HIPAA Standards for Privacy of Individually Identifiable Health Information

Richard Stokes

Municipal Technical Advisory Service, Richard.Stokes@tennessee.edu

Follow this and additional works at: http://trace.tennessee.edu/utk_mtastech

Part of the Public Administration Commons

The MTAS publications provided on this website are archival documents intended for informational purposes only and should not be considered as authoritative. The content contained in these publications may be outdated, and the laws referenced therein may have changed or may not be applicable to your city or circumstances.

For current information, please visit the MTAS website at: mtas.tennessee.edu.

Recommended Citation

http://trace.tennessee.edu/utk_mtastech/88
Overview

On August 21, 1996, President Clinton signed into law the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The act amended the Public Health Service Act (PHS Act), the Employee Retirement Income Security Act of 1974 (ERISA), and the Internal Revenue Code of 1986 to provide for the portability and continuity of health insurance coverage. On April 14, 2001, the Department of Health and Human Services issued modifications to HIPAA rules (45 CFR Part 160 and 164) by establishing standards, requirements and implementation specifications to protect the confidentiality of health information.

The new rules create a national standard to protect individuals’ medical records and other personal health information by:
1. Giving patients more control over their health information;
2. Setting boundaries on the use and release of health records;
3. Establishing appropriate safeguards for health care providers and others that protect the privacy of health information;
4. Holding violators accountable with civil and criminal penalties that can be imposed if they violate patients’ privacy rights; and
5. Striking a balance when public responsibility requires disclosure of some forms of data (for example, to protect public health).

According to the standards (45 CFR 164.530), administratively covered entities must:
1. Designate and document a privacy official who is responsible for the development and implementation of the entity’s policies and procedures;
2. Designate and document a contact person or office who is responsible for receiving complaints under the rules and who is able to provide further information about matters covered by the notice requirements;
3. Train all members of its workforce on policies and procedures with respect to protected health information (PHI) as necessary and appropriate for such members carry out their functions;

4. Provide training to each member of its workforce by no later than the compliance date and thereafter to new members of the workforce within a reasonable time after the person joins the staff and to each member of the workforce whose functions are affected by a change in the policies or procedures;

5. Document that the training has been provided;

6. Have in place appropriate administrative, technical and physical safeguards to protect the privacy of PHI (i.e., safeguard information from any intentional or unintentional use or disclosure);

7. Provide a process for individuals to make complaints concerning the covered entity’s policies and procedures;

8. Document all complaints received and their disposition;

9. Have and apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures;

10. Document all sanctions that are applied;

11. Mitigate any harmful effect of a use or disclosure in violation of the policies and procedures that is known to the covered entity;

12. Refrain from intimidating, threatening, coercing, discriminating or retaliating against individuals for the exercise of any rights under the act, including:
   a. Filing a complaint;
   b. Testifying;
   c. Assisting or participating in an investigation, compliance review, proceedings or hearing;
   d. Opposing any act or practice made unlawful by this act, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI.

Covered Entities

Entities covered under the new rules are health plans, health care clearinghouses, and health care providers who transmit health information in electronic format, such as electronic billing and fund transfers (45 CFR 160.102(a)). Most health plans and health care providers must comply by April 14, 2003. Small health plans (those with fewer than 50 participants) have until April 14, 2004, to come into compliance (45 CFR 164.534(b)). Where Tennessee state law provides stronger privacy protection, it will prevail over the new federal privacy standard.

The rules (45 CFR 160.103) define a “health plan” as an individual or group plan that provides or pays the cost of medical care. Health plans include any combination of the following:

1. A group health plan;
2. A health insurance issuer;
3. An HMO;
4. Part A or part B of the Medicare program;
5. The Medicaid program;
6. The issuer of a Medicare supplemental policy;
7. An issuer of a long term care policy;
8. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
9. The health care program for active military personnel;
10. The veterans health care program;
11. The Civilian Health and Medical Program of the Uniformed Services;
12. The Indian Health Services program;
13. The Federal Employees Health Benefit Program;
14. An approved state child health plan;
15. The Medicare + Choice program;
16. A high risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals; and
17. Any other individual or group plan or combination of individual or group plans that provides or pays for the cost of medical care.
A **“group health plan”** is defined by the rules as an employer welfare benefit plan, including insured and self-insured plans, that provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement or otherwise that:

1. Has 50 or more participants; or
2. Is administered by an entity other than the employer that established and maintains the plan.

Excluded from the definition of a group health plan are any policies, plans or programs that provide or pay for the cost of excepted benefits. Excepted benefits, according to the Public Health Services Act (42 USC 300gg-91(a)(2)), include:

1. Benefits not subject to the requirements:
   a. Coverage only for accident or disability income insurance or any combination thereof;
   b. Coverage issued as a supplement to liability insurance;
   c. Liability insurance, including general liability insurance and automobile liability insurance;
   d. Workers’ compensation or similar insurance;
   e. Automobile medical payment insurance;
   f. Credit-only insurance;
   g. Coverage for on-site medical clinics;
   h. Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

2. Benefits not subject to the requirements if offered separately, which include:
   a. Limited scope dental or vision benefits;
   b. Benefits for long-term care, nursing home care, home health care, community-based care, or any combination thereof;
   c. Such other similar, limited benefits as are specified in regulations.

3. Benefits not subject to the requirements if offered as independent, non-coordinated benefits, which include:
   a. Coverage for only a specified disease or illness;
   b. Hospital indemnity or other fixed indemnity insurance.

4. Benefits not subject to the requirements if offered as separate insurance policy.

The rules define a **“health care clearinghouse”** as a public or private entity, including a billing service, repricing company, community health management information system or community health information system, or “value added” networks and switches that either process or facilitate the processing of health information received from another entity or that process or facilitate the processing of health information for the receiving entity.

A **“health care provider”** is defined by the Public Health Services Act (42 USC 1395x(u)) as a provider of medical or health services. The definition also includes any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health care is the care, services, or supplies related to the health of an individual. It includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, as well as counseling services, assessment or procedures with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body. Health care also includes the sale and dispensing of a drug, device, equipment, or other items in accordance with a prescription. In local governments, emergency medical technicians and occupational nurses might fall under this category.

Health information is information that is created or received by a health care provider, health plan, employee, or health care clearinghouse in electronic, written, oral or any other form. It generally relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care.

A health care transaction is the transmission of information between two parties to carry out financial or administrative activities related to health care. It may include the following types of information transmissions:

1. Health care claims or equivalent encounter information;
2. Health care payment and remittance advice;
3. Coordination of benefits;
4. Health care claim status;
5. Enrollment and disenrollment in a health plan;
6. Eligibility for a health plan;
7. Health plan premium payments;
8. Referral certification and authorization;
9. First report of injury;
10. Health claim attachments;
11. Other transactions that the Secretary of Health and Human Services may provide.

Standards of Privacy

The standards (45 CFR 164.502(a)(1)) provide that a covered entity may use or disclose PHI:
1. To the individual;
2. With a consent to carry out treatment, payment or health care operations;
3. Without consent if there exists an indirect treatment relationship with the individual or the provider who created or received the PHI;
4. Without prior consent in emergency treatment situations (if required by law to treat the individual or if communication barriers prevent clear consent);
5. With and in compliance with an authorization;
6. With the agreement of the individual;
7. When required by law or for public health activities – situations involving victims of abuse, neglect or domestic violence; for health oversight activities; for judicial and administrative proceedings; for law enforcement purposes; for decedents; for cadaver organ, eye or tissue donation purposes; for research purposes; to avert a serious threat to health or safety; for specialized government functions; and for workers’ compensation.

A covered entity is required to disclose PHI (45 CFR 164.502(a)(2)) to an individual when requested by the individual and when required by the Secretary of Health and Human Services. An individual has a right to inspect and obtain a copy of PHI about him or herself for as long as the PHI is maintained (except for psychotherapy notes; information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding; and PHI maintained by a covered entity that is subject to the Clinical Laboratory Improvement Act of 1988).

The covered entity may require the individual to make any request for access in writing (45 CFR 164.524(b)), and the covered entity must act on the request for access no later than 30 days after receipt of such request. The covered entity must inform the individual of whether the request has been accepted or denied. If the covered entity grants access to the PHI, it must be done in a timely manner. If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, a reasonable, cost-based fee may be imposed, provided the fee includes only the cost of copying (including the cost of supplies for and labor of copying), postage (when the request is for the information to be mailed), and preparing an explanation or summary of the PHI.

A covered entity may deny an individual access to PHI without providing the individual an opportunity for review (45 CFR 164.524(a)(1-4)) if:
1. The protected information is excepted from the right of access (above);
2. A covered entity is a correctional institution or covered health care provider acting under the direction of the correctional institution if releasing a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate. “Correctional institution” means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense (45 CFR 164.501);
3. An individual’s access to PHI (created or obtained by a covered health care provider in the course of research that includes treatment) is suspended if the individual has agreed to the denial of access and the health care provider has informed the individual that the right of access will be reinstated upon completion of the research;
4. An individual’s access to PHI is subject to the Privacy Act;
5. The PHI was obtained from someone other than a health care provider under a promise of confidentiality.

A covered entity may deny an individual access, provided the individual is given a right to have such denials reviewed (45 CFR 164.524(a)(3)) if:
1. A licensed health care professional has determined that access is reasonably likely to endanger the life or physical safety of the individual or another person;
2. The PHI makes reference to another person, and a licensed health care professional has determined that the access is reasonably likely to cause substantial harm to that other person;
3. The request for access is made by the individual’s personal representative, and a licensed health care professional has determined that providing access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If the covered entity denies access to PHI, it must:
1. Give the individual access to any other PHI requested, after excluding the PHI the covered entity has grounds to deny;
2. Provide a timely, written denial to the individual containing the basis for the denial, a statement of the individual’s review rights, including a description of how the individual may exercise such review rights, and a description of how the individual may complain to the covered entity or the secretary. (45 CFR 164.524(b))

A covered entity must disclose PHI when required by the Secretary of Health and Human Services to investigate or determine the covered entity’s compliance with the law. Such investigation may include a review of the pertinent policies, procedures, or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance (45 CFR 160.306(c)).

A covered health care provider must obtain the individual’s consent prior to using or disclosing PHI to carry out treatment, payment, or health care operations (45 CFR 164.506(a)(1)). The consent must be in plain language and:
1. Inform the individual that PHI may be used and disclosed to carry out treatment, payment, or health care operations;
2. Refer the individual to the notice requirement for a more complete description of such uses and disclosures, and state that the individual has the right to review the notice prior to signing the consent;
3. State that the terms of its notice may be changed, and describe how the individual may obtain a revised notice;
4. State that the individual has the right to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment, or health care operations;
5. State that the covered entity is not required to agree to requested restrictions; and
6. If the covered entity agrees to a requested restriction, state that the restriction is binding on the covered entity;
7. State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action; and
8. Be signed by the individual and dated.

A covered health care provider may condition treatment on the individual providing consent. A health plan may condition enrollment in the health plan on the individual providing a consent sought in conjunction with such enrollment. A covered entity must document and retain any signed consent. A consent, however, may not be combined into a single document with the notice required under 45 CFR 164.520. Additionally, an individual may revoke a consent at any time, except to the extent that the covered entity has taken action in reliance upon the consent. Such revocation must be in writing.

A health care provider may use or disclose PHI without a consent when the provider has a direct treatment relationship with the individual or when the provider created or received the information in the course of providing care to inmates (45 CFR 164.506(a)(2)). The covered health care provider must document all attempts to obtain consent and the reason why consent was not obtained (45 CFR 164.506(a)(3)(ii)). A covered entity
may use or disclose PHI without prior consent in order to carry out treatment, payment or health care operations:
1. In an emergency treatment situation;
2. If required by law but when unable to obtain consent; or
3. If unable to obtain consent because of communication barriers.

A covered entity may not disclose PHI without a valid authorization and must provide the individual with a copy of the signed authorization (45 CFR 164.508(c)). The authorization must be written in plain language and must contain at least the following elements:
1. A description of the information to be used or disclosed that identifies such information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure;
4. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
5. A statement of the individual’s right to revoke the authorization in writing and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
6. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;
7. Signature of the individual and date;
8. If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual.

Additionally, authorizations requested by a covered entity for its own uses and disclosures must be copied to the individual (45 CFR 164.508(d)) and include the following elements:
1. A statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual providing authorization for the requested use or disclosure;
2. A description of each purpose of the requested use or disclosure;
3. A statement that the individual may:
   a. Inspect or copy the PHI to be used or disclosed; and
   b. Refuse to sign the authorization; and
   c. If use or disclosure of the requested information will result in direct or indirect payment to the covered entity from a third party, a statement that such payment will result.

An authorization is required for any use or disclosure of psychotherapy notes except notes used to carry out treatment, payment, or health care operations (45 CFR 164.508(a)(2)(ii)) if:
1. The provider is the originator of the treatment notes;
2. The information is used in training programs in which students, trainees or practitioners in mental health learn and practice or improve their skills in group, family, or individual counseling;
3. To defend a legal action.

Psychotherapy notes are notes recorded by a mental health professional documenting or analyzing the content of conversation during a private counseling session or a group, joint, or family counseling session. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop time, modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date (45 CFR 164.501).

Other exceptions to the authorization requirement include:
1. When use and disclosure is required by law (45 CFR 164.512(a)): disclosure about victims of abuse, neglect or domestic violence; disclosure for judicial and administrative procedures or for law enforcement purposes;
2. Use and disclosure for health oversight activities authorized by law (45 CFR 164.512(d)): audit, civil, administrative, or criminal investigations, inspections, licenses or disciplinary action;
3. Uses and disclosures about the deceased (45 CFR 512(g)(l));
4. Uses and disclosures to avert a serious threat to health and safety (45 CFR 164.512(j)(1)(i)).

According to the rules, an authorization is not valid if the document submitted has any of the following defects (45 CFR 164.508(b)(2)):

1. The expiration date has passed, or the expiration event is known by the covered entity to have occurred;
2. The authorization has not been filled out completely;
3. The authorization is known by the covered entity to have been revoked;
4. The authorization lacks an element required by the standard;
5. The authorization was combined with other documents creating a compound authorization;
6. Any material information in the authorization is known by the covered entity to be false.

A covered entity may use or disclose PHI without a written consent or authorization provided the individual is informed in advance and has the opportunity to agree to or prohibit or restrict the disclosure (45 CFR 164.510). The covered entity may inform the individual orally and obtain his/her oral agreement or objection to use or disclose the information for facility directories, involvement in the individual’s care and notification purposes.

A covered health care provider may use PHI to maintain a directory of individuals in its facility and may disclose the directory to members of the clergy or to other persons who ask for an individual by name (45 CFR 164.510(a)(1)(i)). The covered health care provider must inform the individual of the PHI that may be included in a directory and the persons to whom it may disclose such information and provide the individual with an opportunity to restrict or prohibit some or all of the uses or disclosures.

A covered entity may use or disclose PHI to a family member, other relative, a close personal friend, or any other person identified by the individual for involvement in the individual’s care or for payment or notification purposes (45 CFR 164.510(b)(1)(i)). A covered entity may use or disclose PHI to notify or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the individual’s care of the individual’s location, general condition, or death.

A covered entity may use or disclose PHI without the written consent or authorization of the individual or the opportunity for the individual to agree to or object to the extent that such use or disclosure is required by law, and the use or disclosure complies with and is limited to relevant requirements of the law (45 CFR 164.512). Covered entities may disclosed PHI for public health activities with regard to abuse, neglect or domestic violence; for health oversight activities; for judicial and administrative proceedings; to law enforcement officials as required by law; to a coroner or medical examiner about decedents; for research purposes; to avert a serious threat to health or safety; for specialized governmental functions; and for workers’ compensation.

A covered entity may use or disclose PHI for public health activities to prevent or control disease, injury, or disability, including, but not limited to, reporting disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health intervention. PHI may be disclosed to a public health authority or other appropriate government authority authorized to receive reports of child abuse and neglect. PHI also may be used or disclosed to a public health authority or a person subject to the jurisdiction of the Food and Drug Administration to report adverse events, product defects or problems, or biological product deviations; to track products; to enable product recall, repair or replacement; or to conduct post-marketing surveillance. PHI also may be used or disclosed to a person who has been exposed to a communicable disease or who may otherwise be at risk of contracting or spreading a disease or condition (45 CFR 164.512(b)).

PHI may be used or disclosed to an employer about an individual who is a member of the employer’s workforce (45 CFR 164.512(b)(v)) if:

1. The covered entity is a health care provider who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer to either conduct an evaluation relating
to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury;
2. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
3. The employer needs such findings to comply with its obligations under OSHA or applicable state laws;
4. The covered health care provider provides written notice to the individual that PHI relating to medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time health care is provided or, if health care is provided on the work site, by posting the notice in a prominent place where the health care is provided.

A covered entity may disclose PHI about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence (45 CFR 164.512(c)). A covered entity that makes such a disclosure must promptly inform the individual that a report has been or will be made, except if:
1. The covered entity, in the exercise of professional judgment, believes informing the individual would place that individual at risk of serious harm; or
2. The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such a person would not be in the best interests of the individual as determined by the covered entity in the exercise of professional judgment.

A covered entity may disclose PHI to a health oversight agency for oversight activities, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight (45 CFR 164.512(d)(1)) of:
1. The health care system;
2. Government benefit programs for which health information is relevant to beneficiary eligibility;
3. Entities subject to government regulatory programs for which health information is necessary to determine compliance with program standards; or
4. Entities subject to civil rights laws for which health information is necessary to determine compliance.

A covered entity may disclose PHI in the course of any judicial or administrative proceeding (45 CFR 164.512(e)) in response to an order of a court or administrative tribunal, provided the covered entity discloses only the PHI expressly authorized by such order; or in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal; and if a covered entity receives satisfactory assurances from the party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:
1. The party requesting such information has made a good faith attempt to provide written notice to the individual, or, if the individual’s location is unknown, to mail a notice to the individual’s last known address;
2. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
3. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objections were filed; or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

A covered entity may disclose PHI for a law enforcement purpose to a law enforcement official (45 CFR 164.512(f)(1)):
1. As required by a law that requires reporting certain types of wounds or other physical injuries; or
2. In compliance with and as limited by the relevant requirements of a court order or court-ordered warrant or a subpoena or summons issued by a judicial officer; a grand jury subpoena; or an administrative request, including an administrative
subpoena or summons, a civil or authorized investigative demand, or similar process authorized under law, provided that:
   a. The information sought is relevant and material to a legitimate law enforcement inquiry;
   b. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
   c. De-identified information could not reasonably be used.

Except for disclosures required by law, a covered entity may disclose PHI in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided the covered entity may disclose only the following information (45 CFR 164.512(f)(2)):
   1. Name and address;
   2. Date and place of birth;
   3. Social security number;
   4. ABO blood type and Rh factor;
   5. Type of injury;
   6. Date and time of treatment;
   7. Date and time of death, if applicable; and
   8. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

The covered entity may not disclose, for the purposes of identification or location, any PHI related to the individual’s DNA or DNA analysis; dental records; or typing, samples, or analysis of body fluids or tissue.

A covered entity may disclose PHI in response to a law enforcement official’s request for such information about an individual who is or is suspected to be a victim of a crime if the individual agrees to the disclosure; or the covered entity is unable to obtain the individual’s agreement because of incapacity or other emergency circumstance (45 CFR 164.512(f)(3)) provided that:
   1. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
   2. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
   3. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

A covered entity may disclose PHI about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the individual’s death if the covered entity has a suspicion that such death may have resulted from criminal conduct (45 CFR 164.512(f)(4)).

A covered entity may disclose to a law enforcement official PHI that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity (45 CFR 164.512(f)(5)).

A covered health care provider delivering emergency health care in response to a medical emergency, other than an emergency on the premises of the covered health care provider, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement (45 CFR 164.512(f)(6)) to:
   1. The commission and nature of a crime;
   2. The location of such crime or of the victim(s) of the crime; and
   3. The identity, description, and location of the perpetrator of the crime.

A covered entity may use or disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining the cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use PHI. Additionally, a covered entity may disclose PHI to funeral directors as necessary to carry out their duties with respect to the deceased (45 CFR 164.512(g)).

A covered entity may use or disclose PHI to organ procurement organizations or other entities engaged in
the procurement, banking, or transplantation of cadaver organs, eyes, or tissues for the purpose of facilitating organ, eye, or tissue donation and transplantation (45 CFR 164.512(h)).

A covered entity also may use or disclose PHI for research regardless of the source of funding of the research, provided the covered entity obtains documentation that an alteration to or waiver of the individual’s authorization has been approved by either an institutional review board or a privacy board (45 CFR 164.512(i)).

A covered entity may use or disclose PHI if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody (45 CFR 164.512(j)).

A covered entity may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual if the correctional institution or such law enforcement official represents that obtaining such PHI is necessary for (45 CFR 164.512(k)(5):
1. Providing health care to the individuals;
2. The health and safety of the individual or other inmates;
3. The health and safety of officers or employees of or others at the correctional institution;
4. The health and safety of the individuals and officers or other persons responsible for transporting inmates or transferring them from one institution, facility, or setting to another;
5. Law enforcement on the premises of the correctional institution; and
6. The administration and maintenance of the safety, security, and good order of the correctional institution.

A covered entity that is a correctional institution may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed. An individual is no longer an inmate when released on parole, probation, or supervised release or when otherwise is no longer in lawful custody (45 CFR 164.512(k)(5).

A covered entity may disclose PHI to the extent necessary to comply with laws relating to workers’ compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault (45 CFR 164.512(l)).

The Privacy Standards also require covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary (45 CFR 164.502(b), 164.514(d)). The provisions require a covered entity to develop and implement appropriate policies and procedures. The policies and procedures must identify the people within the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate for such access (45 CFR 164.530(a)(1)).

The standards allow a covered entity to use and disclose de-identified PHI (45 CFR 164.502 (d)), that is, information that does not identify a specific individual. Individually identifiable health information is a subset of health information, including demographic information, that is created or received by a health care provider, health plan, employee or health care clearinghouse. Such information generally relates to past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or past,
present or future payment for the provision of health care. The information identifies the individual or creates a reasonable basis to believe the information can be used to identify the individual. Information relayed orally is covered to ensure that information retains protection even when discussed or read aloud from a computer screen or a written document.

Health information that does not identify an individual and for which there is no reasonable basis to believe that it can be used to identify an individual is not individually identifiable health information. A covered entity may determine that health information is not individually identifiable only if identifiers of the individual or of relatives, employers, or household members of the individual are removed. This includes name, street address, city, county, precinct, ZIP code and equivalent geocodes, birth date, admission date, discharge date, date of death; telephone and fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Internet universal resource locators (URLs) and Internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and any other unique identifying number, characteristic, or code.

The standards allow providers and plans to give PHI to business associates (45 CFR 164.502(e)) if the providers and plans obtain satisfactory assurances that the business associates will use the information only for the purposes for which they are engaged. A business associate is a person/entity who works on behalf of the covered entity but who is not a member of the workforce who performs a function involving the use and disclosure of individually identifiable health information, including claims, processing or administrative data, data analysis, utilization review, billing, benefit management and repricing. It also includes legal, actuarial, accounting, consulting, data aggregation, accreditation or financial services (45 CFR 160.103, 164.502(e), 164.514(e)) A health care provider, health plan or other covered entity may, however, be a business associate to another covered entity.

A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information (45 CFR 164.502(e)(1)). That assurance is not needed if the disclosure is to a health care provider concerning treatment of the individual or disclosure by a group health plan or health insurance insurer or HMO to the plan sponsor (45 CFR 164.02(e)(1)(ii)).

A covered entity must document satisfactory assurance through a written contract or other written agreement or arrangement with the business associate (45 CFR 164.502(e)(1)). The contract or other arrangement between the covered entity and the business associate must:

1. Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate requirements of the act, except that:
   a. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate;
   b. The contract may permit the business associate to provide data aggregation services relating to health care operations of the covered entity.

2. Provide that the business associate will:
   a. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
   b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided by its contract;
   c. Report to the covered entity any use or disclosure of the information of which it becomes aware not provided for by its contract;
   d. Ensure that any agent, including a subcontractor, to whom it provides PHI received from or created or received by the business associate on behalf of the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
e. Make PHI available to the individual except as provided by the act (45 CFR 164.524(a)(1));

f. Make PHI available for amendment, and incorporate any amendments to PHI in accordance with the law. (An individual has the right to have a covered entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.) (45 CFR 164.526(a)(1));

g. Make available the information required to provide an accounting of disclosures. (With a few exceptions, an individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested.) (45 CFR 164.528(a)(1));

h. 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 Health and Human Services for purposes of determining the covered entity’s compliance with the law; and

i. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protection of the contract to the information, and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

According to the rules, a covered entity may use and disclose PHI for payment purposes (45 CFR 164.506). “Payment” encompasses the various activities of health care providers to obtain payment or to be reimbursed for their services and for a health plan to obtain premiums, to fulfill coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. Common payment activities include, but are not limited to:

1. Determining eligibility or coverage under a plan and adjudicating claims;
2. Risk adjustments;
3. Billing and collection activities;
4. Reviewing health care services for medical necessity, coverage, justification, or charges and the like;
5. Utilization review activities; and
6. Disclosure to consumer reporting agencies.

The privacy rules permit covered entities to continue to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the “payment” definition. Through a business association arrangement, the covered entity may engage a debt collection agency to perform this function on its behalf.

**Group Health Plan**

Before a group health plan can disclose health information to the plan sponsor or permit the disclosure of PHI to the plan sponsor by a health insurance issuer or HMO, the plan must ensure that its documents restrict uses and disclosure by the plan sponsor. The group health plan may disclose summary health information to the plan sponsor if the sponsor requests such information to obtain premium bids from health plans or to modify, amend or terminate a group health plan (45 CFR 164.504).

The group health plan’s plan document must be amended to incorporate provisions to establish permitted and required uses and disclosures of PHI by the plan sponsor. The plan document must provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification that the plan documents have been amended. The plan document must authorize termination of the contract by the covered entity if the...
covered entity determines that the business associate has violated the terms of the contract.

The amended certification document must indicate that the plan sponsor agrees (45 CFR 164.504(f) to:
1. Not use or further disclose the information other than as permitted or required by the plan document or as required by law;
2. Use appropriate safeguards to prevent the use or disclosure of the information other than as provided by the contract;
3. Ensure that any agents, including subcontractors, agree to the same restrictions and conditions that apply to the plan sponsor;
4. Not to use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan;
5. Report to the group health plan any use or disclosure of the information of which it becomes aware that is inconsistent with the uses or disclosures provided for;
6. Make PHI available to the individual;
7. Make PHI available for amendment, and incorporate any amendments to PHI with regard to an individual’s right to amend PHI as long as the PHI is maintained;
8. Make PHI available as required to allow the individual to receive an accounting of PHI disclosures made by a covered entity in the six years prior to the date on which the accounting is requested;
9. Make available to the Secretary of Health and Human Services 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; and
10. At termination of the contract, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form, and retain no copies of such information, or, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The plan document of the group health plan must also provide for adequate separation between the group health plan and the plan sponsor. It must describe employees or classes of employees under the control of the plan sponsor who will be given access to the PHI to be disclosed. Any employee who receives PHI relating to payment, health care operations, or other matters pertaining to the group health plan in the ordinary course of business also must be included. The plan document also must restrict access to and use by such employees to the function that the plan sponsor performs for the group health plan.

The rules also provide that an individual has a right to adequate notice of the uses and disclosure of PHI that may be made by the covered entity and of the individual’s rights and the covered entity’s legal duty to protect the health information (45 CFR 164.520(a)). An individual enrolled in a group health plan has a right to notice:
1. From the group plan if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health issuer or HMO; or
2. From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

A health plan must provide notice:
1. No later than the compliance date for the health plan to individuals then covered by the plan;
2. Thereafter, at the time of enrollment, to individuals who are new enrollees; and
3. Within 60 days of a material revision to the notice to individuals then covered by the plan.

No less frequently than once every three years the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice. The health plan satisfies the requirement if notice is provided to the named insured of a policy under which coverage is provided and one or more dependents. If a health plan has more than one notice, it satisfies the requirement by providing the notice that is relevant to the individual or other person requesting the notice.

The notice must be provided in plain language and must contain the following elements (45 CFR 164.520(b)):
1. The notice must contain the following statement as a header or be otherwise prominently displayed: “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;”

2. The notice must contain:
   a. A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted to make for each of the following purposes: treatment, payment, and health care operations;
   b. A description of each of the other purposes for which the covered entity is permitted or required to use or disclose PHI without the individual’s written consent or authorization;
   c. If a use or disclosure is prohibited or materially limited by other applicable laws, the description of such use or disclosure must reflect the more stringent law;
   d. For each purpose described, the description must include sufficient detail to place the individual on notice of the use and disclosures that are permitted or required;
   e. A statement that “other uses and disclosures will be made only with the individual’s written authorization” and that the individual may revoke such authorization.

3. If the covered entity intends to engage in other activities, the description must include a separate statement about the other activities. For example, the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services. Another example would be that the covered entity may contact the individual to raise funds for itself;

4. The notice must contain a statement of the individual’s rights with respect to PHI and a brief description of how the individual may exercise those rights. (The right to request restrictions on certain uses and disclosures of PHI, including a statement that the covered entity is not required to agree to a requested restriction; the right to receive confidential communications of PHI; the right to inspect and copy the PHI; the right to amend PHI; the right to receive an accounting of disclosures of PHI; and the right of an individual, including the individual who has agreed to receive the notice electronically, to obtain a paper copy of the notice from the covered entity);

5. The notice must also contain:
   a. A statement that the covered entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices;
   b. A statement that the covered entity is required to abide by the terms of the notice currently in effect; and
   c. For the covered entity to apply a change in a privacy practice that is described in the notice, a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains. The statement also must describe how it will provide individuals with a revised notice.

6. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary of Health and Human Services if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint;

7. The notice must contain the name or title and telephone number of a person or office to contact for further information;

8. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

Revisions to the notice must be revised and distributed promptly whenever there is a material change to the uses or disclosures, the individual’s rights, the covered entity’s legal duties, or other privacy practices. The notice must be made available upon request to any person and to individuals as applicable.

A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO and does not create or receive PHI other than summary health information or information on whether an individual is participating in the group health plan or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan is not required to maintain or provide notice (45 CFR 164.530(k)).
Health Care Clearinghouse

When a clearinghouse creates or receives PHI as a business associate of another covered entity, the clearinghouse must comply with the standards, requirements and implementation specifications of the law. A clearinghouse is prohibited from using or disclosing PHI. A clearinghouse, like other covered entities (45 CFR 164.500(b)), may use or disclose PHI:

1. To the individual;
2. With a consent to carry out treatment, payment or health care operations;
3. With an authorization;
4. With an agreement to prohibit or restrict the disclosure;
5. Without consent if consent is not required and has not been sought to carry out treatment, payment or health care operations;
6. When an entity uses or discloses PHI to make a marketing communication to an individual that occurs either in a face-to-face encounter or concerns products or services of nominal value or concerns health-related products and services;
7. When uses and disclosures are for fundraising (demographic information relating to the individual, date of health care);
8. For underwriting and related purposes; and
9. When required by the Secretary of Health and Human Services.

A clearinghouse may use or disclose PHI without consent or authorization or the opportunity for the individual to agree or object (45 CFR 164.512) when the information is used or disclosed to:

1. A public health authority authorized to collect or receive such information for the purpose of preventing or controlling disease, injury or disability;
2. A public health authority authorized to receive reports of child abuse or neglect;
3. People subject to the jurisdiction of the Food and Drug Administration;
4. People who may have been exposed to a communicable disease or who may otherwise be at risk for contracting or spreading a disease;
5. An employer about an individual who is a member of the employer’s workforce if:

a. The covered entity is a health care provider who is member of the workforce of such employer or who provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance or the workplace or to evaluate whether the individual has a work-related illness or injury;
b. The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
c. The employer needs such findings in order to comply with its obligations under the act; and
d. The covered health care provider provides written notice to the individual that PHI relating to medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by either giving a copy of the notice to the individual at the time the health care is provided or by posting the notice in a prominent place in the worksite if the health care is provided on site.

Penalties

The Health and Human Services (HHS) Office for Civil Rights will be responsible for enforcing the regulations (45 CFR 160.310). Compliance with the rules involves:

1. Providing records and compliance reports;
2. Cooperating with complaint investigation and compliance review;
3. Permitting access to information.

Plan participants may trigger noncompliance inquiries by filing complaints with HHS, which may follow up with an investigation and compliance review. Enforcement activities include working with covered entities to secure voluntary compliance through the provision of technical assistance and other means; responding to questions regarding regulations and providing interpretations and guidance; responding to state requests for exception determinations; investigating complaints and conducting compliance reviews; and, where voluntary compliance cannot be achieved, seeking civil monetary penalties and making referrals for criminal prosecution.
HHS will inform the group plan if it discovers a failure to comply. Enforcement actions may be taken if cooperation and compliance cannot be achieved informally (Public Health Services Act 42 United States Code 2722). Health plans and other covered entities that violate the privacy rules can face:

1. Civil penalties from $100 per violation/incident up to a maximum of $25,000 limit per person, per year, per standard; and
2. Criminal penalties up to:
   a. $50,000 fine and one year in prison for obtaining or disclosing protected information;
   b. $100,000 fine and up to five years in prison for obtaining protected information under false pretenses; and
   c. $250,000 fine and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

Conclusion

Several steps need to be taken to comply with the rules. Plan sponsors will be held to a good faith compliance standard; however, every effort to comply is expected. The following steps are necessary for a covered entity to comply:

1. Educate all employees at all levels about the new privacy rules;
2. Train all employees at all levels to recognize when they may or may not use and disclose PHI;
3. Communicate new privacy policies and procedures to employees and to third parties that send or receive information.

Privacy policies and practices will take time to implement. People likely will be resistant to changes and will be uncertain and afraid to handle protected information for fear of violating privacy protections. Monitoring and review should be ongoing once education, training, and policies and practices are implemented.

For More Information

For more information about this subject, feel free to contact your MTAS Human Resources Consultant. Information also is available through the office of the Secretary of Health of Human Services Office of Civil Rights at www.hhs.gov/ocr.

Or, call the MTAS Answer Line to receive quick answers to short questions: (888) 667-MTAS (6827). You also may visit our Web site at www.mtas.utk.edu.

The Municipal Technical Advisory Service (MTAS) is a statewide agency of The University of Tennessee’s Institute for Public Service. MTAS operates in cooperation with the Tennessee Municipal League to provide technical assistance services to officials of Tennessee’s incorporated municipalities. Assistance is offered in areas such as accounting, administration, finance, public works, ordinance codification, and wastewater management.

MTAS Technical Bulletins are information briefs that provide a timely review of topics of interest to Tennessee municipal officials. Bulletins are free to Tennessee local, state, and federal government officials and are available to others for $2 each.