual's or his or her family member's request for or receipt of genetic services, or participation in clinical research which includes genetic services.

b) Prohibition on Use. CEs that are health plans, other than issuers of long-term-care insurance, are now prohibited from using or disclosing genetic information for underwriting purposes. HHS notes that it is continuing to study the exclusion of long-term-care issuers from the prohibition, and will reassess their inclusion in the prohibition in the future. HHS emphasized that long-term-care plans continue to be bound by HIPAA to protect genetic information from improper uses and disclosures, and to use genetic information only as required or expressly permitted by the Privacy Rule.

15. Violations and Civil Money Penalties.

a) CEs and BAs are Liable for Violations. The Final Rule incorporates the HITECH Act requirements that both CEs and BAs are directly liable for civil money penalties if they violate applicable HIPAA requirements. In addition, CEs and BAs are liable for violations committed by their respective

agents, including workforce members, and newly added under the Final Rule, business associates or subcontractors respectively, acting within the scope of their agency authority. Whether or not an agency relationship exists between the CE and a BA, or between a BA and its subcontractor, will be determined in accordance with federal law, and will largely depend on the right or authority of the CE to control the BA's conduct, or on the BA's right or authority to control its subcontractor's conduct, in the course of performing services on behalf of the CE or BA.

b) Amount of Civil Penalties. Civil monetary penalty amounts are determined using a tiered structure, based upon the level of culpability of the violator.

   (1) $100 to $50,000 for each violation where the CE or BA as applicable did not know, and by exercising reasonable diligence would not have known, of the violation, capped at $1.5 million for violations of the same requirement or prohibition in one calendar year;

   (2) $1,000 to $50,000 for each violation due to reasonable cause and not to willful neglect, capped at $1.5 million for violations of the same requirement or prohibition in one calendar year;

   (3) $10,000 to $50,000 for each violation due to willful neglect that was corrected during the 30-day period beginning on the first date the CE or BA liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred, capped at $1.5 million for violations of the same requirement or prohibition in one calendar year; and

   (4) $50,000 for each violation due to willful neglect that was not corrected during the 30-day period beginning on the first date the CE or BA liable for the penalty knew or, by exercising reasonable diligence, would have known that the violation occurred, capped at $1.5 million for violations of the same requirement or prohibition in one calendar year.

c) Aggravating and Mitigating Factors. HHS is required to determine the amount of the penalty on a case-by-case basis depending on the nature and extent of the violation, the nature and extent of the resulting harm, and certain additional mitigating and aggravating factors. These include (1) the number of individuals affected, (2) the time period during which the violation occurred, (3) whether the violation resulted in physical, financial, or reputational harm, (4) whether the violation affected the individual's ability to obtain health care, (5) the history of prior HIPAA compliance, including prior violations, attempts to correct previous indications of noncompliance, and response to prior complaints, (6) how the CE or BA has responded to technical assistance from HHS in the context of compliance effort, and (7) the financial condition and size of the CE or BA, including the presence of financial difficulties that affect its ability to comply and whether monetary penalties would jeopardize the ability of the CE or BA to continue to provide or pay for health care.

16. Criminal Penalties. CEs, BAs, and other individuals and entities may be held criminally liable for violations of HIPAA. The U.S. Department of Justice may seek the imposition of criminal penalties, including monetary penalties and imprisonment, if a person or entity knowingly uses or obtains and discloses PHI in violation of HIPAA. "Knowingly" means the person has knowledge of the facts that constitute the violation, but not necessarily that the act violates the law.

State Law and Preemption

Many states, including Washington, have adopted state privacy regulations governing the use and disclosure of personal health information. Except in limited specific instances, if the standards and requirements of HIPAA are contrary to a provision of state law, HIPAA preempts the state law provision. One such exception is that where state law is more stringent than HIPAA, state law takes priority over HIPAA and must be complied with. This means that if Washington law restricts or prohibits the use or disclosure of personal health information in circumstances under which HIPAA would permit the use or disclosure, the restrictions and prohibitions imposed by Washington law must be complied with.

Conclusion. HIPAA rules, regulations, and standards have and will continue to evolve under the direction of the federal government. It is important that your practice's compliance program, policies, and procedures are periodically reviewed and updated as necessary to reflect these changes. Initial training of new staff members and ongoing retraining of existing staff is required under the HIPAA regulations.

In addition to the resources available on our Web site at www.phyins.com, the Department of Health and Human Services Office for Civil Rights (OCR) is another valuable source of information for meeting the various HIPAA requirements. The OCR Web site is available at http://www.hhs.gov/ocr/privacy. You can find an extensive list of HIPAA-related questions and answers at http://www.hhs.gov/hipaafaq.

We're here to help you. Contact your Physicians Insurance risk management representative for more information about the new legislation affecting the HIPAA Privacy and Security Rules and Washington State privacy laws. Call us in Western Washington and Oregon at (206) 343-7300 or 1-800-962-1399, or call us in Eastern Washington and Idaho at (509) 456-5868 or 1-800-962-1398. E-mail our experts at risk@phyins.com.