

## **Fundamentals of Health Law**

# **Privacy, Confidentiality and Technology**

**Jennifer A. Stiller, Esquire**  
Law Offices of Jennifer A. Stiller  
Haverford

**Darice McNelis, Esquire**  
Buchanan Ingersoll, P.C.  
Pittsburgh

©2003 Pennsylvania Bar Institute  
Used with Permission

## **I. INTRODUCTION: PRIVACY, CONFIDENTIALITY, AND TECHNOLOGY**

- A.** The issue of medical privacy was brought sharply into focus in April, 2003, when new federal regulations governing privacy of individually identifiable health information went into effect. Suddenly, a visit to the family doctor meant that the patient was handed a multiple-page form explaining privacy rights and privacy practices. Ironically – for the regulations were designed to provide *more* protections for consumers – such a “Notice of Privacy Practices” was the first inkling that many citizens had as to the degree to which private health information is routinely available to third-party payors and government oversight agencies.
- B.** This paper addresses the principles of Pennsylvania law applicable to the privacy and confidentiality of medical information, and then discusses the regulations adopted pursuant to the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (“HIPAA”).

## **II. PRIVACY AND CONFIDENTIALITY OF MEDICAL INFORMATION UNDER PENNSYLVANIA LAW**

### **A. General Principles**

1. Physician-patient privilege
  - a. 42 Pa.C.S. § 5929 provides: “No physician shall be allowed, in any civil matter, to disclose any information which he acquired in attending the patient in a professional capacity, and which was necessary to enable him to act in that capacity, which shall tend to blacken the character of the patient, without consent of said patient, except in civil matters brought by such patient, for damages on account of personal injuries.”
  - b. Purpose of the privilege is to create a confidential atmosphere in which the patient will be encouraged to disclose all possible information bearing on illness so that the physician may render effective treatment. *In re June 1979 Allegheny County Investigating Grand Jury*, 490 Pa. 143, 149, 415 A.2d 73, 77 (1980).

- c. Accordingly, case law draws a distinction between information learned by physician through patient's communications and that acquired through examination and observation. *Id.*
2. Psychotherapist-patient privilege
    - a. 42 Pa.C.S. § 5944 provides: "No psychiatrist or person who has been licensed . . . to practice psychology shall be, without the written consent of his client, examined in any civil or criminal matter as to any information acquired in the course of his professional services in behalf of such client. The confidential relations and communications between a psychologist or psychiatrist and his client shall be on the same basis as those provided or prescribed by law between an attorney and client."
    - b. Psychotherapist-patient privilege has been held to be absolute. *Commonwealth v. Kennedy*, 413 Pa. Super. 95, 110, 604 A.2d 1036, 1044 (1992) (en banc), *appeal denied*, 531 Pa. 638, 611 A.2d 711 (1992).
    - c. Privilege applies to both testimony and records created in the course of the confidential relationship. *Commonwealth v. Eck*, 413 Pa. Super. 538,545, 605 A.2d 1248, 1252 (1990).
  3. Patient privacy interests not covered by a statutory privilege could, under circumstances where the disclosure in question would pose a serious threat to a patient's right not to have personal matters revealed, be protected under the United States Constitution or Art. I, § 1 of the Pennsylvania Constitution. *Allegheny County*, 490 Pa. at 151, 415 A.2d at 77-78. (However, the court in that case did not find that such circumstances existed where disclosure was to a Grand Jury pursuant to an investigatory subpoena.)
  4. Disclosure by physician in non-judicial circumstances
    - a. The Pennsylvania courts have recently recognized a cause of action for breach of physician-patient confidentiality in circumstances where judicial proceedings are not involved. *Haddad v. Gopal*, 2001 Pa. Super. 317, 787 A.2d 975, *appeal denied*, 572 Pa. 705, 813 A.2d 842 (2002).

- b. Physicians have a duty to obtain either express or implied consent prior to releasing confidential information to third parties. Failure to do so will result in civil liability. *Id.*, 787 A.2d at 981.
  - c. In limited circumstances, based on an objective review of the totality of the circumstances, a patient's conduct may result in implied consent to disclose confidential information. *Id.*
  - d. Such consent also serves as an affirmative defense to an action for breach of physician-patient confidentiality. *Id.*
5. Other disclosures of medical information
- a. *Haddad*, by its own terms, applies only to disclosures by physicians. Other disclosures would presumably be governed by earlier case law, where Pennsylvania courts recognized that improper disclosure of health information might constitute the tort of invasion of privacy.
  - b. The tort has four elements:
    - (1) Intentional intrusion . . .
    - (2) Upon the solitude or seclusion of another or his private affairs or concerns; and the intrusion is
    - (3) Substantial; and
    - (4) Highly offensive to a reasonable person.
      - (a) *Chicarella v. Passant*, 343 Pa. Super. 330, 339, 494 A.2d 1109, 1114 (1985).
  - c. In *Chicarella*, insurance company in auto accident case hired investigator to investigate plaintiff's work history, physical condition, and community standing. In the course of doing so, the investigator spoke with a hospital's credit manager and, in the process, secured credit records that described, in summary form, that plaintiff had received outpatient treatments for bronchitis, hematemesis, a shoulder injury, and a series of migraine headaches.

- (1) Plaintiff sued investigator, insurance company, and hospital, for invasion of privacy.
  - (2) Court dismissed the complaint, holding that “[t]he brief descriptions of appellant’s medical treatment cannot be deemed a substantial intrusion” and that “the information disclosed by the hospital records is not the sort which would ‘cause mental suffering, shame or humiliation to a person of ordinary sensibilities.’ [citing cases].” *Chicarella*, 343 Pa. Super. at 339, 494 A.2d at 1114.
- d. Unauthorized disclosure of the mental and physical health records of patients seeking counseling at a mental health, drug and alcohol treatment center, irrespective of their content, has been held to meet the “substantial” and “highly offensive” standard. *Katlin v. Tremoglie*, 43 Pa. D.&C. 4th 373, 394 (Philadelphia 1999).

**B. Special Statutory and Regulatory Provisions Applicable To Particular Kinds of Healthcare Treatment**

1. Hospital records
  - a. Department of Health regulations governing hospitals require the hospital to establish a Patient’s Bill of Rights which contains provisions to the effect that:
    - (1) A patient has the right to every consideration of his privacy concerning his own medical care program. Case discussion, consultation, examination, and treatment are considered confidential and should be conducted discreetly. 28 Pa. Code § 103.22(b)(3).
    - (2) A patient has the right to have all records pertaining to his medical care treated as confidential except as otherwise provided by law or third-party contractual arrangements. 28 Pa. Code § 103.22(b)(4).
    - (3) Note: 28 Pa. Code § 103.21 states: “Nothing in these sections is intended to serve as evidence of a standard of reasonable conduct for the purpose of

determining civil liability between providers and consumers of health services.”

- b. 28 Pa. Code § 115.27, entitled “Confidentiality of Medical Records,” provides: “All records shall be treated as confidential. Only authorized personnel shall have access to the records. The written authorization of the patient shall be presented and then maintained in the original record as authority for release of medical information outside the hospital.”
2. Long-term care nursing facility records
    - a. Information contained in residents’ clinical records shall be privileged and confidential. Written consent of the resident, or of a designated responsible agent acting on the resident’s behalf, is required for release of information. 28 Pa. Code § 211.5.
    - b. Written consent is not necessary for authorized representatives of the state and federal government during the conduct of their official duties. *Id.*
  3. Drug and alcohol facilities and programs
    - a. Pennsylvania Drug and Alcohol Abuse Control Act (71 P.S. § 1690.101 *et seq.*) establishes a county-based system which funds prevention, intervention, and treatment programs for drug and alcohol abuse.
    - b. The Act provides that patient records prepared or maintained by these programs and all information contained therein,” shall remain confidential, and may be disclosed only with the patient's consent and only (i) to medical personnel exclusively for purposes of diagnosis and treatment of the patient or (ii) to government or other officials exclusively for the purpose of obtaining benefits due the patient as a result of his drug or alcohol abuse or ... dependence.” 71 P.S. § 1690.108(b).
    - c. Exceptions:

- (1) In emergency, where patient's life is in jeopardy, records or information can be released without patient's consent solely for the purpose of her medical treatment.
    - (2) Disclosure pursuant to an order of court of common pleas, issued after court has weighed the need for the information sought to be disclosed against the possible harm of disclosure to the person to whom such information pertains, the physician-patient relationship, and to the treatment services. Court may condition disclosure of the information upon any appropriate safeguards.
  - d. The Act also provides similar protection to patient records and all information therein "prepared or obtained by a private practitioner, hospital, clinic, drug rehabilitation or drug treatment center." Such information may be released for treatment purposes under the emergency exception, but cannot be released by court order. 71 P.S. § 1690.108 (c).
  - e. Related federal protections for drug and alcohol treatment information: 42 U.S.C. § 290dd-2; 42 C.F.R. §§ 2.1 – 2.67.
4. Mental health records – see section C below.
  5. HIV and AIDS information – see section D below.
  6. HMOs
    - a. A managed care plan (gatekeeper model) and utilization review entity must "adopt and maintain procedures to ensure that all identifiable information regarding enrollee health, diagnosis and treatment is adequately protected and remains confidential in compliance with all applicable Federal and State laws and regulations and professional ethical standards." 40 P.S. § 991.2102(a).
    - b. If a managed care plan maintains medical records, it must ensure that enrollees have timely access to their medical records unless prohibited by Federal or State law or regulation. 40 P.S. § 991.2012(b).

7. Clinical laboratories: Reports of clinical laboratory results are to be made only to the person submitting the specimen or requesting the analysis, or his or her authorized agent, except for statutory reports to state and local officials. 28 Pa. Code § 5.47.

### C. Mental Health Records

1. The Mental Health Procedures Act, 50 P.S. §§ 7101 *et seq.* (“MHPA”), contains a very broad confidentiality provision, which has been strictly construed by the courts. *In re Roy*, 423 Pa. Super. 183, 620 A.2d 1172, 1173 (1993), *appeal denied*, 536 Pa. 644, 639 A.2d 30 (1994), and *Commonwealth v. Moyer*, 407 Pa. Super. 336, 595 A.2d 1177, 1179 (1991), *appeal denied*, 529 Pa. 656, 604 A.2d 248 (1992).
2. Section 111(a) of the MHPA, 50 P.S. § 7111(a) provides that “all documents concerning persons in treatment shall be kept confidential,” with five exceptions:
  - a. Patient has given written consent to disclosure.
  - b. Disclosure is to “those engaged in providing treatment for the person.” 50 P.S. § 7111(a)(1).
  - c. Disclosure to the county administrator, pursuant to 50 P.S. § 7110 (relating to applications for emergency examinations). 50 P.S. § 7111(a)(2).
  - d. Disclosure to a court in the course of “legal proceedings authorized by this act.” 50 P.S. § 7111(a)(3). This exception has been held to include only involuntary and voluntary mental health commitment proceedings, as those are the only legal proceedings authorized by the Act. *Hahnemann Univ. Hosp. v. Edgar*, 74 F.3d 456, 463 (E.D. Pa. 1996), citing *In re Roy*, 620 A.2d at 1173-74 and *Commonwealth v. Moyer*, 595 A.2d at 1179.
  - e. Pursuant to federal rules, statutes and regulations governing disclosure of patient information *where treatment is undertaken in a federal agency*. 50 P.S. § 7111(a)(4).
3. Section 111(b) of the MHPA specifies that Section 111 shall not restrict judges of the courts of common pleas, mental health review

officers and county mental health and mental retardation administrators from disclosing information to the Pennsylvania State Police, or the State Police from disclosing it to any person, pursuant to 18 Pa.C.S. § 6105(c)(4), which bars a person who has been involuntarily committed for inpatient care under the MHPA from owning or trafficking in firearms.

4. The confidentiality provisions of the MHPA apply to all involuntary treatment of mental illness (whether inpatient or outpatient) and also to voluntary treatment “that requires full or part-time residence in a facility.” 50 P.S. § 7103.
5. Section 111 of the MHPA does not create a conventional privilege protecting communications only if they satisfy certain elements. On the contrary, section 111 is much broader in scope, covering *any document* that “concern[s] persons in treatment.” Disclosure is prohibited unless one of the statutory exceptions applies. *Hahnemann Univ. Hosp. v. Edgar*, 74 F.3d at 463 (emphasis in original).
6. Duty to warn:
  - a. Notwithstanding the psychotherapist-patient privilege and the MHPA, a mental health professional has a duty to warn a third party:
    - (1) When a specific and immediate threat of serious bodily injury has been communicated to the professional; and
    - (2) Such threat is made against a specifically identified or readily identifiable victim.
    - (3) *Emerich v. Philadelphia Center for Human Development*, 554 Pa. 209, 226, 720 A.2 1032, 1040 (1998), *reargument denied*, 554 Pa. 209, 720 A.2d 1032 (1999).
  - b. Court interprets such duty to warn as being authorized by MHPA implementing regulation at 55 Pa. Code § 5100.32(a)(9). *Emerich*, 554 Pa. at 230-231, 720 A.2 at 1043.

**D. HIV/AIDS**

1. The Confidentiality of HIV-Related Information Act, 35 P.S. §§ 7601 – 7612, provides broad confidentiality for HIV-related information.
  - a. Statute was enacted to promote testing and counseling by establishing confidentiality requirements to protect individuals from inappropriate disclosure and subsequent misuse of HIV-related information. 35 P.S. § 7602(a).
  - b. “Confidential HIV-related information” is broadly defined to mean “Any information which is in the possession of a person who provides one or more health or social services or who obtains the information pursuant to a release of confidential HIV-related information and which concerns whether an individual has been the subject of an HIV-related test, or has HIV, HIV-related illness or AIDS; or any information which identifies or reasonably could identify an individual as having one or more of these conditions, including information pertaining to the individual's contacts. 35 P.S. § 7603.
  - c. No one who obtains confidential HIV-related information in the course of providing any health or social service, or pursuant to a written consent to disclosure by the person who is the subject of the disclosure, may disclose that information except to 12 designated persons. 35 P.S. § 7607(a). These persons are:
    - (1) The individual who is the subject of the information or his guardian.
    - (2) The physician who ordered the test, or her designee.
    - (3) A person specifically designated to receive such information in a written consent meeting the requirements of 35 P.S. § 7607(c).
    - (4) An agent, employee or medical staff member of a healthcare provider in the course of treatment.

- (5) A peer review organization, nationally recognized accreditation agency or Federal or State government agency with oversight responsibilities over healthcare providers.
  - (6) An individual healthcare provider who needs to know in order to provide emergency care, or healthcare providers consulted to determine the diagnosis or treatment of the individual.
  - (7) An insurer, for reimbursement purposes.
  - (8) Persons authorized to gather, transmit, or receive vital statistics under the Vital Statistics Law.
  - (9) The Pennsylvania Department of Health and local boards and departments of health.
  - (10) Persons designated in a court order issued pursuant to 35 P.S. § 7608.
  - (11) A funeral director.
  - (12) Specified county and State officials.
- d. Protected information may not be released to any other person or entity except with the subject's consent. The consent must be in writing and must include a number of specified elements, including an expiration date. No consent for disclosure is valid if it fails to conform to these requirements, is known to be materially false or to have been revoked, or has expired. 35 P.S. § 7607.
- e. No court may order access to confidential HIV-related information unless it finds that the person seeking the information or seeking to disclose the information has a compelling need to do so. 35 P.S. § 7608.
- f. Notwithstanding all these requirements, 35 P.S. § 7609 permits a physician to disclose confidential HIV-related information if all of the following four conditions are met:

- (1) The disclosure is made to a known contact of the subject;
  - (2) The physician reasonably believes disclosure is medically appropriate, and there is a significant risk of future infection to the contact;
  - (3) The physician has counseled the subject regarding the need to notify the contact, and the physician reasonably believes the subject will not inform the contact or abstain from sexual or needle-sharing behavior which poses a significant risk of infection to the contact; and
  - (4) The physician has informed the subject of her intent to make such disclosure.
  - (5) The physician must make such disclosure in person if possible, and must not reveal the subject's identity. The physician has not duty to identify, locate, or notify contacts.
- g. Any person aggrieved by a violation of the Confidentiality of HIV-Related Information Act has the right to a cause of action against the person who committed the violation. 35 P.S. § 7610.
2. In cases involving HIV infection via transfusions with infected blood, the courts:
- a. Have permitted the infected blood donor to be questioned, on the condition that the donor's identity not be disclosed. *Stenger v. Lehigh Valley Hospital Center*, 530 Pa. 426, 609 A.2d 796 (1992); *Marcella v. Brandywine Hospital*, 47 F.3d 618 (M.D. Pa. 1995).
  - b. Have permitted plaintiffs to obtain in discovery the blood tests performed on other recipients of the infected donor's blood, without revealing such recipients' identities. *Stenger*, 530 Pa. at 799, 609 A.2d at 432.
  - c. Have ruled, in *dicta*, that such disclosures met the requirements of the Confidentiality of HIV-Related

Information Act. *Stenger*, 530 Pa. at 803, 609 A.2d at 439 (note 10).

3. The Pennsylvania Supreme Court considered the “compelling need” standard of 35 P.S. § 7608 in *Application of Milton S. Hershey Medical Center*, 535 Pa. 9, 634 A.2d 159 (1993).
  - a. Dr. Doe, an obstetrics resident, discovered he was HIV-positive and took a leave of absence. The two hospitals in which he had practiced petitioned common pleas court for an order permitting notification of patients during whose treatment Dr. Doe might conceivably have sustained cuts that would have allowed his blood to come into contact with that of the patient.
  - b. Common pleas court entered order authorizing the following (and only the following) disclosures:
    - (1) Provision of Dr. Doe’s name to physicians in the Obstetrics and Gynecology Departments at the two hospitals, including physicians in the residency program;
    - (2) Provision of Dr. Doe’s name to a physician authorized in writing by a patient for whom Dr. Doe participated in a surgical procedure or obstetrical care; and
    - (3) Describing Dr. Doe in letters to patients and media releases as “a physician in our joint Obstetrics and Gynecology residency program” and setting forth the relevant period of such service.
  - c. The court also ordered that “each physician to whom the name of Dr. Doe is provided” under its order “shall be reminded that the Act prohibits further disclosure of such information.”
  - d. The Supreme Court held that the trial court had not abused its discretion in concluding that the hospitals had met the burden of showing a compelling need for disclosure, as it had conducted the balancing analysis required under the statute, considered all the relevant factors, “and reached a

decision that reasonably balance the interests of Dr. Doe, the public, and the hospitals.”

- e. In so doing, the Court relied upon:
- (1) The fact that all of the medical experts who testified agreed that, in light of the risks presented, it was reasonable to give some form of notice to the patients;
  - (2) The possibility that disclosure would help limit the spread of HIV, and thereby save lives;
  - (3) The fact that the trial court’s order was narrowly drawn to protect the privacy interests of Dr. Doe; and
  - (4) Disclosure was clearly consistent with the primary purpose of the HIV Act – “to reduce the spread of HIV and AIDS.”

**E. Obligations of Health Insurers**

1. State Insurance Department in October 2002 adopted regulations relating to privacy of insurance health information, based on a determination by the Insurance Commissioner that “improper disclosure or marketing, or both, of nonpublic personal health information by members of the insurance industry constitutes an unfair method of competition and unfair or deceptive act or practice” under the Unfair Insurance Practices Act (40 P.S. §§ 1171.1 – 1171.14). 32 Pa.B. 5268 (Oct. 26, 2002); regulations codified at 31 Pa. Code § 146b-1 *et seq.*
2. Regulations cover all licensees of the Insurance Department except bail bondsmen, motor vehicle physical damage inspectors, and governmental insurance programs.
  - a. However, licensees that enroll participants through governmental insurance programs (Medicare, Medicaid, CHIP), or insure or otherwise provide insurance services through such a program *are* subject to the regulations.
  - b. Licensees include:

- (1) Any individual, corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyds insurer and any other legal entity engaged in the business of insurance, including agents and brokers;
  - (2) Blue Cross and Blue Shield plans;
  - (3) HMOs;
  - (4) Preferred provider organizations;
  - (5) Beneficial and fraternal beneficial societies; and
  - (6) Any other entity required to be licensed, authorized, or registered under the Insurance Department Act of 1921 (40 P.S. §§ 1 – 321) or the Insurance Company Law of 1921 (40 P.S. §§ 361 – 991.2361).
3. Licensees may not disclose nonpublic personal health information about a consumer to a third party unless an authorization is obtained from that individual.
- a. However, to the extent that disclosure is necessary for the performance of one or more specified insurance functions by or on behalf of the licensee, the nondisclosure rule does not apply. (There are 33 specified insurance functions.)
  - b. To be valid, an authorization must:
    - (1) Be written or in electronic form.
    - (2) Contain all of the following:
      - (a) The identity of the affected consumer,
      - (b) A general description of the types of nonpublic personal health information to be disclosed,
      - (c) General descriptions of the parties to whom the licensee discloses the information, the

purpose of the disclosure, and how the information will be used,

- (d) The signature of the affected consumer or an individual who is legally empowered to grant authority on his/her behalf, and
  - (e) The date signed.
- (3) Specify the length of time that the authorization remains valid, not to exceed 24 months.
- c. “Nonpublic personal health information” is defined as information that identifies, or for which there is a reasonable basis to believe identifies, the individual who is the subject of the information, and which:
- (1) Is created or derived from a healthcare provider or the consumer; and
  - (2) Relates to one or more of the following:
    - (a) The past, present, or future physical, mental or behavioral health or condition of an individual;
    - (b) The provision of health care to an individual; or
    - (c) Payment for the provision of health care to an individual.
4. A licensee may not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of nonpublic health information.
5. Violations of regulations are subject to penalties and remedies under the Unfair Insurance Practices Act. Once such a violation has been proven in an administrative hearing, penalties and remedies may include:
- a. Issuance of cease-and-desist order by Insurance Commissioner, enforceable by injunction.

- b. Suspension or revocation of license.
  - c. Civil monetary penalties (up to \$50,000 in a six-month period), awarded by a court in an action filed by the Commissioner.
6. Relationship of Insurance Department regulations to federal HIPAA privacy regulations:
- a. Insurance Department regulations have broader scope of coverage than HIPAA regulations. For example, they apply (as HIPAA does not) to:
    - (1) Workers' compensation insurance
    - (2) Life insurance
    - (3) Casualty insurance
    - (4) Annuities
    - (5) Mortgage insurance
  - b. A licensee that complies with the HIPAA privacy regulations (discussed in Part IV below), *whether or not such licensee is in fact subject to those federal regulations*, is not subject to these Insurance Department regulations. 31 Pa. Code § 146b.21(a).
  - c. Compliance dates are tied to those for the HIPAA privacy regulations.
    - (1) Compliance date for licensees with \$5 million or more in annual receipts is the same as for large health plans under HIPAA (i.e., April 14, 2003).
    - (2) Compliance date for licensees with less than \$5 million in annual receipts is the same as for small health plans under HIPAA (i.e., April 14, 2004).

**F. Employee Health Records**

- 1. Case law on access to employee health records has arisen in only two contexts: Governmental employers and efforts by a

governmental agency to obtain the records. In both kinds of cases, the U.S. Constitution is implicated, because individuals have a constitutional right not to have their private affairs made public by the government. *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570 (3d Cir. 1980), citing *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).

2. Access by government agency
  - a. Where OSHA sought employee medical records from an employer, the *Westinghouse* court held that:
    - (1) The constitutional privacy interest articulated in *Whalen v. Roe* applies to employees' medical records.
    - (2) The right of the individual to control access to her medical history is not absolute; courts and legislatures have determined that public health or other public concerns may support access to facts an individual might otherwise choose to withhold.
    - (3) Court must weigh competing interests of employee privacy and government need for disclosure, considering seven factors:
      - (a) Type of record requested;
      - (b) The information it does or might contain;
      - (c) Potential for harm in any subsequent nonconsensual disclosure;
      - (d) Injury from disclosure to the relationship in which the record was generated;
      - (e) Adequacy of safeguards to prevent unauthorized disclosure;
      - (f) Degree of need for access; and
      - (g) Whether there is an express statutory mandate, articulated public policy, or other

recognizable public interest militating  
toward access.

3. Access by supervisor, where the employer is a governmental entity: *Doe v. SEPTA*, 72 F.3d 1133 (3d Cir. 1995), *cert. denied* 519 U.S. 808 (1996).
  - a. Privacy right articulated in *Westinghouse* extends to records of prescription medications ordered by an employee under employer's health benefits plan. 72 F.3d at 1138.
  - b. Even though the information in question, which was shared among a handful of SEPTA employees involved in managing its health-benefits program, related to Doe's HIV-positive status, the court found no invasion of privacy where:
    - (1) Individuals to whom the information was disclosed had already learned of Doe's health status from Doe himself;
    - (2) No actual harm occurred from the disclosure, since plaintiff admittedly suffered no economic deprivation, nor any discrimination, nor any harassment; and
    - (3) Manager, who obtained the information inadvertently, had a legitimate need for requesting the information she had sought and handled the information she received in "a legitimate, careful and confidential manner."
  - c. Dissent expressed concern with the implications of the majority's position, predicting that this decision would "make it far easier in the future for employers to disclose their employees' private medical information, obtained during an audit of the company's health benefits plan, and to escape constitutional liability for harassment or other harms suffered by their employees as a result of that disclosure." 72 F.3d at 1147.

4. Access by plaintiffs in civil rights case against governmental entity: *Wilson v. Penna. State Police Dept.*, 1999 U.S. Dist. LEXIS 3165 (E.D. Pa. 1999).
  - a. In case brought under Americans with Disabilities Act, plaintiffs sought vision-testing results for certain State Troopers.
  - b. Using *Westinghouse* test, court granted discovery motion, where plaintiffs agreed to a confidentiality agreement and court ordered vision information to be extracted from the original medical records so that disclosure would be limited to this information only.
  
5. Access by press under Right to Know Act, 65 P.S. §§ 66.1 – 66.4: *Cypress Media, Inc. v. Hazleton Area School District*, 708 A.2d 866 (Pa. Cmwlth.1998).
  - a. Courts have interpreted personal security and personal reputation exceptions of Section 1(2) of the Act to create a privacy exception to the Act's general disclosure rule. *Tribune-Review Publishing Co. v. Allegheny County Housing Authority*, 662 A.2d 677 (Pa. Cmwlth. 1995), *appeal denied*, 546 Pa. 688, 686 A.2d 1315 (1996).
  - b. Disclosure of medical records in public school teachers' employment applications would infringe on the teachers' "substantial" privacy interests, with no countervailing public benefit to disclosure; physical examination reports may therefore not be released. *Cypress Media*, 708 A.2d at 870-71.

### **III. FEDERAL REGULATION OF PRIVACY AND SECURITY OF ELECTRONICALLY MAINTAINED OR TRANSMITTED HEALTH INFORMATION**

#### **A. Background**

1. The Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191, title II, subtitle F, 42 U.S.C. ch. 7, was designed to improve the efficiency and effectiveness of the healthcare system

by facilitating the electronic exchange of information with respect to certain financial and administrative transactions carried out by health plans, healthcare clearinghouses, and healthcare providers.

2. At the same time, Congress recognized the challenges to the confidentiality of health information presented by advances in health information technology and communications. Accordingly, Congress directed the Secretary of Health and Human Services (“HHS Secretary”) to adopt regulations to protect the privacy of individually identifiable health information. 42 U.S.C. § 1320d-2 note.

## **B. HIPAA Regulations**

1. This paper discusses the two principal sets of regulations issued under HIPAA that are broadly applicable to the protection of privacy of health information and the security of electronic media used to store and transmit such information.
2. The HIPAA privacy regulations, discussed in Part IV below, are currently effective (since April 14, 2003) as to most people and entities covered by them. They apply to all forms of “protected health information,” whether maintained electronically or otherwise. (For more on protected health information, see Part IV below).
3. The HIPAA security regulations were published as a final rule on February 20, 2003 and will not become applicable to affected Covered Entities until 2005 or 2006. The Security Rule applies only to electronic protected health information, not all protected health information, and is discussed in detail in Part V below.
4. A third set of HIPAA regulations, the Transactions and Code Set Standards, are highly technical rules applicable to billing for healthcare services, and are of little interest to anyone outside the industry. For that reason, they are not discussed here, but anyone who is interested can find them at 68 Fed. Reg. 8380 (Feb. 20, 2003).

## **IV. THE HIPAA PRIVACY REGULATIONS**

**A. The Basics:**

1. Regulations were adopted at 67 Fed. Reg. 53181 (Aug. 14, 2002) and are codified at 45 C.F.R. §§ 160.101 – 160.312 and 164.102 – 164.534. They are complex and often confusing. It should be noted that the summary description of the regulations in this outline is of necessity considerably less detailed than the regulations themselves.
2. Regulatory obligations are imposed only on *Covered Entities*.
  - a. The following are Covered Entities:
    - (1) Health plans -- Basically, any kind of health insurance. (Workers' compensation and casualty insurance are specifically excluded by statute.)
    - (2) Healthcare providers -- Broadly defined to include anyone who furnishes, bills, or is paid for health care in the normal course of business, as long as they engage in electronic transmission of data for certain specified purposes (e.g., billing).
    - (3) Healthcare clearinghouses -- Basically, entities that process data for health plans or healthcare providers.
  - b. Persons who are not Covered Entities may nonetheless find themselves affected by the HIPAA privacy requirements.
    - (1) For example, if an attorney requests protected health information from a Covered Entity but does not supply a patient authorization that, in the opinion of the Covered Entity, does not meet the HIPAA requirements, the Covered Entity may not honor that request.
    - (2) Covered Entities are required to impose confidentiality requirements on those to whom they disclose protected health information for certain legitimate purposes of the Covered Entity. This may include lawyers who represent them. (For more detailed discussion of HIPAA requirements of

special interest to lawyers, see sections E and F below.)

- (3) HIPAA statute imposes criminal penalties on any *person* (not limited to Covered Entities) who knowingly obtains or discloses individually identifiable health information. 42 U.S.C. § 1320d-6.
3. The regulations set forth detailed rules governing Covered Entities' internal use and external disclosure of *protected health information* (PHI), including complicated rules for when a patient authorization is or is not required for use and disclosure, and what that authorization must contain.
4. The regulations create new individual patient rights, including rights to:
  - a. Inspect and copy their own PHI;
  - b. Request amendments of erroneous or incomplete information;
  - c. Obtain an accounting of disclosures of their information;
  - d. Request a restriction of a use or disclosure for treatment, payment, or healthcare operations ("TPO");
  - e. Receive confidential communications;
  - f. Receive notice of the provider's privacy practices (*Notice of Privacy Practices*, or NPP); and
  - g. File written complaints.
5. New administrative requirements applicable to Covered Entities include:
  - a. Written policies and procedures to protect the privacy of health information;
  - b. Appointment of a privacy official to develop these policies;
  - c. Workforce training on privacy practices;

- d. Posting of NPP;
- e. Establishment of procedures for handling complaints and accounting for disclosures of PHI.
- f. Requirement for contracts with Business Associates who assist the provider with treatment, payment, or healthcare operations (TPO), to assure that they also protect the privacy of health information.

**B. Key Concept: Protected Health Information**

- 1. *Protected health information (PHI) is individually identifiable health information, written or oral, maintained or transmitted in any form or medium.*
- 2. Information that does not identify an individual, and with respect to which there is no reasonable basis to believe an individual can be identified, is not “individually identifiable health information” and therefore is not PHI.
- 3. Information can be “de-identified” by either of two methods:
  - a. Documented determination by a qualified statistician that the risk is very small that the intended recipient could identify the individual (taking into account reasonably available information from other sources).
  - b. Removal of 18 specific identifying characteristics combined with the disclosing entity’s not having actual knowledge that the information, when used alone or in combination with other information, could be used to identify and individual.
  - c. There are also standards for re-identifying de-identified information and for the use of limited data sets.

**C. Covered Entity’s Use and Disclosure of Protected Health Information Without Patient Authorization or Opportunity To Object**

- 1. Treatment, payment and operations

- a. A Covered Entity may use and disclose PHI for purposes of treatment, payment, and operations without patient permission.
  - b. The terms “treatment,” “payment,” and “operations” are defined quite broadly.
  - c. Specifically, such disclosures may include:
    - (1) A Covered Entity’s use and disclosure of PHI for its own treatment, payment, and operations.
    - (2) A Covered Entity’s sharing an individual’s PHI with other providers treating that person for the purpose of treatment.
    - (3) A Covered Entity’s sharing of PHI with other Covered Entities and healthcare providers for the receiving entity’s payment purposes.
    - (4) A Covered Entity’s disclosure of PHI to another Covered Entity for the second entity’s healthcare operations, if both entities have or had a relationship with the individual in question and the operations in question either:
      - (a) Involve quality assessment and improvement, provider credentialing, peer review, and like functions; or
      - (b) Are for the purpose of healthcare fraud and abuse detection or compliance.
2. Uses and disclosures required by law
- a. Use and disclosure must be required by law and limited to the relevant requirements of such law.
  - b. There are special rules for disclosures about victims of neglect, abuse, or domestic violence. See 45 C.F.R. § 164.512(c).

- c. Disclosures in administrative and judicial proceedings are discussed in Section F.1 below.
- d. Disclosures for law enforcement purposes:
  - (1) Pursuant to laws requiring the reporting of certain types of wounds or physical injuries.
  - (2) In compliance with and limited by the relevant requirements of:
    - (a) A court order, court-ordered warrant, or subpoena or summons issued by a judicial officer;
    - (b) A grand jury subpoena; or
    - (c) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by law, provided that:
      - 1) The information sought is relevant and material to a legitimate law enforcement inquiry;
      - 2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
      - 3) De-identified information could not reasonably be used.
  - (3) Identification and location information for the purpose of locating a suspect, fugitive, material witness, or missing person; see 45 C.F.R. § 164.512(f)(2).
  - (4) Identity of crime victims; see 45 C.F.R. § 164.512(f)(3).

- (5) To alert authorities to a suspicious death.
  - (6) Evidence of criminal conduct that the Covered Entity reasonably believes occurred on its premises.
  - (7) Reporting by emergency healthcare providers necessary to alert authorities to commission, nature, and location of a crime, or the identity, description, and location of a perpetrator.
3. Other permitted uses or disclosures
- a. Public health activities
  - b. Disclosures to health oversight agencies
  - c. Disclosures about decedents to coroners, medical examiners, and funeral directors
  - d. Disclosures to facilitate cadaveric organ, eye, or tissue donation and transplantation.
  - e. Disclosures for research purposes *if* a waiver of individual authorization has been approved by an institutional review board or privacy board as specified in 45 C.F.R. § 164.512(i).
  - f. Certain disclosures where necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; see 45 C.F.R. § 164.512(j).
  - g. Miscellaneous disclosures for specialized government functions – see 45 C.F.R. § 164.512(k).
  - h. Disclosures authorized by laws relating to workers' compensation and similar programs.

**D. Disclosures Subject to Patient's Opportunity to Object**

1. Facility directories
2. Disclosures to family members
3. Uses and disclosures when the affected individual is present

4. Limited uses and disclosures when the individual is not present, incapacitated or in an emergency
  - a. Reasonable exercise of professional judgment
  - b. Disclosure in best interest of patient
  - c. Limited to disclosure of PHI that is directly relevant to the receiving person's involvement with the patient's health care
  - d. Example: Relative picks up filled prescription, medical supplies, or X-rays.
5. Uses and disclosures for the purpose of coordinating disaster relief with authorized agencies.

**E. Authorization by Affected Individual**

1. If a use or disclosure is not otherwise permitted or required under the HIPAA privacy regulations, a Covered Entity may not use or disclose PHI without an authorization meeting the requirements of 45 C.F.R. § 164.508(b)(1).
2. When a Covered Entity obtains or receives a valid authorization for its use or disclosure of PHI, the use or disclosure must be consistent with such authorization.
3. Requirements for valid authorizations
  - a. The authorization must be written in plain language, and a copy of the signed authorization must be provided to the individual who signed it.
  - b. Core elements: A valid authorization must contain at least the following elements:
    - (1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
  - (3) The name or other specific identification of the person(s), or class of persons, to whom the Covered Entity may make the requested use or disclosure.
  - (4) A description of each purpose of the requested use or disclosure.
  - (5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
  - (6) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.
- c. Required statements: In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
- (1) The individual's right to revoke the authorization in writing, and either:
    - (a) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
    - (b) To the extent that such exceptions are set forth in the Covered Entity's Notice of Privacy Practices, a reference to that NPP.
  - (2) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either that:
    - (a) The Covered Entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs

the authorization (if none of the exceptions specified in 45 C.F.R. § 164.508(b)(4) applies); or

- (b) The consequences to the individual of a refusal to sign the authorization when one of the exceptions to 45 C.F.R. § 164.508(b)(4) permits the Covered Entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
  - d. If the authorization is for marketing purposes, and the marketing involves direct or indirect remuneration to the Covered Entity from a third party, the authorization must state that such remuneration is involved.
4. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except in certain limited circumstances spelled out in 45 C.F.R. § 164.508(b)(3).
5. An authorization is considered to be defective, and hence invalid, if:
- a. The expiration date has passed or the expiration event is known by the Covered Entity to have occurred;
  - b. The authorization has not been filled out completely, with respect to a core element described in section 3.b above (if applicable);
  - c. The authorization is known by the Covered Entity to have been revoked;
  - d. The authorization is combined with another document to create a compound authorization, except as permitted by 45 C.F.R. § 164.508(b)(3);
  - e. The signing of the authorization was required in order for the individual to receive treatment, payment, enrollment in the health plan, or eligibility for benefits (except as permitted by 45 C.F.R. § 164.508(b)(4));

- f. Any material information in the authorization is known by the Covered Entity to be false.

**F. Other Provisions of Special Interest to Lawyers**

1. Judicial and administrative proceedings

- a. A Covered Entity may disclose PHI in the course of any judicial or administrative proceeding:
  - (1) In response to an order of a court or administrative tribunal, provided that the Covered Entity discloses only the PHI expressly authorized by such order; or
  - (2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:
    - (a) The Covered Entity receives satisfactory assurance, as described in paragraph 1.b(1) below, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or
    - (b) The Covered Entity receives satisfactory assurance, as described in paragraph 1.b(2) below, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order (as described in paragraph 1.c below).
    - (c) The Covered Entity itself makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraphs 1.b(1)(a), (b), and (c) below or to seek a qualified protective order.
- b. “Satisfactory assurances” of:

- (1) Reasonable efforts to notify the affected person means that the Covered Entity has received from the party seeking the information a written statement and accompanying documentation demonstrating that:
  - (a) The party requesting the information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
  - (b) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and
  - (c) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
    - 1) No objections were filed; or
    - 2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
- (2) Reasonable efforts to secure a qualified protective order means that the Covered Entity has received from the party seeking the information a written statement and accompanying documentation demonstrating that:
  - (a) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

- (b) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.
  - c. A *qualified protective order* is an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:
    - (1) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
    - (2) Requires the return to the Covered Entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.
- 2. Lawyer as Business Associate of Covered Entity
  - a. Section 160.504(e)(1) of the HIPAA privacy regulations permits a Covered Entity to disclose PHI to a *Business Associate* and may allow a Business Associate to create or receive protected health information on its behalf, if the Covered Entity has a written contract, agreement or arrangement with the Business Associate that meets the applicable requirements of 45 C.F.R. § 164.504(e).
    - (1) Covered Entities may disclose protected health information to an entity in its role as a Business Associate only to help the Covered Entity carry out its healthcare functions – not for the Business Associate’s independent use or purposes, except as needed for the proper management and administration of the Business Associate.
    - (2) Where a Covered Entity knows of a material breach or violation by the Business Associate of the contract or agreement, the Covered Entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or

arrangement. If termination of the contract or agreement is not feasible, the Covered Entity is required to report the problem to the OCR.

- b. For outside counsel, it is important to note that the definition of “Business Associate” specifically includes anyone who provides legal services to or for a Covered Entity, where the provision of the service involves the disclosure of individually identifiable health information from the Covered Entity or from another of its Business Associates, to the lawyer. See 45 C.F.R. § 160.103 (definition of “Business Associate”). Keeping this definition in mind:
- (1) A defense lawyer who represents a physician in a malpractice claim *is* a Business Associate of the physician, and must have a Business Associate agreement with him.
  - (2) The plaintiff’s lawyer suing the physician *is not* a Business Associate of the physician.
  - (3) The plaintiff’s lawyer who wishes to obtain her client’s medical records from healthcare providers who are not defendants in the litigation *is not* a Business Associate of such providers (because she is not providing legal services to them) – although they may insist she is and require her to sign a Business Associate agreement anyway. (The proper approach would be to supply a HIPAA-qualifying authorization to these healthcare providers.)
  - (4) The commercial litigator who represents a hospital in a dispute over a failed real estate deal *is not* a Business Associate of the hospital because the representation does not involve access by the lawyer to individually identifiable health information.
- c. A Business Associate contract must:
- (1) Establish the permitted and required uses and disclosures of PHI by the Business Associate. The

contract may not authorize the Business Associate to use or further disclose the information in a manner that would violate the requirements of the HIPAA privacy regulations if done by the Covered Entity.

- (2) Provide that the Business Associate will:
- (a) Not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
  - (b) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
  - (c) Report to the Covered Entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
  - (d) Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;
  - (e) Make available PHI when access, amendment of the PHI, or an accounting of PHI disclosures is requested by the affected individual;
  - (f) Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity available to the HHS Secretary for purposes of determining the Covered Entity's compliance with the regulations; and

- (g) At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity that the Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
  - (3) Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the Business Associate has violated a material term of the contract.
- d. Note: Once individually identifiable health information is in the possession of a person who is neither a Covered Entity nor the Business Associate of a Covered Entity, that information is no longer PHI, and the HIPAA regulations do not apply to it. (There may, of course, be other legal obligations, such as those created by contract or other laws regarding privacy, that attach to such information.)
3. Mandatory disclosure of PHI to the affected individual
- a. Covered Entities are required to permit patients to view and copy their own protected health information in certain specified circumstances.
  - b. Individuals generally have the right to view and copy their own PHI upon request and in accordance with the Covered Entity's policies and procedures, except for the following PHI:
    - (1) Psychotherapy notes;
    - (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

- (3) Certain clinical laboratory information.
- c. If one of these exceptions applies, and in certain other specified circumstances specified in 45 C.F.R. § 164.524(a)(2), the Covered Entity may deny access and there is no right to review of that decision.
  - d. A Covered Entity may deny access, subject to the patient's right to have that denial reviewed by a licensed health professional not involved in the original decision, if:
    - (1) A licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
    - (2) The protected health information makes reference to another person (unless such other person is a healthcare provider) and a licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
    - (3) The request for access is made by the individual's personal representative and a licensed healthcare professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
  - e. The Covered Entity must respond to a request for access to PHI within 30 days (60 days if the information is kept off-site).
  - f. The Covered Entity must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as the parties agree to. If the

individual agrees, a summary or explanation may be provided in lieu of the actual records.

- g. If the individual requests a copy or a summary, the Covered Entity may impose a reasonable, cost-based fee for providing it. The fee may be based only on the cost of supplies for and labor of copying (and postage, if the individual has requested that the materials be mailed). If the individual requests a summary or explanation, the Covered Entity may charge a fee for preparing it, if the requestor has agreed to pay such fee at the time the request was made.

## **G. Penalties**

- 1. Generally, enforcement of the HIPAA privacy regulations is by the Office of Civil Rights (OCR) in the U.S. Department of Health and Human Services (DHHS).
  - a. OCR has announced several times that the government's initial focus will be to assist Covered Entities in complying with the regulations.
  - b. Anyone who believes a Covered Entity is not complying with the HIPAA privacy regulations may file a complaint with the HHS Secretary.
  - c. Complaints must:
    - (1) Be filed in writing, either on paper or electronically.
    - (2) Name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable regulations.
    - (3) Be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.
  - d. The HHS Secretary may investigate complaints. Such investigation may include a review of the pertinent policies, procedures, or practices of the Covered Entity and of the

circumstances regarding any alleged acts or omissions concerning compliance.

- e. The HHS Secretary can also conduct compliance reviews of Covered Entities to determine whether they are complying with the regulations.
  - f. Covered Entities must cooperate with compliance reviews and complaint investigations.
2. Secretarial action resulting from complaint or compliance review
- a. If a complaint investigation or compliance review indicates a failure to comply:
    - (1) The Secretary will so inform the Covered Entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.
    - (2) If the Secretary determines that the matter cannot be resolved by informal means, he may issue to the Covered Entity and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.
  - b. If, after an investigation or compliance review, the Secretary determines that further action is not warranted, the Secretary will so inform the Covered Entity and, if the matter arose from a complaint, the complainant in writing.
  - c. DHHS plans to issue an Enforcement Rule that applies to all of the regulations that the Department issues under the Administrative Simplification provisions of HIPAA. This regulation will address the imposition of civil monetary penalties and the referral of criminal cases where there has been a violation of this rule.
3. Statutory penalties
- a. Criminal violation – intentional use and disclosure

- (1) A person who knowingly obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person, is subject to criminal penalties which vary with the seriousness of the violation.
  - (2) The basic violation is subject to a fine of \$50,000 and/or imprisonment for one year.
  - (3) If the offense is committed under false pretenses, the penalties are \$100,000 and/or five years imprisonment.
  - (4) If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the penalties are \$250,000 and/or ten years imprisonment.
- b. Civil monetary penalties for noncompliance with the regulations
- (1) General rule: The Secretary may impose a fine of \$100 per violation (using administrative procedures already applicable to civil monetary penalties under Medicare), “except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000.”
  - (2) Limitations: A penalty may not be imposed if:
    - (a) The act in question is punishable under the criminal provision described in 3.a above.
    - (b) It is established to the satisfaction of the Secretary that the person liable for the penalty did not know, and by exercising reasonable diligence would not have known, that he or she violated the provision.

- (c) The failure to comply was due to reasonable cause and not to willful neglect. (This may result in complete waiver of the penalty or in a partial waiver “to the extent that the payment of such penalty would be excessive relative to the compliance failure involved.”)
- (d) The failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty knew, or by exercising reasonable diligence would have known, that the failure to comply occurred. This 30-day period may be extended at the discretion of the Secretary.

## **H. Interplay of HIPAA Privacy Regulations with State Law**

1. The HIPAA statute gave the HHS Secretary the power to specify by regulation the degree to which the federal privacy law would preempt contrary state law provisions relating to the privacy of individually identifiable health information. 42 U.S.C. § 1320d-7(a)(2)(B). As a result, the HIPAA privacy regulations contain unusual provisions regarding the interaction between those regulations and state law.
2. The regulations deal with preemption in four ways:
  - a. By setting forth the general rule that a standard, requirement, or implementation specification in the HIPAA privacy regulations that is contrary to a provision of State law preempts the provision of State law, unless one of four exceptions applies;
  - b. By stating clearly that state law preempts the federal rules in two areas;
  - c. By establishing a complex formula for determining whether or not a particular state law provision is preempted by HIPAA; and
  - d. By establishing procedures whereby a State’s chief elected official can request that the HHS Secretary determine that

an exception to federal preemption is appropriate for a particular provision of state law.

3. In all of these circumstances, a provision of state law is defined as “contrary” to a HIPAA requirement if:
  - a. A Covered Entity would find it impossible to comply with both the state and federal requirements; or
  - b. The provision of state law is an obstacle to the accomplishment and execution of the full purposes and objectives of the HIPAA privacy statute and regulations.
4. Areas where state law clearly preempts the HIPAA regulations:
  - a. The provision of state law (including state procedures established under such law) provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.
  - b. The provision of state law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.
5. The most difficult provision in the HIPAA preemption standards for lawyers to grapple with is 45 C.F.R. § 160.203(b), which states that the HIPAA regulations preempt contrary *state law* unless the provision of state law *relates to the privacy of individually identifiable health information* and is *more stringent* than a standard, requirement, or implementation specification in the HIPAA privacy regulations. The definitions of the terms provided here in italics are key:
  - a. “State law” means a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law.
  - b. “Relates to the privacy of individually identifiable health information” means, with respect to a state law, that the state law has the specific purpose of protecting the privacy

of health information or affects the privacy of health information in a direct, clear, and substantial way.

- c. “More stringent” means that the state law in question:
- (1) Prohibits or restricts a use or disclosure of PHI in circumstances under which such use or disclosure otherwise would be permitted under the HIPAA privacy regulations , except if the disclosure is:
    - (a) Required by the HHS Secretary in connection with determining whether a Covered Entity is in compliance with the HIPAA regulations; or
    - (b) To the individual who is the subject of the individually identifiable health information.
  - (2) Permits the individual who is the subject of the individually identifiable health information greater rights to access or amend the information.
  - (3) Permits the subject individual to have a greater amount of information with regard to use, disclosure, rights, and remedies concerning the information.
  - (4) With respect to the form, substance, or the need for express legal permission from the subject individual for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission.
  - (5) With regard to accounting for disclosures, provides for the retention of records for a longer duration or reporting of more detailed information.

- (6) In general, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.
6. Determination by the HHS Secretary that an exception is warranted
- a. As noted above, such a determination can only be requested through the State's highest elected official or his designee. Procedures for such requests may be found at 45 C.F.R. § 160.204.
  - b. In order to grant such an exception, the Secretary must determine that the provision of state law:
    - (1) Is necessary:
      - (a) To prevent fraud and abuse related to the provision of or payment for health care;
      - (b) To ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
      - (c) For state reporting on healthcare delivery or costs; or
      - (d) For purposes of serving a compelling need related to public health, safety, or welfare, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
    - (2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. § 802), or that is deemed a controlled substance by state law.

**V. TECHNOLOGICAL APPROACHES TO PATIENT PRIVACY: THE HIPAA SECURITY RULE**

**A. The Basics**

1. The Security Rule requires Covered Entities to protect the confidentiality and availability of all electronic protected health information that the Covered Entity creates, receives, maintains or transmits.
2. The Security Rule requires:
  - a. Protections against threats or hazards to security<sup>1</sup>;
  - b. Protections against unauthorized uses or disclosures; and
  - c. Ensuring compliance by the Covered Entity's workforce.
3. These requirements are accomplished through various levels of security measures that can be applied according to the size and structure of the Covered Entity.
4. The Security Rule was adopted at 68 Fed. Reg. 8333 (Feb. 20, 2003), with an effective date of April 21, 2003. However, affected providers, clearinghouses, and large health plans will have until April 20, 2005 to comply with the standards. (The compliance date for small health plans is April 20, 2006.)
5. The Security Rule was designed to work in tandem with the HIPAA privacy regulations, and uses many of the same terms and definitions.
6. The Rule is organized around three categories -- administrative, physical and technical safeguards -- which are discussed in sections D, E, and F below.
7. As in the privacy regulations, information stripped of all identifiers does not come within the purview of the final Security Rule.
8. Note that section 164.530(c) of the privacy regulations still requires application of "appropriate security" to all PHI in any form.

---

<sup>1</sup> "Security or Security measures" encompass all of the administrative, physical, and technical safeguards in an information system. 45 C.F.R. § 164.304.

**B. Applicability and scope (45 C.F.R. § 164.302)**

1. The standards apply to the following:
  - a. A health plan.
  - b. A healthcare clearinghouse or healthcare provider that takes one of the following actions:
    - (1) Processes any electronic transaction between any combination of healthcare entities listed in § 164.302.
    - (2) Electronically maintains any health information used in an electronic transmission that has been sent or received between any combination of healthcare entities listed in § 164.302.
2. If a healthcare clearinghouse is part of a larger organization, it is required to ensure that all health information is protected from unauthorized access by the larger organization.
3. Applicability to researchers
  - a. The final Security Rules apply only to researchers who are part of a Covered Entity or are within the healthcare component of a hybrid Covered Entity.
  - b. Researchers outside of these categories are not subject to the Security Rule unless they independently qualify as a Covered Entity.

**C. General Rules (45 C.F.R. § 164.306)**

1. Covered Entities must do the following:
  - a. Ensure<sup>2</sup> the confidentiality, integrity, and availability of all electronic PHI the Covered Entity creates, receives, maintains or transmits.

---

<sup>2</sup> The Security Rule uses the word “ensure” frequently; Covered Entities must “ensure” confidentiality, integrity and availability of electronic PHI and “ensure” compliance by their workforce. In the preamble to the Rule, DHHS acknowledged that there is no perfect system without risk, and said that “ensure” does not

- (1) "Integrity" means the property that data or information have not been altered or destroyed in an unauthorized manner.
  - (2) "Confidentiality" means the property that data or information is not made available or disclosed to unauthorized persons or processes.
  - (3) "Availability" means the property that data or information is accessible and useable upon demand by an authorized person.
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
  - c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.
  - d. Ensure compliance with the Security Rule by its workforce.
2. Flexibility of approach
- a. Covered entities may use any security measures that allow the Covered Entity to reasonably and appropriately implement the standards and implementation specifications.
  - b. Through the use of an implementation specification analysis, Covered Entities can now consider several factors, which allows more flexibility and prevents the imposition of such a large burden on smaller Covered Entities. In deciding which security measures to use, a Covered Entity must take into account the following factors:
    - (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; and

---

mean protect at great expense: it means take steps to the best of one's ability, a balancing of risk and benefit.

- (4) The probability and criticality of potential risks to electronic PHI.

3. Implementation specifications

- a. The Security Rule contains implementation specifications that are either required or “addressable.”
- b. If an implementation specification is required, it must be implemented.
- c. If an implementation specification is addressable, the Covered Entity must:
  - (1) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic PHI; and
  - (2) As applicable to the entity:
    - (a) Implement the implementation specification if reasonable and appropriate; or
    - (b) If implementing the implementation specification is not reasonable and appropriate --
      - 1) Document why it would not be reasonable and appropriate to implement the implementation specification; and
      - 2) Implement an equivalent alternative measure if reasonable and appropriate.
- d. Internal and external data. The preamble to the Security Rule clarifies that there is no distinction between internal data and external data, which means that Covered Entities need to ensure all safeguards apply not only to outside

transmission of PHI, but also their internal network and security measures.

**D. Security Administrative Safeguards (45 C.F.R. § 164.308)**

1. The term "administrative safeguards" refers to administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information. 45 C.F.R. § 164.304.
2. As part of the administrative safeguards, a Covered Entity must:
  - a. Implement policies and procedures to prevent, detect, contain and correct security violations. The implementation specifications associated with this process include:
    - (1) Risk analysis (required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the Covered Entity.
    - (2) Risk management (required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
    - (3) Sanction policy (required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Covered Entity.
    - (4) Information system activity review (required). Implement procedures to regularly review records of information system activity, such as audit logs, access<sup>3</sup> reports and security incident tracking reports.

---

<sup>3</sup> "Access," as used in the Security Rule, refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource. 45 C.F.R. § 164.304.

- (a) “Information system” refers to an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. 45 C.F.R. § 164.304.
  - (b) A “security incident” is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *Id.*
- b. Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule for the entity.
- c. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, and to prevent those workforce members who do not have access from obtaining access to electronic PHI. The implementation specifications associated with this process include:
  - (1) Authorization and/or supervision (addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.
  - (2) Workforce clearance procedure (addressable). Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.
  - (3) Termination procedures (addressable). Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends.
- d. Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable

requirements of the HIPAA privacy regulations. The implementation specifications associated with this process include:

- (1) Isolating healthcare clearinghouse functions (required). If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization.
  - (2) Implement access authorization policies and procedures for granting access to electronic PHI, for example, through access to a workstation,<sup>4</sup> transaction, program, process, or other mechanism (addressable).
  - (3) Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process (addressable). (A "user" is defined as a person or entity with authorized access.)
- e. Implement a security awareness and training program for all members of the workforce, including management. Implementation specifications associated with this process include:
- (1) Security reminders (addressable). Periodic security updates.
  - (2) Protection from malicious software (addressable). Procedures for guarding against, detecting, and reporting malicious software. ("Malicious software" means software, for example, a virus, designed to damage or disrupt a system.)

---

<sup>4</sup> "Workstation" refers to any electronic computing device -- for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. 45 C.F.R. § 164.304. This would include a handheld device (such as a Blackberry or Palm Pilot), and a home computer.

- (3) Log-in monitoring (addressable). Procedures for monitoring log-in attempts and reporting discrepancies.
- f. Password management (addressable). Procedures for creating, changing and safeguarding passwords. “Password” refers to confidential authentication information composed of a string of characters. (“Authentication” means the corroboration that a person is the one claimed.)
  - g. Implement policies and procedures to address security incidents through the following implementation specification (required): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Covered Entity; and document security incidents and their outcomes.
  - h. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI. The implementation specifications associated with this contingency plan include:
    - (1) Data backup plan (required). Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.
    - (2) Disaster recovery plan (required). Establish (and implement as needed) procedures to restore any loss of data.
    - (3) Emergency mode operation plan (required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
    - (4) Testing and revision procedures (addressable). Implement procedures for periodic testing and revision of contingency plans.

- (5) Applications and data criticality analysis (addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.
    - i. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, that establishes the extent to which an entity's security policies and procedures meet the Rule's requirements.
3. Business Associate contracts and other arrangements
  - a. A Covered Entity, in accordance with §164.306 (General Rules), may permit a Business Associate to create, receive, maintain or transmit electronic PHI on the Covered Entity's behalf only if the Covered Entity obtains satisfactory assurances, in accordance with the organizational requirements that the Business Associate will appropriately safeguard the information.
  - b. This standard does not apply to:
    - (1) The transmission by a Covered Entity of electronic PHI to a healthcare provider concerning the treatment of an individual.
    - (2) The transmission of electronic PHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) (organizational requirements for group health plans) and §164.504(f) (Privacy Rule organizational requirements for group health plans) apply and are met; or
    - (3) The transmission of electronic PHI from or to other agencies providing the services at §164.502(e)(1)(ii)(C) (Privacy Rule Business Associates), when the Covered Entity is a health plan that is a government program providing public

benefits, and if the requirements of §164.502(e)(1)(ii)(C) are met.

- c. The satisfactory assurances are to be documented through a written contract or other arrangement with the Business Associate that meets the applicable requirements of §164.314(a).
- d. A Covered Entity that violates the satisfactory assurances it provided as a Business Associate of another Covered Entity will be in noncompliance with the standards, implementation specifications, and requirements of § 164.308(b)(3) and § 164.314(a) (organizational requirements for Business Associates).

**E. Physical Safeguards (45 C.F.R. § 164.310)**

- 1. "Physical safeguards" are physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. 45 C.F.R. § 164.304.
- 2. Under this section, a Covered Entity must adopt standards for facility access controls, workstation use, workstation security, and device and media controls.
- 3. Facility access controls: The entity 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. The implementation specifications associated with these controls include:
  - a. Contingency operations (addressable). 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.
  - b. Facility security plan (addressable). Implement policies and procedures to safeguard the facility and the equipment

therein from unauthorized physical access, tampering and theft.

- c. Access control and validation procedures (addressable). 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.
  - d. Maintenance records (addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which related to security (for example, hardware, walls, doors, and locks).
4. Workstation use: The Covered Entity must 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 workstation that can access electronic protected health information.
  5. Workstation security: The Covered Entity must implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.
  6. Device and media controls: The Covered Entity must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.
    - a. Definitions
      - (1) "Electronic media" includes:
        - (a) Computer fax but not paper fax;
        - (b) Voice mail;
        - (c) Copier;
        - (d) Telephone call; and

- (e) Video conferencing.
- (2) “Facility” refers to the physical premises and the interior and exterior of a building(s).
- b. The implementation specifications associated with these device and media controls include:
  - (1) Disposal (required). Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.
  - (2) Media re-use (required). Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.
  - (3) Accountability (addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
  - (4) Data backup and storage (addressable). Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

**F. Technical Safeguards (45 C.F.R. § 164.312)**

- 1. "Technical safeguards" refer to the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45 C.F.R. § 164.304.
- 2. Under this section, a Covered Entity must enact the following safeguards, in accordance with §164.306 (General Rules):
  - a. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. The implementation specifications associated with these controls include:
    - (1) Unique user identification (required). Assign a unique name and/or number for identifying and tracking user identity.

- (2) Emergency access procedure (required). Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
  - (3) Automatic logoff (addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- b. Encryption and decryption (addressable). Implement a mechanism to encrypt and decrypt electronic PHI. ("Encryption" refers to the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. 45 C.F.R. § 164.304.)
  - c. Implement hardware, software, and/or procedural audit control mechanisms that record and examine activity in information systems that contain or use electronic PHI.
  - d. Implement policies and procedures to protect electronic PHI from improper alteration or destruction., as follows:  
The implementation specification associated with this system integrity requirement is as follows: Mechanism to authenticate electronic PHI (addressable). Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.
  - e. Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.
  - f. Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. The implementation specifications associated with these transmission security measures include:
    - (1) Integrity controls (addressable). Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

- (2) Encryption (addressable). Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

**G. Miscellaneous Other Requirements**

1. Business associates – 45 C.F.R. § 164.314(a)
  - a. Security requirements also pertain to the electronic storage, maintenance, and transmission of PHI by Business Associates (through the Business Associate agreement).
  - b. The contract between a Covered Entity 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 Covered Entity as required by the Security Rule;
    - (2) Ensure that any agent, including a subcontractor, 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 Covered Entity determines that the Business Associate has violated a material term of the contract.
  - c. Special rules apply when a Covered Entity and its Business Associate are both governmental entities.
2. Requirements for group health plans – 45 C.F.R. § 164.314(b)
  - a. Except when the only electronic disclosures of PHI to a plan sponsor are as authorized by certain specific sections of the privacy regulations, a group health plan must ensure

that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

- b. Affected plan sponsors are subject to required implementation specifications which mandate that they must:
- (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 group health plan;
  - (2) Ensure that the adequate separation required by §164.504(f)(2)(iii) (organizational requirements for group health plans) is supported by reasonable and appropriate security measures;
  - (3) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
  - (4) Report to the group health plan any security incident of which it becomes aware

3. Policies and procedures – 45 C.F.R. § 164.316(a)
  - a. A Covered Entity must implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule, taking into account those factors specified in 45 C.F.R. §164.306 (General Rules).
  - b. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of the Privacy Rule. A Covered Entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the regulations.
  
4. Documentation – 45 C.F.R. § 164.316(b)
  - a. A Covered Entity must maintain the policies and procedures implemented to comply with the Security Rule in written form; and if an action, activity or assessment is required by the Rule to be documented, maintain a written record of the action, activity or assessment. Written records may be in electronic form.
  - b. The implementation specifications associated with the documentation requirement are as follows:
    - (1) Time limit (required). Retain the documentation required by this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
    - (2) Availability (required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
    - (3) Updates (required). Review documentation periodically, and update as needed, in response to

environmental or operational changes affecting the security of the electronic PHI.

#### **H. Selected Points from Regulatory Preamble**

1. A Covered Entity must use reasonable and appropriate safeguards. This means evaluating the security risks an entity faces, implementing countermeasures proportional to those risks, and managing the countermeasures to remain current with new or increased risks. (Risk assessment and risk management).
2. DHHS believes the standards set by the Security Rule to be consistent with industry practice. Healthcare and payor industry groups were consulted, though the National Automated Clearing House Association (NACHA) was not.
3. The National Institute of Standards and Technology (NIST) is working to create a list of federally "certified" secure software.
4. Encryption
  - a. When electronic PHI is sent from one location to another, it must be protected in a manner commensurate with the associated risk.
  - b. Covered Entities are "encouraged" to use encryption for internet transmission.
  - c. Use of encryption for data in transit or at rest should be based on an entity's risk analysis.
5. Regulations for electronic signatures will be published at a later date.
6. Regulations for enforcement will be published at a later date.