

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
PRIVACY NOTICE**

**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.**

Plan: The Carnegie Mellon University Benefit Plan (the Plan)
Effective Date: April 14, 2003

Introduction

This plan is required by law to maintain the privacy of protected health information (PHI) and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information. This is the purpose of this notice.

The plan will abide by this notice unless and until it is changed. The plan reserves the right to change the terms of this notice and to make the changes applicable to all protected health information that it maintains, regardless of whether the information was created before or after the change. You will be notified of any changes.

Protected Health Information

Protected health information is "health information" that is "individually identifiable."

Health information means any information created or received by the health plan that 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 to an individual.

Please note that information developed by the employer in its capacity as employer is not created or maintained by the plan and therefore is not protected health information. Thus, information created or maintained by the employer for the purpose of administering sick pay or disability or worker's compensation programs, for example, is not protected health information.

Individually identifiable health information is health information that:

- < identifies the individual; or

- < with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Use and Disclosure for Treatment, Payment or Health Care Operations

Under the law, the plan may use or disclose protected health information without the consent of the individual in order to carry out "treatment, payment or health care operations." The plan will not be involved with "treatment," which means treatment by doctors and hospitals, but it may be involved with "payment" and "health care operations." Disclosure may be made to the sponsor of the plan, as described in the plan amendment implementing the privacy rules of HIPAA.

"Payment" means anything related to money coming into the plan (*i.e.*, premiums) or going out of the plan (*i.e.*, benefits). For example, that means:

- < determining eligibility for the plan or actual coverage under the plan,
- < determining benefits under the plan, including coordination of benefits and subrogation,
- < determination of premiums,
- < billing, claims management, collection activities, collecting on stop-loss insurance, and related data processing,
- < determinations of medical necessity, appropriateness or justification of charges, and
- < utilization review, pre-certification, and concurrent and retrospective review.

"Health care operations" means virtually everything else that the plan administrator (or someone retained by the plan administrator) might do with respect to a health plan, including:

- < case management,
- < credentialing doctors and hospitals, as well as training, accreditation, certification, and licensing,
- < underwriting, premium rating and other activities relating to creating, renewing or replacing a health insurance contract or stop-loss contract (provided some additional rules are met),
- < conducting or arranging for medical review, legal services and auditing functions,
- < business planning and development, such as conducting cost management and other analyses relating to managing and operating the entity, including development of formularies, methods of payment and coverage policies, and
- < management and general administration of the entity, including customer service, resolution of grievances, due diligence in connection with a sale or transfer of assets to another plan.

There is one exception to the exception: the ability to use or disclose protected health information to carry out treatment, payment or other health care operations does not apply to *psychotherapy notes*.

Use and Disclosure for Other Purposes

Under the law, the plan may use protected health information for a number of other purposes, which are set out in detail in a regulation of the federal Department of Health and Human Services at 42 C.F.R § Parts 160 and 164. It's not likely that any of them would apply, but the government makes us describe them.

Disclosure About an Individual to That Individual

The plan may disclose protected health information about an individual to that individual. If the individual is an adult (or an emancipated minor), it may also disclose protected health information about an individual to that individual's "personal representative" who has authority to make decisions related to health care (think of a living will).

If the individual is an unemancipated minor, disclosure depends on two factors:

- < If the minor has consented to the treatment and does not need the consent of a parent, guardian or other person acting *in loco parentis*, then the plan may *not* share information with the parent, guardian or person acting *in loco parentis* unless the minor asks the plan to do so.
- < If the plan has a reasonable belief that the individual has been (or may be) subjected to domestic violence, abuse or neglect and disclosing information to the personal representative could endanger the individual, the plan need not share any information with the personal representative.

Otherwise, the plan will treat the parent, guardian, or other person acting *in loco parentis* as personal representative of a minor and give them all the same information that it would give the individual.

If you die, your protected health information will remain protected. But the plan will treat your executor, administrator or other such person as your personal representative.

Disclosure to Family Where the Individual Agrees or Doesn't Object

If the individual is there, the plan may disclose protected health information to a member of the family, other relative, or close personal friend (or anyone else that the individual designates) as long as:

- < the individual agrees orally, or

- < the individual is given an opportunity to object and doesn't do so, or
- < the plan reasonably infers from the circumstances that the individual would not object.

In those circumstances, the plan may also use or disclose protected health information to notify a member of the family, a personal representative, or another person who is responsible for the health care of the individual, of the individual's location, general condition, or death. This also permits disclosure to agencies that assist in disaster relief.

If the individual is not there or is incapacitated, the plan may still make the disclosure if it reasonably determines that disclosure would be in the best interest of the individual.

Where the Individual Signs a Written Authorization

If use or disclosure is not otherwise permitted, the plan may always get a written authorization from the individual to use or disclose the individually identifiable health information.

To Create "De-Identified" Information

Protected health information may be used to create information that is not protected health information (awkwardly called "de-identified information" by the regulations). In order to be considered "de-identified," the information:

- < must not contain names, telephone numbers, fax numbers, e-mail addresses, Social Security numbers, medical record numbers, account numbers, license numbers, license plate and similar numbers, device identifiers, URL's, IP numbers, biometric identifiers such as fingerprints and voiceprints and photographs;
- < must not contain any geographic identification smaller than a state, except that it may show ZIP codes aggregated to the first three digits if aggregating those ZIP codes make a geographic unit with more than 20,000 people in it (if aggregating ZIP codes with the first three digits doesn't cover a population of more than 20,000 people, the information must show the ZIP code as "000"); and
- < if it contains dates of birth, admission, discharge or death, only the year is shown and, for ages over 89, it says only "over 89."

Information that is "de-identified" may contain a code that enables the creator to "re-identify" it, but then use or disclosure of the code is considered use or disclosure of protected health information.

Alternatively, the plan may have a statistician bless the information, as long as he or she has "appropriate knowledge of and experience with generally accepted statistical and scientific

principles and methods for rendering information not protected" *and* determines that the risk is very small *and* documents the methods and results of the analysis that justify that conclusion.

When the Government Wants to Know

When the government wants to know protected health information about someone, the plan is only permitted but *required* to disclose it, and you have no say in the matter. The list of possible government uses of protected health information is long and includes, for example:

- < for public health agencies to prevent or control disease,
- < for public health agencies to receive reports of child abuse or neglect,
- < for social service agencies to receive reports of abuse, neglect or domestic violence,
- < for the Food and Drug Administration to safeguard food and drug products,
- < for a "health oversight agency" for oversight of the health care system and government benefit programs,
- < for judicial and administrative proceedings (subpoenas, discovery requests, and so forth) as long as some requirements are met,
- < for law enforcement purposes (with some limitations), including information about victims of crime, suspicious deaths, crimes on the premises of the health care provider, and information needed to locate victims, suspects, fugitives, witnesses and missing persons,
- < for use by a coroner or medical examiner,
- < for use by funeral directors,
- < for government research purposes (within limits),
- < to avert a serious threat to health or safety, including apprehending a suspect,
- < for military and veterans activities,
- < for national security and intelligence activities,
- < for protecting the president of the United States and others entitled to government protection such as foreign heads of state,
- < for the proper operation of correctional institutions and other custodial situations, and
- < to comply with workers' compensation laws.

Whistleblowers

Anyone may disclose protected health information to a government agency if he or she has a good faith belief that their plan (or a business associate of the plan) has broken the law or violated professional or clinical standards or that the care, services or conditions provided by the plan (or business associate) endanger patients, workers or the public. This includes lawyers retained by whistleblowers.

Extent of Disclosure

Even if use or disclosure is permitted, the law requires that the plan use or disclose only the minimum necessary to accomplish the permitted use or disclosure. This means:

- < The plan will identify those employees (or business associates) who have a need to know individually identifiable health information, identify what individually identifiable health information they need to know, and then taking steps to ensure that none of them has access to individually identifiable health information that they *don't* need to know.

- < The plan will apply rules to limit the disclosure of protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought and then review each request for disclosure individually to make sure it satisfies the criteria.

- < When requesting protected health information, the plan will always limit its request to the minimum necessary to accomplish its function.

For example, a request for (or disclosure of) an entire medical record will rarely be made or honored, because "an entire medical record" will almost never be the "minimum necessary" information.

Individual Rights

You have a variety of rights with respect to use and disclosure of protected health information, beyond simply insisting on privacy as described up to this point.

Additional Restrictions That You Request

You have the right to request that the plan restrict the use or disclosure of protected health information. The plan does not have to agree to the restriction, and it is the policy of the plan not to agree to additional restrictions beyond what the law requires.

You have the right to make reasonable requests to receive communications of individually identifiable health information by "alternative means" or at "alternative locations" if the you clearly state that the disclosure of all or part of that information could endanger you. For example, you might ask that results of medical tests be given to you at the office rather than sent to your home. The plan is not permitted to require any further explanation of the circumstances and must comply with your request.

Inspection and Copying

Upon your written request to the plan administrator, you may inspect and copy your own protected health information, except for (a) psychotherapy notes, (b) information compiled for use in (or in anticipation of) a civil, criminal or administrative proceeding, and (c) information

protected by a federal law relating to clinical laboratories. Here are the rules:

- < You will get a response to your request within 30 days, unless the information is not maintained (or accessible) on-site, in which case the plan administrator may take up to 60 days to respond. In addition, the plan administrator may have one extension of up to 30 days as long as you are provided with a written statement by the original deadline explaining why the extension is needed and when the plan administrator expects to act on the request.
- < Access will be provided in the form that you requested if the information is readily producible in that format. If not, the plan will provide a written copy (or any other form that you agree to).
- < If you agree in advance to settle for a "summary" of the information and agree in advance to pay any costs, the plan will provide only a "summary."
- < The plan administrator will arrange with you for a convenient time and place or you may agree that mailing will suffice.
- < If the same information is stored in more than one place, the plan need only provide access to one.
- < The plan will charge you for the actual costs, including labor and supplies for copying, postage if the information is mailed, and labor in preparing a summary (if you agree to take a summary).

Access and copying may be denied where a licensed health care professional determines that access is reasonably likely to endanger the life or safety of you or another person, or that the information contains a reference to some other person and access is reasonably likely to cause substantial harm to that other person. In addition, access may be denied to a personal representative where a licensed health care professional determines that access is reasonably likely to cause substantial harm to the individual or another person.

If inspection and copying are denied as to any part of the information, you must be given all other information. The denial must be written and explain the basis for the denial and set out the right to appeal (including a complaint to the Secretary of Health and Human Services). If the plan doesn't have the information requested, but knows who does, the plan administrator will tell you.

You will be afforded an appeal to a licensed health care professional who is designated as the reviewing official (and who did not make the initial determination, of course). The decision on appeal must be in writing. The decision of the reviewing official is final.

Correcting Your Own Protected Health Information

Upon your written request to the plan administrator, you have a right to correct your own protected health information maintained by the plan unless the plan didn't create the information (except the plan still has to change it if the originator is no longer available to change it), or it is not available for inspection, or it is already accurate and complete. Your request must explain in what way the information is incorrect.

The plan administrator will act on the request within 60 days, except that the plan administrator may have one extension of up to 30 days as long as the plan administrator explains to you, by the original deadline, why the plan needs more time and when the plan expects to take action on your request.

If your request is granted, the plan will correct the information, or at least identify the records that are not correct and provide a link to the change. In addition, the plan will provide the correction to all others, such as business associates, who have the bad information if the plan knows that they have relied, or could foreseeably rely, on the wrong information. And the plan will provide the correction to anyone else that you identify as having received the wrong information and needing the correction.

If your request is denied, the plan administrator will advise you in writing and describe the following remedies. In response, you may submit a "statement of disagreement," explaining why you disagree with the denial of the amendment, as long as it is reasonable in length and content. The plan may then prepare a written rebuttal to your statement of disagreement, and give it to you. Then the plan will keep as part of the record your request for correction, the plan administrator's denial, the statement of disagreement, and the rebuttal. Whenever the plan discloses the information, the plan will disclose all of those materials.

On the other hand, you need not submit a "statement of disagreement." If not, you may nevertheless require the plan to provide the request for correction and the denial in any subsequent disclosure of the information.

Naturally, if the plan is informed by another "covered entity" of a correction to any protected health information, the plan will make the correction on its records.

Getting an Accounting of Disclosures

Upon your written request to the plan administrator, you are entitled to an accounting of all disclosures over the past six years (but not before HIPAA took effect) of disclosures of protected health information other than the normal disclosures such as for treatment, payment or other health care operations and except for "incidental" disclosures.

The accounting must be in writing and must include disclosures to or by business associates. It must be provided within 60 days after the request (with one possible extension of 30 days). The first such accounting during any 12-month period must be free; you can be charged for subsequent accountings within that 12-month period.

The accounting will contain:

- < the date of the disclosure,
- < the name of the person who received the information and, if known, the address,
- < a brief description of the information that was disclosed, and
- < a brief statement of the purpose for the disclosure (or a copy of the individual's authorization).

If disclosure has been made repeatedly to the same person for the same purpose, the accounting may simply identify the first disclosure and then specify the frequency, "periodicity," or number of the disclosures, and finally identify the date of the last disclosure.

Further Information or Complaints

For further information, please ask the plan administrator:

Carnegie Mellon Benefits Office
UTDC - 4516 Henry Street, Pittsburgh, PA 15213-3730
412-268-4747

If you believe that your privacy rights have been violated, you may file a complaint with the plan administrator simply by sending a letter. You may also file a complaint with the U. S. Department of Health and Human Services. No one will retaliate against you for filing a complaint.