

# WISCONSIN CHIEFS OF POLICE ASSOCIATION

## LEGAL UPDATE

March 5, 2004

Kimberly, Wisconsin

James R. Korom  
von Briesen & Roper, S.C.  
411 East Wisconsin Avenue, Suite 700  
Milwaukee, Wisconsin 53202  
(414) 276-1122  
(800) 622-0607  
(414) 287-1231 (Mr. Korom's direct line)  
[jkorom@vonbriesen.com](mailto:jkorom@vonbriesen.com)

## I. THE “NEW” OPEN RECORDS LAW: IS THE WOZNICKI FIX IN?

### A. Overview of the Legal Developments Leading to the Change

1. *Woznicki v. Erickson*
2. *MTEA v. Milw. Bd. of School Directors*
3. *Monfils v. Charles*

### B. The Possible Role of Politics in the Change

1. Including police/fire chief in the definition of local public official
2. Removing the right to notice and challenge from ordinary citizens
3. The interests of the press and the right to intervene in the challenge process

### C. Section 19.31 of the Wisconsin Statutes States That:

[I]t is declared to be the public policy of this state that all persons are entitled to the greatest possible information regarding the affairs of government and the official acts of those officers and employees who represent them. Further, providing persons with such information is declared to be an essential function of representative government and an integral part of the routine duties of officers and employees whose responsibility it is to provide such information. To that end, ss. 19.32 to 19.37 shall be construed in every instance with a presumption of complete public access, consistent with the conduct of governmental business. The denial of public access generally is contrary to the public interest, and only in exceptional cases may access be denied.

### D. *Local Public Office*, § 19.32 (1dm)

(1dm) “local public office” has the meaning given in s. 19.42 (7w), and also includes any appointive office or position of a local governmental unit in which an individual serves as the head of a department, agency, or division of the local governmental unit, but does not include any office or position filled by a municipal employee, as defined in s. 111.70(1)(i).

### E. *Employee*, § 19.32 (1bg)

19.32 (1bg) “Employee” means any individual who is employed by an authority, other than an individual holding local public office or a state public office, or any individual who is employed by an employer other than an authority.

### F. Exemptions From “Employee Personnel Records,” § 19.36 (10)

1. Information maintained, prepared, or provided by an employer concerning the home address, home electronic mail address, home telephone number, or social security number of an employee, unless the employee authorizes the authority to provide access to such information.
  2. Information relating to the current investigation of a possible criminal offense or possible misconduct connected with employment by an employee prior to disposition of the investigation.
  3. Information pertaining to an employee's employment examination, except an examination score if access to that score is not otherwise prohibited.
  4. Information relating to one or more specific employees that is used by an authority or by the employer of the employees for staff management planning, including performance evaluations, judgments, or recommendations concerning future salary adjustments or other wage treatments, management bonus plans, promotions, job assignments, letters of reference, or other comments or ratings relating to employees.
- G. "DAYS" Computed as Business Days (i.e. Excluding Saturday, Sunday, and Legal Holidays).
- H. Each Office Must Adopt, Display and Make Available for Inspection and Copying a Notice Containing:
1. A description of its organization and the times and places may access records;
  2. The legal custodian for the office;
  3. The costs for records;
  4. The method by which the public may request access or copies to records; and
  5. Those positions you consider to be a "local public office"
- I. A Step-By-Step Analysis in Approving or Denying Records Requests
1. Does the request have an unreasonable limitation as to subject matter and length of time?
  2. Does it meet any of the statutory exceptions (examples above)?
  3. Does it meet any of the exemptions under section 19.85 and can the custodian show that there is a "need to restrict public access" at that time?  
Some examples:

- a) Deliberations of a pending judicial or quasi-judicial nature;
  - b) Documents regarding pending investigations or pending discipline or removal of public employee;
  - c) Documents regarding pending decisions relating to employment, promotion, compensation, or performance evaluation of any public employee;
  - d) Documents regarding the negotiation for purchase of public properties, investing of public funds or other public business where competitive or bargaining reasons require a closed session;
  - e) Documents relating to the financial, medical, social or personal histories or disciplinary data of specific persons which would be likely to negatively affect reputation;
  - f) Legal advice.
4. Does the Public's interest in not disclosing the record outweigh the public's interest in disclosing the record?
5. If you decide to disclose:
- a) Are they the records of a "local public official?" If so, give notice and opportunity to "augment" the record.
    - 1) Notice within three days of the decision to release.
    - 2) Notice by certified mail or personal service
    - 3) Notice must "briefly describe" the record
    - 4) Notice must describe rights to augment
    - 5) LPO has five days after notice to augment in writing
    - 6) Final release must contain the record as augmented
    - 7) No right to challenge release for LPO
  - b) Are they records of an "employee?" If so, give notice and opportunity to challenge. (Note: Specific exemptions from release considered above):
    - 1) Notice within three days of the decision to release
    - 2) Notice by certified mail or personal service

- 3) Notice must “briefly describe” the record
- 4) Notice must describe challenge process
- 5) Employee may give notice of intent to seek court order within five days of receipt of notice
- 6) Employee may commence action on court within 10 days of receipt of notice
- 7) If no action commenced within 12 days of sending the notice, release required
- 8) If action commenced, release prohibited until court action complete
- 9) Custodian responsible to notify requester of results of court action if requester does not intervene

J. *Hempel v. Baraboo*, No. 03-0500 (Ct. App. 2003). Allows protection of the identity of a harassment complainant’s identity as part of the balancing test. Note due process issue.

## II. HIPAA (SEE ATTACHED)

A. The Practical Issues Likely to Arise in the Police/Fire/EMT Setting.

1. Firefighters sharing information with police
2. EMTs/paramedics sharing information with police
3. Police sharing/using information against victims/suspects
4. Proper radio/dispatch practices
  - a) Dispatch with police/fire
  - b) Dispatch with EMTs/paramedics
  - c) EMTs/paramedics with the ER
5. Getting medical information from health care providers about employees.

B. HIPAA Controls Few of These Issues

1. A firefighter/police officer is normally not a covered entity
  - a) Do not regularly bill for medical services

- b) Do not transmit medical information or bills electronically
  - 2. EMTs/paramedics normally are covered if they electronically bill for medical services.
  - 3. HIPAA allows release of Personal Health Information (PHI) by a “covered entity” for some law-enforcement purposes. Key points:
    - a) PHI defined as related to physical/mental health or condition of the individual, or the provision of health care to the individual; some statements by the patient may relate to a crime, but not to treatment.
    - b) Release of PHI to law enforcement specifically allowed for ID of suspects, witnesses and victims; for location purposes; for a death you suspect resulted from criminal conduct; or to avert serious threat to health or safety.
  - 4. PHI can be disclosed for purposes of treatment, but such disclosures must be as limited as possible to protect privacy while securing effective treatment; will impact common radio practices, requiring careful thought, training, planning, and some risk.
  - 5. PHI can be disclosed to those responsible for monitoring the quality of the medical services, for that purpose. Supervisors can review the records created by subordinates.
- C. Pre-existing Wisconsin law
- 1. Section 146.82 Wis. Stats. protects the confidentiality of patient health care records.
  - 2. There is no general exception for law enforcement; specific but narrow exceptions apply for child abuse, ongoing threat to the life of the patient, etc.
- D. If HIPAA applies, and PHI is involved, and no exception exists, patient authorizations are required.
- 1. Elements of a valid authorization are listed in HIPAA (see attached).
  - 2. Would be required for release of your employees’ medical records to you (e.g., FMLA, ADA, etc.).

**AN OVERVIEW OF THE HEALTH INSURANCE PORTABILITY AND  
ACCOUNTABILITY ACT (HIPAA) PRIVACY REGULATIONS**

*Attorney Monica Hocum (414) 287-1406*

*Attorney Sarah Elliott (414) 287-1271*

## I. WHAT IS HIPAA?

### A. *The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).*

1. The HIPAA statute was signed into law August 21, 1996, and encompasses two main components, “Portability” and “Administrative Simplification”.
  - a) The Portability provisions were implemented previously.
  - b) The Administrative Simplification provisions will include five separate sets of regulations:
    - (1) Privacy regulations.
    - (2) Transactions and Code Set Standards.
    - (3) Security and Electronic Signature Standards.
    - (4) Standard Unique Employer Identifier.
    - (5) National Standard Health Care Provider Identifier.
2. The compliance date for the privacy regulations is April 14, 2003 (or April 14, 2004, for small health plans).

### B. *Who must comply with the privacy regulations?*

1. The regulations apply to “covered entities,” which include:
  - a) Health plans.
  - b) Health care clearinghouses.
  - c) Health care providers who transmit any health information in electronic form in connection with a covered transaction.
    - (1) Health care providers are subject to the privacy regulations *only* if they electronically transmit health information in connection with a covered transaction.
2. Examples of covered entities:
  - a) A health plan includes any individual or group plan that provides or pays the cost of medical care.
  - b) A health care clearinghouse includes any entity that processes health care transactions by translating data from a given format

(e.g. non-standard) into one acceptable (standard format) to the intended payor and then forwarding the processed transaction for payment.

c) A health care provider includes hospitals, physicians, psychologists, clinical social workers and any “person or organization who furnishes, bills, or is paid for health care in the normal course of business.”

3. A number of entities fall outside of these definitions including third party administrators, researchers, life insurance companies, employers, plan sponsors and others. To the extent these entities may be a “business associate” of a covered entity, the rules will apply to them indirectly under the business associate rules.

## **II. WHAT ARE THE BUSINESS ASSOCIATES REQUIREMENTS UNDER THE PRIVACY REGULATIONS?**

### *A. Definition of business associate.*

1. A business associate is a person or entity who:

a) On behalf of a covered entity, performs or assists in the performance of, a function or activity that involves the use or disclosure of individually identifiable health information, including:

- (1) Claims processing or administration.
- (2) Data analysis, processing or administration.
- (3) Billing.
- (4) Benefit management.
- (5) Practice management.
- (6) Utilization review.
- (7) Quality assurance.
- (8) Repricing.

b) Performs any of the following services to or for a covered entity involving the use or disclosure of individually identifiable health information:

- (1) Legal.

- (2) Actuarial.
- (3) Accounting.
- (4) Consulting.
- (5) Data aggregation.
- (6) Management.
- (7) Administrative.
- (8) Accreditation.
- (9) Financial.

2. Business associates include lawyers, accountants, actuaries, consultants, third party administrators, data processing firms, billing firms and others if performance of the services involves disclosure of individually identifiable health information.

B. *Exceptions to the definition.*

1. The regulations specifically exclude from the class of business associates members of the covered entity's workforce.
2. Entities that are merely conduits for information (e.g., post office) are not business associates.
3. Financial institutions that process consumer payments for health care services are not business associates (assuming minimum necessary information is provided to such institutions).

C. *HIPAA does not authorize DHHS to regulate directly the activities of business associates.* DHHS made the requirements of the privacy regulations apply indirectly to business associates by requiring covered entities to obtain "satisfactory assurances" in the form of a written agreement that their business associates will appropriately safeguard the information.

1. The regulations prevent covered entities from providing PHI to any business associate or allowing a business associate to create PHI on behalf of the entity unless a contract exists between them limiting the business associate's uses and disclosures of the PHI.
2. The business associate's use and disclosure is limited to that which is the minimum necessary to accomplish its functions. Covered entities can rely on the business associate's representation that the information requested is the minimum necessary.

3. Covered entities will be required to amend every contract (or enter into an appropriate written agreement) with every business associate before continuing to do business with them to comply with the specific requirements of the regulations.

D. *Contract provisions or amendments.*

1. The regulations require that the business associate contract contain specific provisions. Any negotiations with regard to the contract should keep in mind that some provisions simply are not negotiable.
2. The privacy regulations require that the business associate agreement must include the following provisions:
  - a) Establish the uses and disclosures of PHI that the business associate is permitted to make on behalf of the covered entity.
  - b) Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law.
  - c) Require that the business associate will limit uses and disclosures of PHI to the minimum information necessary to accomplish the intended purposes of the use or disclosure.
  - d) Require that the business associate will use appropriate safeguards to prevent uses or disclosures other than as provided for by its contract.
  - e) Require that the business associate ensure that any agents or subcontractors to whom it provides PHI agrees to the same restrictions and conditions that apply to the business associate with respect to such information.
  - f) Require that the business associate report to the covered entity any improper use or disclosure of the information of which it becomes aware.
  - g) Require that the business associate provide a right of access to PHI to the individual.
  - h) Require that the business associate make the information available for amendment and incorporate any amendments to PHI.
  - i) Require that the business associate will provide an accounting of disclosures upon request.

- j) Require that the business associate allow the Secretary of HHS access to its internal practices, books and records relating to the use and disclosure of PHI.
- k) Authorize termination of the agreement by the covered entity if the covered entity determines the business associate violated a material term of the agreement.
- l) Require that the business associate return or destroy the PHI at the termination of the agreement, or, if not feasible, extend the protections of the agreement and limit uses and disclosures to those purposes that make return of information not feasible.

### **III. WHAT INFORMATION IS PROTECTED UNDER THE PRIVACY REGULATIONS?**

A. *The regulations are intended to ensure the privacy of protected health information (“PHI”). To be protected, health information must satisfy the following criteria:*

- 1. It must relate to:
  - a) The past, present or future physical or mental health or condition of an individual.
  - b) The provision of health care to an individual.
  - c) The past, present or future payment for the provision of health care to an individual.
- 2. It must be created or received by a health care provider, health plan, employer, or health care clearinghouse.
- 3. It must be individually identifiable, *i.e.*, it identifies or there is a reasonable basis to believe the information can be used to identify the individual patient.
- 4. It must be electronically transmitted, electronically maintained or transmitted or maintained in *any other form or medium* by a covered entity.

B. *PHI does not include the following:*

- 1. Education records covered by the Family Educational Rights and Privacy Act (“FERPA”), as amended, 20 U.S.C. 1232g.
- 2. Certain student health records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

3. Employment records held by a covered entity in its role as an employer.
- C. *The regulations cover the information itself*, not just the records that contain the information. Therefore, the regulations will apply to all records containing the information regardless of form, including oral conversations.

#### **IV. WHAT USES AND DISCLOSURES ARE PERMITTED UNDER THE PRIVACY REGULATIONS?**

A. *General rule.*

1. Covered entities may not use or disclose PHI except as specifically authorized by the individual that is the subject of the PHI or as specifically permitted or required by the regulations.

B. *Permitted uses and disclosures.*

1. A covered entity may disclose PHI to the individual who is the subject of the PHI.
2. A covered entity may use or disclose PHI for treatment, payment, or health care operations.
3. A covered entity is permitted to make incidental uses and disclosures of PHI.
  - a) The privacy regulations permit uses and disclosures that are the result of or incidental to an otherwise permitted use or disclosure, provided that the covered entity has implemented reasonable safeguards to limit unintended uses and disclosures and has complied with the minimum necessary standard.
    - (1) Example: An attorney has a file containing PHI open on her desk when building maintenance staff came in to change a light bulb.
    - (2) The incidental uses and disclosures standard is not intended to excuse erroneous uses or disclosures or those that result from mistake or neglect.
  - b) A covered entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the privacy regulations and to limit incidental uses and disclosures.
4. A covered entity may use or disclose PHI pursuant to an authorization.
5. A covered entity may use or disclose PHI as otherwise specifically permitted or required by the regulations.

C. *What is permitted for treatment, payment or health care operations?*

1. The privacy regulations permit health care providers to use or disclose PHI:
  - a) To carry out *treatment*, which includes providing, coordinating or managing health care and related services, including consultation between health care providers and referrals of the patient from one provider to another.
  - b) For purposes of *payment*, which includes obtaining premiums, determining coverage and eligibility, billing, claims management, collection activities and other associated activities.
  - c) For *health care operations*, which includes, among other things, the management functions necessary to support treatment or payment, including quality assessment and improvement; reviewing performance, competence and qualifications of professionals; utilization review; training; insurance activity; business planning and development; medical review and auditing; and business management and general administrative activities of the entity.
2. For purposes of treatment, payment or health care operations, a covered entity may:
  - a) Use or disclose PHI for its own treatment, payment or health care operations activities.
  - b) Disclose PHI for the treatment activities of other health care providers.
  - c) Disclose PHI to other health care providers or covered entities for their payment activities.
  - d) Disclose PHI to other covered entities for their health care operations if:
    - (1) Both parties have or have had a relationship with the patient.
    - (2) The purpose of the disclosure falls within the specified categories of health care operations, including quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, case management, conducting training programs, accreditation, certification, licensing or

credentialing activities, peer review, medical education, and fraud and abuse detection and compliance.

- e) Disclose PHI to another covered entity for any health care operations activities of the organized health care arrangement in which both covered entities participate.

D. *When is patient authorization required?*

1. Patient authorization is required for most types of uses or disclosures of PHI that are not for treatment, payment or health care operations, including:
  - a) Uses or disclosures requested by the individual.
  - b) Marketing of services by the covered entity (except for face to face communication by a covered entity to the individual or a promotional gift of nominal value provided by the covered entity).
  - c) Any use or disclosure of psychotherapy notes (except in limited circumstances).
  - d) Uses or disclosures for fundraising purposes (except in limited circumstances).
  - e) Disclosures to an employer for employment determinations.
  - f) For a research purpose that is unrelated to the treatment.
2. The required elements for an authorization include the following:
  - a) A description of the information to be used or disclosed.
  - b) The name or other specific identification of the person(s) or class of persons authorized to make the use or disclosure.
  - c) 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.
  - d) A description of each purpose of the requested use or disclosure.
  - e) An expiration date or event.
  - f) A statement that the covered entity will not condition treatment, payment or enrollment or eligibility on signing the authorization (or, if it is allowed to do so by the regulations, the consequences of such a refusal).

- g) The signature of the individual and the date.
  - h) A statement of the individual's right to revoke the authorization, the exceptions to this right and a description of how an individual may revoke the authorization.
  - i) A statement of the potential that the information is subject to redisclosure and no longer may be protected by the privacy regulations.
  - j) The entity must provide a copy of the authorization to the individual.
3. A covered entity generally cannot condition treatment or payment on the execution of an authorization for use and disclosure.
  4. The patient's authorization for use and disclosure cannot appear in the same document in which the patient provides informed consent for treatment.

E. *When is patient authorization not required?*

1. Covered entities may (but are not required to) disclose PHI without patient authorization, but the patient must be given an opportunity to object, in the following instances:
  - a) Health care providers can release certain directory information such as name, location in the facility, and general condition to individuals who ask for the patient by name. (Clergy also may receive religious information.) However, the patient must be given an opportunity to object and objections must be honored.
  - b) To family members, relatives or close personal friends if the information is directly relevant to the person's involvement in the individual's care or payment related to the individual's health care or to advise of the individual's location, condition, or death. (There are different standards for disclosure based upon whether the patient is present during the disclosure).
  - c) For disaster relief purposes.
2. Covered entities may (but are not required to) disclose PHI in the following circumstances, without giving the patient an opportunity to object:
  - a) To certain public health authorities and others that are authorized to collect such information for public health purposes.

- b) To a government authority if the covered entity reasonably believes the individual is a victim of abuse, neglect or domestic violence.
  - c) For health oversight activities.
  - d) In response to an order of a court or administrative tribunal.
  - e) To law enforcement personnel for suspect, witness, and victims of crimes identification and location purposes or if there is a death that the entity suspects resulted from criminal conduct.
  - f) To coroners and medical examiners to identify the decedent or determine the cause of death or to funeral directors to carry out their duties.
  - g) To organ procurement or other agencies for the purpose of facilitating organ or tissue donation or transplant.
  - h) For certain research purposes.
  - i) To avert serious threat to health or safety (but not if the information is learned in counseling or therapy or in the course of treatment to affect the propensity to commit the criminal conduct).
  - j) For specialized armed forces personnel activities deemed necessary by military command authority and for national security and intelligence activities.
  - k) For uses and disclosures required by law.
3. Covered entities must disclose PHI in the following circumstances:
- a) To the individual that is the subject of the PHI (with limited exceptions).
  - b) To the Secretary of HHS for compliance review purposes.

## **V. OBLIGATIONS AS A BUSINESS ASSOCIATE.**

### *A. Permitted Uses and Disclosures.*

1. A business associate may use or disclose PHI as permitted by the applicable business associate agreement.
2. A business associate may use or disclose PHI as required by law.

3. A business associate may use or disclose PHI as necessary for the proper management and administration of the business associate or to carry out its legal responsibilities.

B. *Minimum Necessary Requirements.*

1. When using or disclosing PHI, or requesting PHI from the covered entity, a business associate generally must make reasonable efforts to limit the PHI to the *minimum amount of information necessary* to accomplish the intended purpose of the use, disclosure or request.
  - a) The minimum necessary requirements do not apply to disclosures to or requests by a health care provider for treatment purposes, uses or disclosures authorized by the individual, or disclosures required by law or for compliance with the privacy regulations.
2. A covered entity may reasonably rely on a requested disclosure as the minimum necessary when the information is requested by another covered entity or a professional member of its workforce or a business associate.

C. *Reasonable Safeguards.*

1. A business associate must implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI. There are no standards specified in the privacy regulations.
  - a) The security regulations, which have a compliance date of April 21, 2005 for most covered entities (April 21, 2006 for small health plans) will govern the implementation standards for these safeguards.
2. Examples of such safeguards include implementing and enforcing policies and procedures for determining who within an organization reasonably needs access to PHI to perform their duties and establishing mechanisms for restricting access to computerized records pertaining to PHI.

D. *Allow Access to the Secretary of the Department of Health and Human Services.*

1. The regulations require that contracts between a covered entity and a business associate require that the business associate 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 Secretary of the Department of Health and Human Services for the purposes of determining the covered entities compliance with the regulations.

2. Many covered entities also require that they be allowed access to the business associate's internal practices, books and records relating to the use and disclosure of PHI.

E. *Assurances from Subcontractors or Agents.*

1. A covered entity may allow the business associate to use and disclose PHI received in its capacity as a business associate if:
  - a) The business associate obtains reasonable assurances from any agents the person to whom the information is disclosed that it will be held in confidence and used or further disclosed only as required by law or for the purpose for which it was disclosed; and
  - b) The person or entity receiving the information is required to notify the business associate of instances in which the confidentiality of the information has been breached.

F. *Improper Use or Disclosure of PHI.*

1. The business associate must promptly notify the covered entity of any improper uses or disclosures of PHI by the business associate or an agent or subcontractor of the business associate.
2. If there have been ongoing breaches of confidentiality of PHI or the business associate or an agent or subcontractor of the business associate has violated a material term of the business associate agreement, the covered entity must:
  - a) Take reasonable steps to cure the breach or end the violation; and
  - b) If such steps are unsuccessful, the covered entity must terminate the contract or arrangement or if termination is not feasible, the covered entity must report the problem to the Secretary of the Department of Health and Human Services.

G. *Return or Destruction of PHI.*

1. Upon termination or expiration of a contract between a covered entity and a business associate, the business associate must either return or destroy all PHI received from the covered entity, or created or received by a business associate on behalf of the covered entity.
2. The business associate must also recover or arrange for the destruction of any PHI in the possession of its subcontractors or agents.
3. To the extent that it is not feasible or lawful to return or destroy all of the PHI, the business associate must maintain the confidentiality of the PHI

for as long as the information is maintained by the business associate (or its agent or subcontractor) and the PHI shall only be used or disclosed for the purpose or purposes that made the return or destruction of the PHI infeasible.

H. *Mitigation.*

1. Covered entities are required to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of the privacy regulations by the covered entity or its business associate.

I. *Access to PHI.*

1. An individual has a right, with limited exceptions, to inspect and copy PHI maintained in a designated record set by a covered entity (and by business associates) for as long as the information is maintained.
  - a) Exceptions. Individuals do not have a right to inspect and copy the following information:
    - (1) Psychotherapy notes;
    - (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
    - (3) PHI maintained by the covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3.
2. A covered entity must comply with the timing requirements specified in the privacy regulations in responding to such a request.
3. The covered entity can require that the individual make the request for access to PHI in writing.

J. *Amendment of PHI.*

1. An individual has a right to request that a covered entity (or a business associate using or maintaining PHI on behalf of the covered entity) amend PHI or records about the individual.
2. The request for amendment of PHI may be denied if:

- a) The PHI was not created by the covered entity, unless the individual provides a reasonable basis for belief that the originator of the PHI is no longer available to act on the requested amendment.
- b) The PHI is not part of the records used by the covered entity (or business associate on behalf of the covered entity) to make decisions about the individual.
- c) The information would not be accessible by the individual as discussed in Section V.I. above; or
- d) The information is accurate and complete.

K. *Accounting of Disclosures of PHI.*

- 1. Individuals have a right to obtain an accounting of certain disclosures of PHI by a covered entity or a business associate of the covered entity.
- 2. The following disclosures do *not* need to be accounted for:
  - a) Disclosures made for treatment, payment or health care operations.
  - b) Disclosures made pursuant to an authorization signed by the individual or the individual's personal representative.
  - c) Disclosures made to the individual.
  - d) Incidental disclosures.
  - e) Disclosures for a facility directory.
  - f) Absent a prior objection to such disclosures, disclosures to family members, other relatives, or close personal friends of the individual or any other individual identified by the patient of PHI directly relevant to involvement in the individual's care or payment for the care.
  - g) Disclosures to public or private agencies for notification of relatives in disaster relief situations.
  - h) Disclosures for national security or intelligence purposes as authorized by the National Security Act.
  - i) Disclosures to correctional institutions or law enforcement officials where the patient is an inmate or in custody.
  - j) Disclosures that are part of a limited data set used pursuant to a data use agreement for the purpose of research, public health, or

health care operations, or to a business associate to create the limited data set.

- k) Disclosures made prior to April 14, 2003.
  - l) *All* other disclosures must be tracked and recorded.
3. The following information must be included on the written accounting for each disclosure:
- a) The date of disclosure;
  - b) The name and, if known, the address of the entity or person who received the PHI;
  - c) A brief description of the PHI disclosed; and
  - d) A brief summary of the purpose of the disclosure or a copy of a written request for a disclosure, if any.
4. If multiple disclosures have been made to the same person or entity during the accounting time period for a single purpose, the accounting may provide the required information for the first disclosures and then specify the frequency, periodicity, or number of disclosures made during the accounting period, and the date of the last disclosure.

## **VI. WHAT IS THE EFFECT OF THE PRIVACY REGULATIONS ON EXISTING STATE LAW?**

- A. Generally, the privacy regulations preempt state laws that are contrary to or less stringent than the regulations.
- B. DHHS may exempt specified state laws under certain circumstances. This preemption scheme establishes a minimum level of privacy for PHI, but it does not interfere with state laws providing greater protection.
- C. Wisconsin law is more stringent in some instances:
  - 1. HIPAA allows release of PHI pursuant to subpoena; Wisconsin does not unless the subpoena is issued pursuant to a lawful order of a court of record.
  - 2. HIPAA allows release of PHI to law enforcement; Wisconsin generally does not.
  - 3. HIPAA allows releases of PHI to funeral directors; Wisconsin law does not.

## **VII. LIABILITY UNDER THE PRIVACY REGULATIONS.**

### *A. Enforcement of the privacy regulations.*

1. The privacy regulations will be enforced by the DHHS Office of Civil Rights (“OCR”).
  - a) OCR has stated that its enforcement initially will be complaint driven.
  - b) OCR has stated that it will take a cooperative and educational approach and provide technical assistance.
2. In a telephone conversation with OCR we were advised that sanctions will not be imposed if a covered entity has made a reasonable attempt to comply with the regulations and has documented its efforts.

### *B. Sanctions.*

- a) HIPAA provides for significant civil and criminal penalties for violations of the privacy regulations.
- b) The sanctions only apply to covered entities, and do not apply to business associates.
- c) The privacy regulations do not provide a private right of action.

### *C. Liability as a Business Associate.*

1. If a business associate is not a covered entity, the covered entity itself can be held responsible for violations by its business associate. However, the covered entity will be subject to sanctions only if it knew of the business associate’s wrongful activity (i.e., material breach of the contract) and failed to take reasonable steps to cure the breach.
2. Covered entities do not have an obligation to monitor their business associates’ activities.
3. Many covered entities are requesting that business associates indemnify the covered entity for violations of the agreement and that the business associate provide verification of insurance covering the business associates breach of their obligations to protect the confidentiality of PHI.

## **DHHS ISSUES FINAL SECURITY RULE**

**von Briesen & Roper, s.c.**

**By: Monica C. Hocum**

### **Introduction to the Final Security Rule**

On February 20, 2003, the Department of Health and Human Services took another step toward “administrative simplification” with the publication of the long awaited and several times delayed final Security Rule. The final Security Rule requires health plans, health care providers and health care clearinghouses (collectively “covered entities”) to establish procedures and mechanisms to protect the confidentiality, integrity and accessibility of individually identifiable health information received, maintained or transmitted electronically (“Electronic Protected Health Information”). Covered entities must protect Electronic Protected Health Information against deliberate or inadvertent misuse or disclosure. To accomplish this objective, covered entities must establish and implement safeguards to ensure the confidentiality of Electronic Protected Health Information. In other words, the Security Rule provides some assurance that the Privacy Rule will be effective.

### **What is the True Compliance Date?**

The Security Rule is an expansion of the Privacy Rule requirement that covered entities and their business associates implement “appropriate administrative, technical and physical safeguards” which are necessary to maintain the confidentiality of protected health information. Although the compliance date for the Security Rule is not until April 21, 2005 (April 21, 2006 for “small health plans” defined as health plans with \$5 million dollars or less in annual receipts), since privacy cannot be ensured without the proper security measures in place, it is anticipated that the interpretation of “appropriate safeguards” will be determined by the safeguards adopted in the final Security Rule. Accordingly, despite the two-year leeway, it would be prudent for covered entities to get an early start on identification of their security risks and implementation of the necessary security measures.

### **Simplification at Last?**

The final Security Rule looks quite different from the proposed rule. To some extent, the regulations have in fact been simplified in that many of the terms and provisions contained in the proposed Security Rule have been revised so that they more closely track the terminology used in the Privacy Rule. For example, the references to a Chain of Trust Agreement in the proposed Security Rule have been abandoned in favor of expanding the scope of the Business Associate Agreement required by the Privacy Rule.

Additionally, the focus of the Security Rule has shifted from specific mandates for compliance toward a “scalable” approach which, in many instances, provides covered entities with the flexibility to determine which security measures will be most effective given its unique circumstances. With this flexibility, however, comes a requirement for documentation of the assessment and decision-making process used to determine which security measures would be

most appropriate. This documentation will also be instrumental in defending against the challenges that will likely follow claimed breaches in security as the final Security Rule does not include any safe harbors.

Noticeably absent from the final Security Rule are provisions for use of electronic signatures. This is, however, temporary as DHHS has indicated that a final rule for electronic signatures will be forthcoming.

**A Flexible Approach to Implementation.**

Each of the final security standards is categorized as having either “required” or “addressable” implementation specifications. While all covered entities must comply with the Security Rule and implement the required specifications, determination of how to comply with the addressable specifications is based, in part, on the size and complexity of each covered entity and the costs, capabilities and potential risk of improper access to Electronic Protected Health Information.

Clearly there is no one-size-fits all security solution. What works best in one environment may be ineffective in another. Covered entities will need to review and update their security measures as processes and procedures change and technology continues to evolve. A comprehensive security program will include periodic internal and external audits and continual assessment of new threats to the confidentiality and integrity of Electronic Protected Health Information.

The following matrix, summarizing the implementation specifications for the security standards, appears in Appendix A to the Security Rule. (68 FR 8380, February 20, 2003)

Standards	Sections	Implementation Specification (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
Security Management Process.....	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity (R)
Assigned Security Responsibility .....	164.308(a)(2)	(R)
Workforce Security.....	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management .....	164.308(a)(4)	Isolating Health Care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training .....	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures.....	164.308(a)(6)	Response and Reporting (R)
Contingency Plan .....	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A)
Evaluation.....	164.308(a)(8)	Applications and Data Criticality Analysis (A) (R)
Business Associate Contracts and Other Arrangement .....	164.308(b)(1)	Written Contract or Other Arrangement (R)

<b>Physical Safeguards</b>		
Facility Access Controls.....	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use.....	164.310(b)	(R)
Workstation Security.....	164.310(c)	(R)
Device and Media Controls.....	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
<b>Technical Safeguards (see § 164.312)</b>		
Access Control .....	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls.....	164.312(b)	(R)
Integrity.....	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication .....	164.312(d)	(R)
Transmission Security.....	164.312(e)(1)	Integrity Controls (A) Encryption (A)