Honigman Miller Schwartz and Cohn's *April 2001*

HIPAA LAW FOCUS

A Special Joint Newsletter on the HIPAA Privacy Rule
Prepared by the
Health Care and Employee Benefits Departments of HMS&C

SUMMARY OF STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

On December 20, 2000, the Secretary ("Secretary") of the Department of Health and Human Services ("HHS") issued the final rule governing Standards for Privacy of Individually Identifiable Health Information (the "Rule"). The Rule implements the privacy requirements of the Administrative Simplification portion of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Rule establishes standards to (a) protect and enhance consumer rights through access to and control of their Individually Identifiable Health Information, and (b) improve the quality and efficiency of health care. The privacy requirements are intended as a "floor" for protecting privacy. At the same time, the Rule seeks to balance those rights with the legitimate need of others for access to a person's health care information.

NOTEWORTHY

HMS&C has assembled a HIPAA Compliance Team, led by the attorneys listed below from our Health Care and Employee Benefits Departments, and has developed a number of tools to facilitate compliance. We stand ready to help with any aspect of your compliance planning, from developing a compliance checklist to drafting or reviewing policies, contracts, forms and other documents needed under the Rule, and assessing legal requirements beyond the Rule (*i.e.*, state law or other requirements). We would be delighted to answer your questions or otherwise assist you and your colleagues in this important process.

HMS&C Attorneys for HIPAA Compliance

Michael J. Friedman	(313) 465-7388	mjf@honigman.com
Lynn A. Kriser	(313) 465-7670 or (517) 377-0713	lak@honigman.com
Linda S. Ross	(313) 465-7526	lsr@honigman.com
Valerie S. Rup	(313) 465-7586	vsr@honigman.com

Despite efforts to delay or modify the Rule and an additional comment period imposed by the Secretary, the Rule took effect on April 14, 2001. Compliance with the Rule generally is required by April 14, 2003 (or April 14, 2004, for small health plans, *i.e.*, those with annual receipts of $5 million or less). Although the Rule may be modified,[1] it is none to soon to focus on compliance planning. The Rule requires extensive review of and changes to policies, procedures and practices regarding the use and disclosure of individual health information.

A detailed summary of key aspects of the Rule is provided below. Readers should consult the Rule[2] directly in analyzing its impact on particular situations. Capitalized terms in this summary are terms that are defined in the Rule. The term is included in bold where it is defined in this summary. An Index of Defined Terms is provided at the end of this summary.

A. Applicability

The Rule applies to Covered Entities. **A Covered Entity** is defined as a Health Plan, a Health Care Clearinghouse, or a Health Care Provider who transmits any Health Information in electronic form in connection with a transaction to which the Rule applies. The Rule further defines each of these Covered Entities as follows:

- A **Health Plan** means an individual or group plan that provides or pays for medical care, including health insurers, HMOs, Medicare, Medicaid, long-term care insurers, MEWAs, active military and veteran medical programs, CHAMPUS, FEHBP, Indian Health Services, state high risk programs, SCHIP, Medivest, and ERISA-regulated group Health Plans, whether insured or self-funded, which cover more than 50 participants or which are administered by an entity other than the sponsored employer. The term includes virtually any entity or program, but excludes plans that pay for certain excepted benefits as described in HIPAA, such as worker's compensation or coverage for on-site medical clinics (though on-site clinics may be

covered as Health Care Providers as described in Section N below), as well as any government program that is not specifically listed in the definition.

- A **Health Care Clearinghouse** is an entity that either receives Health Information in a nonstandard format and processes it into standard data elements or a standard transaction, or receives a standard transaction from an entity and processes the Health Information into a nonstandard format or nonstandard content for a receiving entity.

- A **Health Care Provider** is a provider of medical or health services or any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. This broad category will cover most physicians, hospitals, clinics, nursing homes, hospices, and physician practice groups. A Health Care Provider is a covered Health Care Provider if it transmits Health Information electronically in connection with a transaction covered by the Rule.

The jurisdiction of the Secretary in promulgating the Rule is limited to Covered Entities; however, the Rule also requires Covered Entities to enter into written agreements with Business Associates (*see* Section M below) to ensure that their Business Associates have the same confidentiality obligations as the Covered Entity. Thus, virtually every person or entity that comes into contact with Protected Health Information ("PHI") will be affected by the Rule.

B. Preemption

The Rule preempts Contrary state law.[3] A state law is **Contrary** to the Rule when it would be impossible for a Covered Entity to comply with both the Rule and the state law. A number of exceptions to preemption exist. For example, exceptions exist for situations in which the Secretary determines that a state law is needed (1) to prevent fraud and abuse, (2) to ensure proper regulation of insurance and Health Plans, (3) for state reporting on health care delivery or costs, (4) to serve a compelling need regarding public health, safety and welfare, or (5) for the primary purpose of regulating controlled substances. Exceptions also exist for state laws providing for the reporting of disease, injury, child abuse, deaths, births, public health surveillance, investigations, or interventions, and for state laws requiring Health Plans to report or give access to information for certain purposes. Additionally, the Rule does not preempt state laws relating to privacy of Health Information that are "More Stringent" than the Rule. **More Stringent** state laws are those that preclude Uses or Disclosures that would otherwise be permitted under the Rule, laws that provide individuals with greater rights of access to or amendment of PHI or with a greater amount of information, or that provide greater rights to individuals regarding consents, authorizations, record keeping, or accountings of Disclosures of PHI. Anyone may seek other exceptions to preemption, and the Rule provides a specific process for doing so.

C. Enforcement

The Secretary delegated to the Office of Civil Rights within the Department of Health and Human Services ("OCR") responsibility for enforcing the Rule. Although the Rule reflects a philosophy of enforcement based on cooperation and assistance, civil and criminal penalties may be imposed for noncompliance. Civil fines are $100 for each violation of the Rule with an annual cap of $25,000. While it is not known how a separate "violation" will be determined, certain mitigating provisions in the statute should lessen the sting of the civil penalties. For example, a penalty may not be imposed if HHS representatives believe that the person did not know, and by exercising due diligence would not have known, that his or her actions constituted a violation. Also, a penalty may not be imposed if the violation was due to reasonable cause and not to willful neglect, and the violation is corrected within a 30-day period, starting on the day the person knew or should have known of the violation. Finally, any penalty may be waived if deemed to be excessive relative to the violation involved.

On the other hand, HIPAA authorizes criminal penalties for knowingly (1) using or causing to be used someone else's unique health identifier, (2) obtaining Individually Identifiable Health Information of another person in violation of the Rule, and (3) improperly Disclosing Individually Identifiable Health Information to another person. The criminal penalties are less forgiving with graduated penalties which begin with a fine of not more than $50,000 or one year in jail or both, increasing to a fine of $100,000 and five years in jail if the offense is committed under false pretenses, and culminating in a fine of up to $250,000 and 10 years in jail if the offense is committed with the intent to sell, transfer or Use Individually Identifiable Health Information for commercial advantage. Anyone can file a complaint alleging that a Covered Entity is noncompliant. The Secretary or the OCR may conduct

investigations and compliance audits. Covered Entities must cooperate with investigations and compliance audits and permit access to relevant information.

D. Overview of the Rule

A Covered Entity must not Use or Disclose Protected Health Information except as otherwise permitted or required by the Rule. The Rule does not apply to De-Identified Information.

- **Use** means, with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of the information within an entity that maintains the information.

- **Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

- **Protected Health Information ("PHI")** is defined as Individually Identifiable Health Information that is transmitted or maintained in any form. PHI excludes education records and some other records described in the Family Educational Right and Privacy Act.

- **Individually Identifiable Health Information** is a subset of Health Information. It must be created or received by a Covered Entity or employer and relate to the past, present or future physical or mental health of an individual, including the provision of or Payment for care. This information must either identify the individual or provide a reasonable basis for such identification.

- **Health Information** is any information, whether oral or recorded, in any form or medium that is created or received by a Covered Entity, public health authority, employer, life insurer, school or university that relates to the past, present or future physical or mental health of an individual, including the provision of and Payment for care.

- **De-Identified Information** is Health Information that does not identify an individual and for which there is no reasonable basis to believe that information can be used to identify the individual. Information may be considered de-identified if (a) a properly qualified person determines that the risk is small and that the information by itself, or in combination with other information, is not individually identifiable, or (b) 18 identifiers specified in the Rule are removed. A Covered Entity can Use or Disclose PHI to create De-Identified Information or Disclose PHI to a Business Associate to do so. Although Covered Entities may establish codes or other means of re-identification, such means cannot be derived from or relate to individual information, and the means may not be Disclosed. Once De-Identified Information is re-identified, the Rule applies.

The Rule requires Disclosure of PHI in only two circumstances: (1) to an individual with respect to his or her own PHI, and (2) to the Secretary in connection with investigations and compliance audits.

The Rule permits the Use and Disclosure of PHI in the following circumstances:

- To an individual with respect to his or her own PHI,

- With a proper consent to carry out Treatment, Payment or Health Care Operations,

- Without consent for Treatment, Payment or Health Care Operations when the Rule provides that consent is not required, and consent has not been sought, except with respect to **Psychotherapy Notes**,[4]

- With a proper authorization, and

- In certain other special circumstances.

From this description of permitted Uses and Disclosures, it is evident that such Uses and Disclosures are connected with concepts of Treatment, Payment and Health Care Operations. These terms are defined as follows:

Treatment means the provision, coordination, or management of care and related services by a Health Care Provider. Treatment includes patient referrals and consultations. An **Indirect Treatment Relationship** means a relationship between an individual and a Health Care Provider in which the Health Care Provider delivers care to the individual based on the orders of another Health Care Provider. Typically, the Health Care Provider delivers

services or products, or it reports results associated with health care to another Health Care Provider. A **Direct Treatment Relationship** is any Treatment relationship which is not indirect.

Payment means activities undertaken by a Health Plan to obtain premiums or to determine coverage. It also includes activities by a Health Care Provider or Health Plan to obtain or provide reimbursement for services. Such activities include: determinations of eligibility for coverage, adjudication or subrogation of health benefit claims, risk adjusting based on enrollee health status and demographics, billing, claims management, collection activities, obtaining Payment under a contract of reinsurance (including stop-loss), health care data processing, review of services for medical necessity, appropriateness of care, justification of charges, utilization review (both concurrent and retrospective), and pre-certification or pre-authorization. Disclosure of certain limited information to consumer reporting agencies in relation to collection of premiums or reimbursement also constitutes Payment.

Health Care Operations means activities of a Covered Entity such as quality assessment, provider evaluation and training, underwriting, conducting or arranging for medical review, legal services, audits, business planning, business management and general administrative activities of the entity including customer service, resolution of internal grievances, due diligence in connection with a sale or transfer of assets, marketing or fundraising.

E. Minimum Necessary Standard

A Covered Entity's Use, Disclosure or request for PHI requires reasonable efforts to limit such PHI to the **Minimum Necessary** for the particular purpose. This standard does not apply to requests of a Health Care Provider for Treatment purposes. The standard also excludes Disclosures to an individual about his or her PHI, Disclosures made pursuant to certain authorizations or Disclosures made as Required by Law. The Minimum Necessary standard requires the Covered Entity to identify (1) the persons or classes of persons in its Workforce who need access to PHI to carry out their duties, (2) the categories of PHI for which access is needed, and (3) any appropriate conditions or limitations to access. The amount of PHI included in any Disclosure should be limited to the amount reasonably necessary to achieve the purpose of the Disclosure. If reasonable, a Covered Entity may rely on a requested Disclosure as consistent with Minimum Necessary standard when making Disclosures to public officials, when requested by another Covered Entity or Business Associate or when the information is requested for research purposes. A Covered Entity may not Use, Disclose or request an entire medical record except when specifically justified.

F. Verification

Prior to any Disclosure permitted by the Rule, a Covered Entity must verify the identity of the person requesting PHI and the basis for his or her authority, if unknown. Exceptions exist for facility directories, emergency circumstances, disaster relief and for those persons involved in the individual's care or with respect to Payment related to the individual's health care. A Covered Entity must obtain oral or written documentation, statements or representations concerning identity and authority from the person requesting the PHI under specified circumstances. Generally, the verification requirements of the Rule are met if the Covered Entity relies on the exercise of good faith professional judgment.

G. Consents

1. When Are Consents Required? The Rule generally requires a covered Health Care Provider to obtain consent prior to the Use or Disclosure of PHI for Treatment, Payment or Health Care Operations. Exceptions exist in specified circumstances (*e.g.*, if a covered Health Care Provider has an Indirect Treatment Relationship with the individual, or the PHI was created or received in the course of providing health care to an inmate). Health Plans may, but are not required to, obtain consent upon enrollment. A Covered Entity may condition Treatment or enrollment in a Health Plan on receipt of consent.

No consent is needed to Use or Disclose PHI for Treatment, Payment or Health Care Operations in emergency situations if (a) consent is sought expeditiously following Treatment and the basis for the failure to obtain consent is documented, (b) Treatment is Required by Law and consent is not obtained despite efforts to do so, or (c) substantial communication barriers exist and a covered Health Care Provider reasonably determines that consent is inferred. If no consent is obtained, the Covered Entity must document its efforts to obtain consent, including the reasons for the failure.

Except for permitted joint consents, a consent obtained by one Covered Entity does not apply to the Use or

Disclosure of PHI by another Covered Entity. Joint consents are permitted, however, for Covered Entities participating in an Organized Health Care Arrangement (*see* Section O below) as long as each of the Covered Entities is identified, the consent complies with the requirements in the Rule, and a Covered Entity that receives a revocation of consent informs the other Covered Entities of the revocation.

2. Form and Content of Consents. The Rule specifies that a consent must be in plain language and inform the individual that PHI may be Used and Disclosed to carry out Treatment, Payment or Health Care Operations. It must make reference to the Notice of Privacy Practices (*see* Section Q below) required by the Rule for more detailed information regarding Uses and Disclosures. Additionally, it must advise the individual of the right to review the Notice of Privacy Practices prior to signing the consent. If applicable, the consent must state that the Notice of Privacy Practices may change and how the revised Notice may be obtained. The consent also must advise individuals of the right to request that a Covered Entity restrict how PHI is Used or Disclosed to carry out Treatment, Payment or Health Care Operations, but the Covered Entity is not bound to the restrictions unless it agrees to it. Additionally, the consent must advise individuals of the right to revoke the consent in writing and that the revocation will be effective except to the extent a Covered Entity has acted in reliance on it. Finally, the consent must be signed and dated by the individual.

3. Specific Requirements for Using Consents. Consents must be distinct from, and not included in, the Notice of Privacy Practices (*see* Section Q below) required by the Rule. Consents may be combined with other consents as long as the consent required by the Rule is visually and organizationally separate from the others and is separately signed and dated. Consents may be revoked at any time absent action taken in reliance on the consent and must be in writing. The most restrictive consent controls. Covered Entities may seek clarification of multiple consents and must document and retain signed consents.

H. Authorizations

1. General Rule for Authorizations. Except as otherwise provided in the Rule, a Covered Entity may not Use or Disclose PHI without a valid authorization. Use of Psychotherapy Notes requires authorization except to carry out certain limited Treatment, Payment or Health Care Operations consistent with the consent requirements in the Rule. Once an authorization is received, the Use and Disclosure of PHI must be consistent with the authorization. A Covered Entity must document and retain signed authorizations. Authorizations may be revoked in writing at any time. Revocations are effective except to the extent that a Covered Entity has acted in reliance on the authorization or the authorization was obtained as a condition of obtaining insurance coverage and other law allows the insurer to Use the PHI to defend a contested claim.

2. Required Content of Authorizations. While authorizations may include other provisions consistent with the Rule, the authorization must be in plain language and include the following:

- Specific meaningful description of the information to be Used or Disclosed.
- Names or other specific identification of the person(s) authorized to make the requested Use or Disclosure.
- Names or other specific identification of person(s) to whom the Covered Entity may make the requested Use or Disclosure.
- Expiration date or event.
- Description of the individual's right to revoke the authorization in writing, how to revoke it and any exceptions to revocation.
- Statement indicating that information Used or Disclosed based on the authorization may be re-Disclosed by the recipient and would then no longer be protected by the Rule.
- Signature of the individual (or personal representative and the basis for the authority of the personal representative) and the date.

In addition to the foregoing requirements, the following must be included in authorizations sought by a Covered Entity for its own Uses and Disclosures:

- Description of each purpose of the Use or Disclosure.
- Statement permitting the individual to inspect or copy the PHI to be Used or Disclosed or to refuse to sign the authorization.

- Disclosure of any remuneration to be received by the Covered Entity from a third party based on the information being Disclosed pursuant to the authorization.

- Statement that the Covered Entity agrees not to impermissibly condition Treatment, Payment, enrollment in a Health Plan or benefit eligibility under a Health Plan upon receipt of the authorization.

- A copy of the authorization must be provided to the individual.

A Covered Entity may request authorization for Disclosure of PHI by another Covered Entity to the requesting entity for Treatment, Payment or Health Care Operations. For example, one hospital may seek an authorization from an individual for Disclosure by another hospital of that individual's PHI. The authorization must include the core elements described above plus certain additional provisions.

3. Limitations on Authorizations. A Covered Entity generally cannot condition Treatment or Payment, enrollment in a Health Plan or eligibility for benefits under a Health Plan on provision of an authorization except under the following circumstances:

- A Health Care Provider may condition research-related Treatment upon obtaining authorization.

- A Health Plan may condition enrollment on receipt of authorization of Disclosures for making eligibility or enrollment determinations or its underwriting and risk rating determinations.

- A Health Plan may condition Payment on authorization of Disclosures necessary to determine proper Payment.

- A Covered Entity may condition the provision of health care that is solely for the purpose of creating PHI for Disclosures to a third party on an authorization to Disclose PHI to that third party.

I. Uses of PHI Not Requiring Consent or Authorization, or Opportunity to Agree

Certain Uses and Disclosures of PHI do not require consent, authorization or an opportunity to agree. These Uses and Disclosures are:

- As Required by Law, or as needed to comply with special provisions concerning Disclosures about victims of abuse, neglect or domestic violence. **Required by Law** means mandated by law, not merely permitted or favored under the law.

- For specified public health activities (*e.g.*, disease prevention and control, vital statistics, public health investigations or interventions, reports of child abuse or neglect, FDA activities, product recalls, communicable disease control, and work-related illnesses).

- To a governmental entity about an individual who a Covered Entity reasonably believes is a victim of abuse, neglect or domestic violence. Generally, the Covered Entity must inform the individual promptly that the report has been or will be made.

- To a health oversight agency for authorized oversight activities that arise out of or are directly related to health care, benefits or services (*e.g.*, audits, investigations, inspections, and civil or criminal proceedings).

- In connection with judicial or administrative proceedings subject to various protections specified in the Rule. For example, Disclosure of PHI pursuant to a judicial order must be limited to the scope of the order.

- To a law enforcement official for law enforcement purposes under specified conditions (*e.g.*, as Required by Law to report certain types of wounds). Except as otherwise Required by Law, a Covered Entity may Disclose only certain specified PHI to aid in the identification or location of a suspect, witness or missing person. For example, Disclosure of DNA information, dental records, or typing, sampling or analysis of tissues or body fluids is not permitted; however, the Disclosure of blood type is permitted. Other permitted Disclosures to law enforcement officials arise in the context of crime victims, decedents, crimes on the premises of a Covered Entity, and reporting crime in emergency situations.

- To coroners and medical examiners and to funeral directors, even in anticipation of death.

- To organ procurement organizations to facilitate organ, eye or tissue donation and transplantation.

- For research, provided a specific waiver of the authorization otherwise required by the Rule has been approved by an Institutional Review Board (or other privacy board), is signed, and various other protections are in place.

- To avoid a serious threat to health or safety subject to specified limitations.

- For specialized government functions related to the military and veterans activities, national security purposes, protective services for the President of the United States and other authorized personnel. Medical suitability determinations in the context of correctional institutions and other law enforcement custodial situations and with respect to Covered Entities that are government programs providing public benefits also are permitted.

- As required to comply with worker's compensation or similar programs established by law.

J. Marketing and Fundraising

1. Marketing. A Covered Entity may not Use or Disclose PHI for marketing purposes without an authorization except when the marketing activity (a) occurs face to face with the individual, (b) concerns products or services of nominal value, or (c) the marketing communication concerns health-related products or services of the Covered Entity or a third party and identifies the Covered Entity as the party making the communication, Discloses whether the Covered Entity has or will receive remuneration for the communication and, except for broad generic type communications (*e.g.*, newsletters), instructs individuals how to opt out of receiving future communications. Covered Entities must make reasonable efforts to honor requests to opt out of receiving such communications. If marketing activities involve Disclosure of PHI to target individuals for various services or products based on their health status, the Covered Entity must first determine that the product or service may be beneficial to that individual, and the communication must explain why and how the product or service relates to that person.

2. Fundraising. A Covered Entity may Use or Disclose demographic information about an individual and dates of health care provided to the individual without an authorization to a Business Associate or an institutionally related foundation to raise funds for the Covered Entity's own benefit if its Notice of Privacy Practices includes that the entity may contact the individual for fundraising purposes. Fundraising materials sent to a person must include a description on how to opt out of receiving further fundraising materials, and the Covered Entity must make reasonable efforts to comply with such requests.

K. Uses and Disclosures Requiring Opportunity to Agree or Object

A Covered Entity may Use or Disclose PHI for certain purposes without the individual's consent or authorization provided that the individual is informed orally or in writing in advance of the intended Use or Disclosure. The individual must have the opportunity to agree to, prohibit or restrict some or all of such Uses or Disclosures.

1. Facility Directories and Clergy. Absent an objection, a hospital or other covered Health Providers may include in a facility directory the person's name, location in the facility, general condition, and religious affiliation. It also may make Disclosures of such PHI to clergy members and, except for religious affiliation, to other persons who ask for the individual by name.

2. Family Members. A Covered Entity also may make Disclosures of PHI (a) to family members, relatives, close personal friends or others named by the individual to the extent relevant to their involvement with the individual's care or Payment for care, or (b) to notify or help notify a family member, personal representative, or others of the individual's location, general condition or death. If the individual is present and able to make health care decisions, the individual has the right to agree or object to the Disclosure. If the individual is not present or exigent circumstances exist, a Covered Entity has latitude to exercise professional judgment regarding such Disclosures.

3. Disaster Relief. A Covered Entity may Use or Disclose PHI for disaster relief efforts to disaster relief organizations.

L. Individual Rights

The Rule provides individuals with various rights

regarding their PHI, including the right to (1) have access to their PHI, (2) amend their PHI, (3) receive an accounting of Disclosures of their PHI, (4) request certain restrictions in the Uses or Disclosures of their PHI, and (5) request that their PHI be provided to the individual on a confidential basis.

1. Access. Generally, the Rule grants individuals the right of access to inspect and obtain a copy of their PHI for as long as the PHI is maintained in a Designated Record Set. A **Designated Record Set** is a group of records maintained by or for a Covered Entity that consist of (a) the medical and billing records of an individual maintained by or for a covered Health Care Provider, (b) enrollment, Payment, claim adjudication records maintained by of for a Health Plan, and (c) is used in whole or in part by or for the Covered Entity to make decisions about the individual. Exceptions to access exist for Psychotherapy Notes, information gathered in reasonable anticipation of or use in a criminal, civil or administrative proceeding, PHI maintained by a Covered Entity subject to the Clinical Laboratories Improvements Act of 1988 ("CLIA") if applicable law precludes access or if the Covered Entity is exempt from CLIA.

A Covered Entity may require requests for access to be written, but must act on a request no later than 30 days after the request is received. If PHI is not maintained or accessible on-site, the Covered Entity must take action within 60 days of the request. Deadlines can be extended one time by 30 days, provided the individual requesting access is informed within the originally prescribed time frame and is advised when action on the request will be complete.

If granted, access must be timely and in the form or format requested if possible. A summary form of the record may be provided if the individual agrees in advance. A Covered Entity may impose reasonable fees for copies of PHI, summaries or explanations. If the Covered Entity does not maintain the PHI that is the subject of the request, it must advise the individual where to direct the request if known.

Denials of access must be timely and in writing. They must address the basis for the denial and the individual's rights, if any, to have the denial reviewed. The denial also must include a description of complaint procedures and a name or title of the contact person or office designated by the Covered Entity to receive complaints. PHI beyond the scope of the basis for denial must be provided.

Denial of access to PHI is permitted without subsequent review if (a) access is excepted under the Rule, (b) access is requested by an inmate and access would jeopardize the health, safety, security, custody or rehabilitation of the inmate or others, (c) during the course of research involving Treatment, provided such denial was agreed to when the individual consented to participate and access is reinstated upon completion of the research, (d) the federal Privacy Act applies and permits denial, or (e) the PHI was received from a source with a promise of confidentiality and access is likely to breach that confidentiality.

Denial of access is subject to review in circumstances where (a) a licensed health care professional reasonably believes that access will endanger the life or safety of the individual or others, (b) the PHI refers to others and the health care professional determines that access is likely to substantially harm the other person, or (c) the request is from a personal representative and the licensed health care professional reasonably believes that access will harm the individual or others. Reviews of such denials must be by a licensed health care professional designated by the Covered Entity who was not involved in the decision to deny access.

2. Amendment. An individual has the right to request that a Covered Entity amend his or her PHI or a record about the individual in a Designated Record Set. Covered Entities must designate persons or offices responsible for handling amendment requests.

Covered Entities may require requests for amendments to be written and to include a reason to support the requested amendment if it notifies individuals in advance of the requirement. Covered Entities must act within 60 days of receipt of the request. A single 30-day extension is authorized as long as the individual receives a written statement regarding the delay and a date by which action on the request will be complete.

A request for amendment can be denied if the Covered Entity did not create the PHI, the PHI is not part of the Designated Record Set, would not be available for access under the Rule or is accurate and complete. Denials must be written, explain the basis for the denial and describe the individual's right to submit and file a written statement disagreeing with the denial. Individuals who do not submit a statement of disagreement can request that the request for amendment and denial be included in any future Disclosures of PHI. Denials must include a description of how to complain to the Covered Entity and to whom. A Covered

Entity can submit a rebuttal statement to a statement of disagreement. All of these records must be retained and appended or linked to the individual's record of PHI. If a statement of disagreement is filed, it and all subsequent responses must be included or summarized with future Disclosures of PHI. Covered Entities that receive notice of amendments must amend the PHI in their respective Designated Record Sets.

Accepted amendments must be appended or linked to the appropriate records, and the individual must be informed of the amendment. Covered Entities must obtain the individual's consent to and make reasonable efforts to inform others of the amendment (*e.g.*, Business Associates and others known to have received PHI).

3. Accounting. An individual has a right to receive an accounting of Disclosures of PHI made by a Covered Entity for up to six (6) years prior to the date on which the accounting is requested. The request also may seek an accounting of Disclosures to or by any Business Associates of the Covered Entity. For each Disclosure, the accounting must include: (a) the date of Disclosure, (b) the name of entity or person who received PHI and address, if known, (c) a brief description of PHI Disclosed, and (d) a brief statement of the basis for the Disclosure. Exceptions exist to the right to an accounting for Disclosures (a) made to carry out Treatment, Payment and Health Care Operations, (b) to individuals, (c) for facility directories, persons involved in the individual's care or certain other specified Disclosures, (d) for national security or intelligence purposes, (e) to correctional institutions, or (f) that occurred prior to the compliance date of the Rule.

Requests for an accounting must be acted upon within 60 days following receipt of the request. One 30-day extension is authorized if the Covered Entity provides the individual with a written statement regarding the basis for the delay and the date by which it will provide the accounting. The first accounting in any twelve (12) month period must be free. Reasonable charges may be imposed thereafter as long as the individual is notified in advance and has an opportunity to modify his or her request.

Covered Entities may require requests for an accounting to be written and must document and retain information subject to accountings, written accountings provided to individuals, and titles and persons or offices responsible for receiving and processing accountings.

4. Restrictions. The Rule provides individuals with the right to request that a Covered Entity restrict the Use and Disclosure of the individual's PHI; however, the Covered Entity need not agree to the request. If it agrees to the request, the Covered Entity generally must document and abide by the restrictions. The Rule specifies procedures for terminating restrictions.

5. Confidentiality Requests. A Covered Entity must permit individuals to request that they receive communications of PHI by alternate means or at alternate locations. A Covered Entity may require these requests to be written and must accommodate all reasonable requests; provided, however, a Health Plan need comply only if the individual indicates that he or she will be harmed by Disclosures made in the typical manner.

M. Business Associates and Business Associate Agreements

1. Rules for Business Associates. A Covered Entity may Disclose PHI to a Business Associate and permit the Business Associate to create or receive PHI on its behalf if the Business Associate provides satisfactory written assurances that it will properly safeguard the information. This requirement also applies to a Covered Entity acting as a Business Associate to another Covered Entity.

A **Business Associate** is any person or entity who performs or assists a Covered Entity with a function that involves the Use or Disclosure of Individually Identifiable Health Information. These functions include claims processing, data analysis, utilization review, quality assurance, Data Aggregation, billing and practice management. A Business Associate also may include persons or entities who provide legal, actuarial, accounting, consulting, administrative, managerial, accreditation or financial services for a Covered Entity to the extent that PHI is Used or Disclosed. A Business Associate does not include the **Workforce** of a Covered Entity. Workforce is defined broadly to include persons under the direct control of the Covered Entity, irrespective of whether they are paid by the Covered Entity.

A Business Associate provides a Covered Entity with satisfactory assurances that it will properly safeguard PHI by signing a Business Associate agreement. A Business Associate agreement is not required for Disclosures by (a) a Covered Entity to a Health Care Provider regarding Treatment of the individual, (b) a self-funded group Health

Plan, or an HMO or health insurance issuer providing benefits under a group Health Plan to the plan sponsor of the group Health Plan so long as certain requirements in the Rule have been met, and (c) a Health Plan that is a government program providing public benefits as long as certain plan functions are handled by entities other than the entity administering the plan.

2. Requirements for Business Associate Agreements. A Business Associate agreement must establish permitted and required Uses and Disclosures of PHI. A Business Associate must not Use or Disclose PHI beyond the scope permitted by its agreement or as Required by Law. Additionally, a Business Associate generally cannot authorize Uses or Disclosures beyond those allowed for the Covered Entity on whose behalf it is performing services. The Rule specifies required and permitted provisions for Business Associate agreements.

In a Business Associate agreement, a Business Associate must agree to:

- Use appropriate safeguards to prevent Uses or Disclosures of PHI beyond the scope permitted by the agreement.
- Report to the Covered Entity any Uses or Disclosures beyond the scope of the agreement of which it becomes aware.
- Ensure that its agents, including subcontractors, to whom it provides PHI received from, created or received on behalf of a Covered Entity agree to be bound to the same terms as the Business Associate regarding confidentiality.
- Make PHI available to individuals who have rights of access, to make amendments and for purposes of accountings for Disclosures.
- Make available its practices, books and records regarding the Use, Disclosure, creation or receipt of PHI to the Secretary to help determine a Covered Entity's compliance with the Rule.
- Upon termination of the Business Associate agreement, return or destroy all PHI that it has, if feasible. It must retain no copies and must provide for limitations on Use and Disclosure when return or destruction of PHI is not feasible.
- Permit termination of the Business Associate agreement if the Covered Entity determines that the Business Associate has violated a material term of the agreement.

Permitted provisions in a Business Associate agreement include authorizing the Use of PHI (a) for proper management and administration of the Business Associate, or (b) to carry out its legal responsibilities, so long as Disclosure is Required by Law or the Business Associate obtains reasonable assurances from the person to whom it Discloses PHI that the PHI will be maintained in confidence and Used or further Disclosed only as Required by Law or for specified purposes, and the person will notify the Business Associate of any confidentiality breaches of which it becomes aware. Additionally, a Business Associate, such as a state hospital association, may provide Data Aggregation services relating to Health Care Operations of the Covered Entity. **Data Aggregation** means the combining of Protected Health Information by a Business Associate with the Protected Health Information received by the Business Associate from another Covered Entity to permit data analyses that relate to the Health Care Operations of the respective Covered Entities.

A Covered Entity violates the Rule if it knew of a pattern or practice of the Business Associate that materially breached its obligations under the Business Associate agreement or arrangement. An exception exists if the Covered Entity took reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminated the agreement if feasible or reported the problem to the Secretary if termination was not feasible.

N. Hybrid and Affiliated Entities

If a Covered Entity is a Hybrid Entity, the Rule generally applies only to the health care component of the entity, and the Covered Entity must ensure compliance with the Rule with respect to that component. A **Hybrid Entity** is a single legal entity that is a Covered Entity and whose covered functions are not its primary functions. For example, a manufacturing facility that has an on-site health clinic is a Hybrid Entity. Only the health clinic component is a Covered Entity. Thus, the health care component may not Disclose PHI to another component of the Covered Entity, and a person with duties in each component must segregate his or her Use and Disclosure of PHI accordingly. Additionally, legally separate Covered Entities may designate themselves as a single affiliated Covered Entity if all of the Covered

Entities are under Common Ownership or Control. **Common Ownership** means possessing an ownership or equity interest of 5% or more; **Common Control** means having the power, directly or indirectly, to influence or direct the actions or policies of another entity.

O. Organized Health Care Arrangement

An **Organized Health Care Arrangement** is defined as one of five types of arrangements, including a clinically integrated care setting in which individuals typically receive health care from more than one provider, a system in which more than one Covered Entity participates and shares specific functions such as Payment activities, and various combinations that include a group Health Plan and plan sponsors or participants. Organized Health Care Arrangements may:

- Provide for joint consents as long as each of the Covered Entities is identified, the consent complies with the requirements in the Rule and a Covered Entity that receives a revocation informs the other Covered Entities of the revocation.

- Provide a joint Notice of Privacy Practices as long as all Covered Entities participating in the arrangement agree to abide by the terms of the Notice, the Notice meets the requirements set forth in Section Q below, describes with reasonable specificity the Covered Entities and the service delivery sites or classes of service delivery sites to which the joint Notice applies. The joint Notice must state, if applicable, that the Covered Entities participating in the Organized Health Care Arrangement will share PHI with each other as necessary to carry out Treatment, Payment or Health Care Operations and that the participating Covered Entities must each provide the joint Notice to individuals upon the first delivery of service.

P. Employers and Group Health Plans

While employer-sponsored medical benefit plans are Covered Entities subject to the Rule, the employers that sponsor those plans are not. Under ERISA, the benefit plan and the employer are separate legal entities, and the Rule is premised on this legal distinction, even for church plans and government plans not regulated under ERISA. While employers generally will be responsible for providing eligibility and enrollment data to their medical plans, the Rule considers the employer as doing so on behalf of the plan's participants and beneficiaries, and not on behalf of the plan itself. This means that, generally, employers will not be considered Business Associates of their own plans and will not generally be required to sign Business Associate agreements (unless the employer actually performs administrative services on behalf of the plan beyond enrollment and disenrollment).

Nevertheless, employers who sponsor benefit plans may not ignore the Rule. The Rule recognizes that employers who are plan sponsors may gain access to PHI by virtue of their plan sponsorship and that certain protections, therefore, must be in place. Specifically, the preamble to the Rule emphasizes the employer's obligation under the American with Disabilities Act ("ADA") to keep medical information obtained about employees confidential. Building on the employer's obligations under the ADA, the Rule creates specific obligations and limitations regarding benefit plan administration and the receipt of PHI by the employer from its group Health Plan or an insurer or HMO providing benefits under that plan.

To permit the Disclosure of PHI to a plan sponsor by a group Health Plan or by an insurer or HMO that provides benefits with respect to that plan:

1. The plan sponsor must certify to the plan, insurer or HMO that the plan sponsor agrees to:

- Prohibit the Use or Disclosure of PHI other than as permitted by the plan document or Required by Law.

- Ensure that any agents of subcontractors to whom it provides PHI will agree to the same restrictions.

- Preclude the Use or Disclosure of any PHI in employment-related decisions.

- Report to the group Health Plan any impermissible Use or Disclosure of which the employer becomes aware.

- Make available to an individual access to his or her own PHI, upon request, pursuant to the Rule.

- Allow individuals to amend their PHI as provided in the Rule.

- Make available to plan participants an accounting

of the plan's Disclosures of PHI as provided in the Rule.

- Make its books and records available to the Secretary to determine compliance.

- If feasible, return all PHI received from its group Health Plan when no longer needed.

- Maintain in place the protective firewalls required to be set forth in the plan documents.

2. The plan document must be amended to:

- Identify the permitted and required Uses and Disclosures of PHI by the plan sponsor.

- Require the plan sponsor certify that it has agreed to the conditions set forth in point 1 above.

- Identify those employees or classes of employees to whom PHI may be Disclosed for purposes of Payment and Health Care Operations in the ordinary course of plan operations.[5]

- Restrict the plan administrative functions performed by the plan sponsor to those persons identified in the plan document.

- Set forth an effective mechanism for resolving any instances of noncompliance by these designated persons.

3. The group Health Plan may:

- Disclose PHI of plan participants and beneficiaries to the plan sponsor to perform plan administrative functions, but only if consistent with the above limitations. (For example, the employer's Health Plan may Disclose PHI only to those persons identified in the plan document.)

- Not permit an insurer or HMO to Disclose the PHI of plan participants and beneficiaries unless consistent with the above limitations.

- Not Disclose the PHI of plan participants and beneficiaries to the plan sponsor for employment-related decisions or in connection with any other benefit or employee benefit plan of the sponsor.

- Provide Summary Health Information to the plan sponsor for the purposes of obtaining premium bids on health insurance or amending or terminating the plan. **Summary Health Information** is information that may be individually identified, but which summarizes claims history, claims expenses or type of claims experienced by individuals who have received plan benefits and from which the 18 identifying factors listed in the Rule have been removed.

- Condition enrollment or entitlement to benefits upon an individual's consent to the Use or Disclosure of PHI for purposes of Payment and Health Care Operations.

4. The group Health Plan must:

- Provide the Notice of Privacy Practices to its participants and beneficiaries if it is self-funded, or if insured and it creates or receives PHI in addition to Summary Health Information and enrollment and/or disenrollment data. (For insured group Health Plans which do not create or receive PHI in addition to Summary Health Information, the Notice must be provided by the insurer or HMO).

- Satisfy the Notice requirements for Covered Entities generally (*see* Section Q below), but group Health Plans must also state that they may Disclose PHI to the plan sponsor.

- Distribute the Notice to plan participants and beneficiaries by April 14, 2003 (or April 14, 2004 for small Health Plans), and after that date, upon enrollment and within 60 days of any material revision to the Notice. Not less frequently than once every three (3) years, individuals covered by the plan must be informed about the availability of the Notice and how to obtain a copy.

- Comply with the all the administrative requirements of the Rule (*see* Section R below), except that group Health Plans that are fully insured and that do not create or receive PHI in addition to Summary Health Information do not have to comply with the requirements for: (a) naming a privacy officer, (b) training personnel in privacy and security compliance, (c) having in place technical, administrative and physical safeguards, (d) having

a complaint procedure in place with respect to privacy and security issues, (e) having policies for sanctioning employees for noncompliance, (f) having in place documented policies and procedures designed to comply with the regulations, or (g) retaining documentation with respect to the policies and procedures for six (6) years.

- Allow participants or beneficiaries to have communications from the plan be treated as confidential and sent to a specified address or sent only in certain formats, but only if the individual certifies to the plan that not doing so will bring him or her harm.

Q. Notice of Privacy Practices

1. General Rule. Covered Entities must provide individuals, other than inmates, with its Notice of Privacy Practices (the "**Notice**"). The Notice must include a description of the Uses and Disclosures of PHI that may be made by the Covered Entity, and of the individual's rights and the Covered Entity's legal duties regarding the Use and Disclosure of PHI. The Covered Entity's actual Use and Disclosure practices must be consistent with the policies and practices set forth in the Covered Entity's Notice. The Notice of Health Plans also must include a statement regarding Disclosures to plan sponsors.

A Covered Entity must promptly revise and distribute its Notice when it materially changes its Uses or Disclosures, its legal duties, or other privacy practices reflected in the Notice. Generally, changes to the Notice take effect when the revised Notice is printed or published.

2. Distribution of Notice. The Notice must be available to anyone on request and must be provided:

- By Health Plans by April 14, 2003 (April 14, 2004 for small Health Plans) to persons covered by the plan, on enrollment to new enrollees, and within 60 days of material revisions to the Notice to persons then covered by the plan. At least once every three (3) years, the plan must notify persons covered by the plan of the availability of the Notice and how to obtain it. A Notice provided under an insurance policy is sufficient if provided to the named insured.

- By Health Care Providers with Direct Treatment Relationships with individuals no later than the first date of service delivery after April 14, 2003. The Notice must be available at the physical delivery sites for individuals to take with them. The Notice also must be posted in a clear and prominent location. Revised Notices must be available upon request on or after the compliance date and must be posted.

- Covered Entities with websites must post their Notice on its website prominently. Such Notices must be available electronically and by paper copy.

3. Required Contents of Notice. The Notice must be in plain English and must prominently display the following words: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

The Notice also must meet the following requirements:

- Include an effective date (no earlier than date on which printed or published).

- Provide the name or title and phone number of the person to contact for further information.

- Describe in sufficient detail the types of Uses and Disclosures permitted by the Covered Entity for each of Treatment, Payment and Health Care Operations. At least one example for each type of Use must be included.

- Describe in sufficient detail each other purpose for which the Covered Entity is permitted or required to Use or Disclose PHI without the person's written consent or authorization.

- If a Use or Disclosure for the above purposes is prohibited or materially limited by other applicable law, describe any Uses or Disclosures consistent with the More Stringent law.

- Include a statement that other Uses and Disclosures will only be made with the individual's written authorization, which authorization may be revoked.

- Explain the individual's right to request restrictions, confidential communications, inspect and copy his

or her PHI, amendment of PHI, accountings of PHI Disclosures, as well as to receive a paper copy of any electronic Notice.

- Include a statement that the Covered Entity is required to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI.

- Include a statement that the Covered Entity is required to abide by the terms of the Notice currently in effect.

- Provide a disclaimer that the Covered Entity has reserved the right to change its privacy practices effective for all PHI maintained and a description of how the individual can obtain a revised Notice.

- Include a statement that the individual may complain to the Covered Entity and to the Secretary if he or she believes his or her privacy rights have been violated, a brief description of how to file a complaint with the Covered Entity, and a Disclosure that the individual will not be retaliated against for the filing of a complaint.

Separate statements are required in the Notice if the Covered Entity intends to (a) contact the individual for appointment reminders, Treatment alternative information, or other health related benefits or services, (b) contact the individual for fundraising for the Covered Entity, or (c) if the Covered Entity is a Health Plan, to Disclose PHI to the sponsor of a group Health Plan. Finally, a number of optional provisions may included in the Notice (*e.g.*, a description of more limited Uses or Disclosures of a Covered Entity that are otherwise permitted by the Rule).

R. <u>Administrative Requirements</u>

Various administrative requirements in the Rule state that Covered Entities must:

- Designate and document the designation of a privacy official to develop and implement PHI policies and procedures. They also must designate and document the designation of a contact person or office responsible for receiving complaints and responding to questions regarding required Notices.

- Train and document training of all members of its Workforce on policies and procedures regarding PHI by April 14, 2003 (except for small Health Plans). Training also must be provided within a reasonable time after new members begin work and within a reasonable time after any material changes are made to policies and procedures.

- Have in place appropriate administrative, technical and physical safeguards to protect privacy of PHI.

- Institute and maintain a process for individuals to make complaints regarding the Covered Entity's policies and procedures and compliance with the Rule. All complaints and their disposition must be documented.

- Apply and document sanctions against workers who violate privacy policies and the Rule.

- Mitigate harmful effects of violations of the Rule by the Covered Entity or its Business Associates.

- Not intimidate, threaten, discriminate or take retaliatory actions against anyone exercising their rights under the Rule. For example, a Covered Entity may not condition Treatment, Payment or the provision of benefits on a person's agreement to waive his or her rights to file complaints.

- Institute and document policies and procedures to comply with the Rule and other laws taking into account the entity's size and PHI-related activities. Provisions for changing policies are addressed in the Rule.

- Retain documentation for six (6) years from date of creation or date last in effect.

---

[1] The topics which received the most comments and may be modified are: (a) requirements for obtaining general consent at the initial point of treatment or enrollment in Health Plans, (b) extension of the Rule to oral communications (though distinctions might need to be made between direct oral communications and electronic oral communications, *e.g.*, cell phone, voicemail, teleconferencing and Internet voice streaming), and (c) access by parents to the PHI of their minor children.

[2] The text of the Rule and explanatory comments of HHS may be found at <u>http://aspe.hhs.gov</u> under the subheading titled, "Administrative Simplification in the Health Care Industry (HIPAA)."

[3] Michigan has numerous laws governing the use and disclosure of PHI. In addition, the Michigan legislature (as well as the other 49 state legislatures) may introduce a plethora of privacy legislation. For example, on February 1, 2001, the Michigan Attorney General issued a press release announcing the development of model legislation intended to protect patient health care information in Michigan. If passed, this legislation will preclude federal preemption to the extent it is more stringent than the Rule or otherwise qualifies for one of the exceptions described in this Section. To date, the model legislation has not been enacted.

[4] **Psychotherapy Notes** are notes recorded in any medium by a Health Care Provider who is a mental health professional that document or analyze the contents of conversations during a counseling session and that are separate from the rest of the individual's medical records. Psychotherapy Notes exclude medication, prescription, monitoring, counseling sessions start and stop times, modalities and frequencies of Treatment furnished, results of clinical tests, and any summary of the diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date of the patient. While Psychotherapy Notes receive special treatment under the Rule, the definition limits this treatment to specific documents of limited scope.

[5] The Rule is clear that Health Plans and Health Care Clearinghouses do not engage in Treatment. Treatment activities are undertaken only by Health Care Providers.

Index of Defined Terms

Honigman Miller Schwartz and Cohn is a general practice law firm headquartered in Detroit, with additional offices in Bingham Farms and Lansing, Michigan. Honigman Miller's staff of more than 175 attorneys and more than 300 support personnel serves thousands of clients regionally, nationally and internationally.

Our health care department includes the fourteen attorneys listed below who practice health care law on a full-time or substantially full-time basis, and a number of other attorneys who practice health care law part-time.

William M. Cassetta
Gerald M. Griffith
William O. Hochkammer
Carey F. Kalmowitz
Lynn A. Kriser
Patrick LePine
Stuart M. Lockman
David Pettinari
Julie E. Robertson
Linda S. Ross
Chris Rossman
Valerie S. Rup
Hideaki Sano
Margaret A. Shannon

Our employee benefits department includes the six attorneys listed below who practice employee benefits law on a full-time basis.

Nicole Bogard
Michael J. Friedman
Mary Jo Larson
Rebecca L. Sczepanski
Sherill Siebert
Lisa B. Zimmer

For further information regarding any of the matters discussed in this newsletter, or a brochure that more specifically describes our practices in health care law or employee benefits law, please feel free to contact any of the attorneys listed above by calling our Detroit office at (313) 465-7000, our Bingham Farms office at (248) 566-8300 or our Lansing office at (517) 484-8282.

Honigman Miller Schwartz and Cohn's HIPAA Law Focus is intended to provide information but not legal advice regarding any particular situation. Any reader requiring legal advice regarding a specific situation should contact an attorney. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about our qualifications and experience.

Honigman Miller Schwartz and Cohn also publishes news and client letters concerning antitrust, employee benefits, employment, environmental and tax matters. If you would like further information regarding these publications, please contact Lee Ann Jones at (313) 465-7224, ljones@honigman.com or visit the Honigman Miller Schwartz and Cohn web site at www.honigman.com.