GEORGETOWN UNIVERSITY

Protection of Health Information
Policies and Procedures Manual

Privacy Policies and Procedures
Table of Contents

Acknowledgement and Thanks

Georgetown University expresses its gratitude to the University of Oklahoma and its General Counsel, Joseph Harroz, Jr., (Georgetown Law '92) for permitting Georgetown University to model its Privacy Policies on those developed by the University of Oklahoma.

Version: 4.04.03.#1

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Introduction	**Coverage:** Health Care Components
Policy #: Privacy-00	**Page:** 1 of 2
HIPAA Section:	**Approved:**
Effective Date: April 12, 2003	**Revised:**

These Policies apply to all health information, regardless of the form in which it is created or maintained (i.e., whether oral, written or electronic).

These Policies apply to the health information of both living and deceased patients.

I. POLICY

It shall be the policy of the University[1] to protect and safeguard the protected health information created, acquired and maintained by its Health Care Components in accordance with the Privacy Regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 and applicable state laws.

The Policies contained in this manual are intended to provide guidance to University Personnel in regard to the protection and enhancement of the privacy rights of patients by (a) establishing rules related to the internal and external use and disclosure of protected health information; (b) affording patients access and information regarding the use and disclosure of their protected health information; and (c) implementing administrative procedures intended to assist patients and University Personnel to effectuate these Policies.

These Policies will apply to all protected health information collected by Health Care Components after April 14, 2003. The Policies apply to all University Personnel within University Health Care Components. These Policies shall apply, in general, to Health Benefit Plans, except to the extent that such Health Benefit Plans (i) have binding commitments from the plan that it is responsible for HIPAA compliance, or (ii) have been granted an "on-site" exemption by the University. University departments providing services to third parties as a Business Associate or which are defined as "Non-covered Providers" by the University may adopt these policies on a departmental basis.

The Policies supersede and replace any existing policies and procedures of any Health Care Component relating to the use and disclosure of protected health information. Health Care Components only can maintain separate policies and procedures relating to the use and disclosure of health information to the extent that they

[1] The University is a Hybrid Entity with designated Health Care Components. See, Privacy-01, number 11.

do not conflict with these Policies. Health Care Components can add to or supplement the Policies or the forms attached hereto, but may not delete anything without first consulting with the Privacy Official.

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Definitions	**Coverage:** Health Care Components
Policy #: Privacy-01 (Definitions)	**Page:** 1 of 8
HIPAA Section: 164.510(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. DEFINITIONS

Unless otherwise provided, the definitions set forth below apply to all of the Privacy Policies. Certain terms will be capitalized when used in the policies to indicate that they have been uniquely defined by the University.

1. Business Associate. A person or entity not employed by the University that provides certain functions, activities, or services for or on behalf of the University, which involves the use and/or disclosure of a patient's protected health information. Such activities may include, but are not limited to, billing, repricing, claims processing and administration, data analysis, legal, accounting, actuarial, consulting, utilization review, quality assurance, and similar services or functions. A business associate may be a covered entity. The definition of a business associate excludes a person who is part of the covered entity's workforce. 45 C.F.R. § 160.103.

2. Compliance Date. The date by which a covered entity must comply with the Privacy Regulations, which is April 14, 2003.

3. Correctional Institution. 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 or other persons held in lawful custody. *Other persons* held in lawful custody include juvenile offenders, adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. 45 C.F.R. § 164.501.

4. Covered Entity. The entities to which the Privacy Regulations apply, which include: (a) a health plan; (b) a health care clearinghouse; and (c) a health care provider who transmits any health information in electronic form in connection with one of the following eleven (11) transactions: (i) health care claims or equivalent encounter information; (ii) health care payment and remittance advice; (iii) coordination of benefits; (iv) health

care claims status; (v) enrollment and disenrollment in a health plan; (vi) eligibility for a health plan; (vii) health plan premium payments; (viii) referral certification and authorization; (ix) first report of injury; (x) health claims attachments; and (xi) other transactions that the Secretary of DHHS may prescribe by regulation. 45 C.F.R. § 160.103.

5. Covered Functions. Those functions of a covered entity the performance of which makes the entity a health care provider. 45 C.F.R. § 160.103.

6. Designated Record Set. A group of records maintained by or for a University Health Care Component that includes the medical and billing records about individuals or that are used, in whole or in part, by University Personnel to make decisions about individuals, regardless of who originally created the information. A designated record set does not include: (a) duplicate information maintained in other systems; (b) data collected and maintained for research; (c) data collected and maintained for peer review purposes; (d) psychotherapy notes; (g) information compiled in reasonable anticipation of litigation or administrative action; (h) employment records; (i) student records; and (j) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films).

This definition refers only to the official record for the patient and not to duplicate information maintained in other systems. 65 Fed Reg. 82559

7. Disclose or Disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the University's Health Care Components. 45 C.F.R. § 164.501.

Exchange of protected health information with a department of the University that is not designated as a Health Care Component is considered a disclosure

8. Direct Treatment Relationship. A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. 45 C.F.R. § 164.501.

9. Health Benefit Plans. The health benefit plans or programs offered by University for the benefit of its faculty, students and staff.[2]

[2] Such plans are: Georgetown Health Plan; Kaiser Permanente HMO Signature; CareFirst Blue Cross Blue Shield Dental; Aetna USHealthcare DMO; EyeMed Vision Discount Card; Faculty and Staff Assistance Program; Athletic Department Secondary Insurance Plan; Athletic Department Medical Clinic; Life Insurance; Short and Long Term Disability; Long Term Care Insurance; Student Health Insurance Plan; Health Care and Dependent Care Flexible Spending Accounts; Flu Vaccine Program; Workers Compensation.

10. Health Care. Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following: (a) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (b) sale or dispensing of a drug, device equipment, or other item in accordance with a prescription. 45 C.F.R. § 160.103.

11. Health Care Component(s). A component or combination of components designated by the University, which is a hybrid entity. The "health care components" of the University include the: (i) Medicare Demonstration Project; (ii) Counseling and Psychiatric Services (CAPS); (iii) Imaging Science and Information Systems Center (ISIS); (iv) Risk Services; (v) Internal Audit; (vi) Health Benefits Group of Human Resources; (vii) Office of University Counsel; and (viii) Health Care Computing Group of University Information Services.

As this term is used in the University's Privacy Policies, it will include all of the constituent parts of a Health Care Component (e.g. departments and clinics) and University Personnel providing health care services on behalf of the University.

12. Health Care Operations. "Health care operations" means any of the following activities of the University to the extent that the activities are related to covered functions:

> (a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of University Personnel and patients with information about treatment alternatives; and related functions that do not include treatment;
>
> (b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as University Personnel, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(c) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(d) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the University, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(e) Business management and general administrative activities of the University, including, but not limited to: (1) management activities relating to implementation of and compliance with the University's privacy policies; (2) resolution of internal grievances; (3) due diligence related to the sale, transfer, merger or consolidation of all or part of a Health Care Component with another covered entity; and (4) creating de-identified health information or a limited data set, and fundraising for the benefit of a Health Care Component(s). 45 C.F.R. § 164.501.

13. Health Care Provider. A provider of services (as defined in § 1861(u) of the Social Security Act, 42 U.S.C. § 1395x(u)), a provider of medical or health services (as defined in § 1861(s) of the Act, 42 U.S.C. § 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. 45 C.F.R. § 160.103.

14. Health Information. Any information, whether oral or recorded in any form or medium, that: (a) is created or received by a health care provider…employer…school or university… and (b) 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. 45 C.F.R. § 160.103.

15. Health Oversight Agency. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. 45 C.F.R. § 164.501.

16. HIPAA. The Health Insurance Portability and Accountability Act of 1996.

17. Hybrid Entity. A single legal entity: (1) that is a covered entity; (2) whose business activities include both covered and non-covered

functions; and (3) that designates Health Care Components. 45 C.F.R. § 164.504.

18. Indirect Treatment Relationship. A relationship between an individual and a health care provider in which: (a) the health care provider delivers health care to the individual based on the orders of another health care provider; and (b) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. 45 C.F.R. § 164.501.

19. Individually Identifiable Health Information. Information that is a subset of health information, including demographic information collected from an individual, and; (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (b) 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; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.503

20. Inmate. A person incarcerated in or otherwise confined to a correctional institution. 45 C.F.R. § 164.501.

21. Institutional Review Board (IRB). A multidisciplinary body, consisting of University employees, health care professionals and community representatives, charged with the responsibility for protecting human subjects in research through initial review and on-going oversight of the conduct of human subject research at the University.

22. Law Enforcement Official. An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (i) investigate or conduct an official inquiry into a potential violation of law; or (ii) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. 45 C.F.R. § 164.501.

23. Legal Counsel. The University's Office of University Counsel and the attorneys and full-time staff members that work therein.

24. Marketing. To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or services unless the communication is made: (a) To describe a health-related product or service (or payment for such product or service) that is provided by the University, including communications about: the entities participating in a health care provider network or health plan network; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (b) for treatment of the individual; or (c) for case management or care coordination for the

individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

25. Non-covered Providers. Those portions of the University which provide health care but which are not considered to be "covered providers" under HIPAA, namely, (i) Georgetown Emergency Response Medical Service (GERMS); (ii) Athletics Department; (iii) Student Health Center; and (iv) Child Development Center.

26. Organized Health Care Arrangement. A clinically integrated care setting in which the individuals typically receive health care from more than one health care provider (example: a hospital and members of its medical staff). 45 C.F.R. § 164.501.

27. Particularly Sensitive Health Information. Protected health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

28. Payment. Any activities by the University, or a Health Care Component, to obtain for providing health care. Such activities relate to the individual to whom health care is provided and included, but are not limited to: (a) billing, claims management, collection activities, and related health care data processing; and (b) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of reimbursement: (i) name and address; (ii) date of birth; (iii) social security number; (iv) payment history; (v) account number; and (vi) name and address of the health care provider. 45 C.F.R. §164.501.

29. Privacy Official. The person designated by the University who is responsible for the development and implementation of the HIPAA policies and procedures of the University. 45 C.F.R. §164.530.

30. Privacy Policies or Policies. This set of policies and procedures drafted and adopted by the University for the use of its Health Care Components relating to the protection and confidentiality of protected health information.

31. Privacy Regulations. The regulations issued by the Department of Health and Human Services implementing the privacy requirements of the Health Insurance Portability Act of 1996, 42 CFR Parts 160 and 164, and are aimed at protecting a patient's right to privacy in matters involving his or her health care.

32. Protected Health Information or PHI. Individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium.

Protected health information excludes individually identifiable health information in: (a) education records covered by the Family Educational Rights and Privacy Act (FERPA); and (b) employment records held by the University in its role as employer.

33. Psychotherapy Notes. Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Psychotherapy notes **excludes medication prescription and monitoring, counseling sessions start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R § 164.501.**

34. Public Health Authority. An agency or authority of the United States, a State, the District of Columbia, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. 45 C.F.R. § 164.501.

35. Required by Law. A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. 45 C.F.R. § 164.501.

36. Research. A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. 45 C.F.R § 164.501.

37. Security Officer. The person designated by the University to be responsible for the promulgation and implementation of the Security Regulations applicable to HIPAA.

38. Treatment. The provision, coordination, or management of health care and related services by University Personnel. 45 C.F.R. § 164.501.

Treatment includes: (a) the coordination or management of health care by a health care provider with a third party; (b) consultation between health care providers relating to a patient; or (c) the referral of a patient for health care from one care provider to another. 45 C.F.R. § 164.501.

40. University Personnel. Faculty, staff, volunteers, students and other trainees, volunteers, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. 45 C.F.R. § 160.103.

41. Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information **within** the University by Health Care Components. 45 C.F.R. § 164.501.

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Personal Representatives	**Coverage:** Health Care Components
Policy #: Privacy-02 (Uses & Disclosures)	**Page:** 1 of 3
HIPAA Section: 164.510(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish who can act on behalf of the patient for purposes of authorizing uses and disclosures and effectuating the patient rights afforded by these Policies.

II. POLICY

A Health Care Component must, except in the limited circumstances set forth in this Policy, treat a personal representative as the patient for purposes of authorizing uses and disclosures and effectuating the patient rights afforded by these Policies. *However, the personal representative must only be treated as the individual patient to the extent that the protected health information is relevant to matters on which the personal representative is authorized to represent the patient.*

If University Personnel have a reasonable belief that the personal representative has abused or neglected the individual patient, or that treating the personal representative as the patient could endanger the patient, and believe it is not in the patient's best interest to treat the person as the personal representative, University Personnel are not required to do so. See, Privacy-05, Patient Access to Protected Health Information.

Adults

The following can act as a personal representative of an adult:

1. Durable Power of Attorney for Health Care. A durable power of attorney is a document by which the patient may designate another as his/her agent to perform certain acts on behalf of the patient. Pursuant to a valid durable power of attorney, and depending on the scope of the power of attorney, the agent may make health and medical care decisions on the patient's behalf. This does not give the agent the power to execute on behalf of the patient an advance directive for health care, living will, or other document purporting to authorize life-sustaining treatment decisions, or make life-sustaining treatment decisions unless the power of attorney complies with the requirements for a health care proxy.

A valid durable power of attorney must be in writing and contain the words "This power of attorney shall not be affected by subsequent disability or incapacity of the principal, or lapse of time," or "This power of attorney shall become effective upon disability or incapacity of the principal," or similar words showing the intent of the

principal that the authority conferred will be exercisable notwithstanding the principal's subsequent disability or incapacity. The document should state whether University Personnel may rely on the power of attorney while the patient is still competent or whether it is only effective once the patient becomes incompetent.

The patient may revoke the power of attorney at any time if competent. Death of the patient also will revoke and terminate the power of attorney. The execution of a durable power of attorney should be witnessed by two witnesses who are at least 18 years old. The signature of the patient and witnesses should be notarized.

2. Health Care Proxy (Advanced Directive). A health care proxy is an adult appointed by a patient to make health care decisions, including but not limited to withholding or withdrawal of life-sustaining treatment, in certain circumstances pursuant to an advanced directive for health care decision. In particular, a health care proxy's authority only becomes effective (i) when the patient is incompetent and (ii) when the patient has been diagnosed with a terminal condition or as persistently unconscious. The directive must be in writing, signed by the patient, and witnessed by two disinterested witnesses. A disinterested witness is a witness who is at least 18 years old and who does not have an interest in the patient's estate.

The appointment of the health care proxy may be completely or partially revoked at any time and in any manner by the patient. A revocation is effective upon communication of the desire to revoke to the attending physician or other University Personnel. If the patient revokes the advanced directive, a health care proxy may no longer qualify as a personal representative.

3. Court Appointed Guardian. This is a person appointed by the court in a court order who legally has authority over the care and management of the person, estate, or both, of a patient who cannot act for him/herself. This order may place certain limitations on the legal activities of the guardian.

4. Experimental Treatment Statute. District of Columbia Code §21-2047 provides that a legal guardian or attorney-in-fact cannot consent to a patient's participation in a research study being conducted by the University that has received IRB approval except as may be ordered by the court.

Minors

For minor patients who are under the age 18 and who do not fall within an exceptions recognized by the laws of the District of Columbia with regard to emancipated minors, either parent, the legal guardian or the legal custodian appointed by a court may act as a minor's personal representative.

University Personnel are required to make a reasonable attempt to inform the spouse, parent or guardian of the minor of any emergency services provided to a minor unless the minor is a possible victim of abuse or such disclosure is prohibited under the laws of the District of Columbia. Should there be a question, the Office of University Counsel should be contacted.

Note, however, that under the law of the District of Columbia, persons under the age of 18, however, are permitted to obtain treatment for mental health disorders, drug and alcohol related conditions, sexually transmitted diseases, and pregnancy without parental consent or notification.

Deceased Individuals

A court-appointed executor, administrator, or personal representative of the deceased's estate can act on behalf of a deceased individual. The court document is known as the Letters Testamentary or Letters of Administration and should be signed by a judge. In some cases, it may be appropriate for next-of-kin to act on behalf of a deceased individual; the Office of University Counsel should be contacted in order to determine the ability of the next-of-kin to act.

III. PROCEDURES

1. University Personnel must review a copy of the document conferring personal representative status to ensure the personal representative's authority is not limited in scope or time and to ensure it meets the requirements described above. Any questions regarding the validity of a document purporting to confer personal representative status must be directed to the Office of University Counsel.

A copy of the written document appointing a person as the personal representative of a patient must be placed in the patient's medical record as verification of the individual's authority.

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Verification	**Coverage:** Health Care Components
Policy #: Privacy-03 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.514(h)	**Approved:**
Effective Date: April 12 2003	**Revised:**

I. PURPOSE

To establish an identity verification process.

II. POLICY

Prior to making a disclosure or processing a patient right request permitted by these Policies, University Personnel must: (i) verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to University Personnel; and (ii) obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure or processing.

University Personnel may rely on:

a. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope and de-identified information could not reasonably be used.

b. Appropriately executed documentation of an IRB or Privacy Board waiver or alteration of the authorization requirement.

c. A request by a public official upon presentation of his/her badge or other official credentials if in person or the appropriate letterhead if the request is made in writing.

d. Personal judgment if a disclosure is being made to avert a serious threat to health or safety or in cases when a patient is only required to be given an opportunity to agree or object.

III. PROCEDURES

Any questions regarding verification or reliance on identity or authority should be directed to the Office of University Counsel. The Office of University Counsel should be contacted prior to responding to any request by law enforcement officials if possible.

Verification of identity can be accomplished by: (1) presentation of picture I.D.; (2) signature comparison; or (3) some other appropriate method.

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Notice of Privacy Practices	**Coverage:** Health Care Components
Policy #: Privacy-04 (Patient Rights)	**Page:** 1 of 3
HIPAA Section: 164.520	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To require the development of a Notice of Privacy Practices and to provide for general distribution procedures.

II. POLICY

The University will develop and distribute a Notice of Privacy Practices for its Health Care Components that includes the information required by § 164.520 of the Privacy Regulations. A copy of the Notice of Privacy Practices will be attached hereto as Form – 04. A Health Care Component may develop its own Notice of Privacy Practices. If a Health Care Component elects to develop its own Notice of Privacy Practices, it must obtain the approval of the Privacy Official before publishing it or revising it. A patient's receipt of the Notice of Privacy Practices must be acknowledged as required by the Privacy Regulations.

The Notice of Privacy Practices must be translated into other languages as required by regulations issued by the Federal Office of Civil Rights regarding accommodations for people with Limited English Proficiency.

University Personnel may not use or disclose protected health information in a manner inconsistent with the University's Notice of Privacy Practices.

III. PROCEDURE

Acknowledgement

University Personnel must make a good faith effort to obtain a written acknowledgement from the patient of his/her receipt of the Notice of Privacy Practices. Each Health Care Component can determine how to obtain a patient's acknowledgement depending on its particular operational requirements.

However, the preferred method for obtaining acknowledgement is to require the patient to initial or sign the following statement which should be included on registration and/or encounter forms: "I acknowledge that I have received a copy of the University's Notice of Privacy Practices and I consent to the use of my protected health information for treatment, payment and the healthcare operations of the University as summarized in the Notice of Privacy Practices."

If the patient does not acknowledge receipt of the Notice of Privacy Practices, a note should be made on the registration form or in the patient's medical record indicating why the acknowledgement was not obtained. Health Care Components should not condition treatment on the patient's acknowledgement of the receipt of the Notice of Privacy Practices.

Distribution

1. University Health Care Components must make the Notice of Privacy Practices available to any person who requests it. The individual making the request does not have to be a current patient of the University.

2. In addition, the Health Care Components must ensure that health care providers with **direct** treatment relationships with patients:

a. Provide the Notice of Privacy Practices to each patient no later than the date of the first service delivery after the compliance date, including service delivered electronically. If the first service delivery to an individual is delivered electronically, a provider must provide an electronic copy of the Notice of Privacy Practices automatically and contemporaneously in response to the individual's first request for service.

During emergency treatment situations, the Notice of Privacy Practices may be provided and the acknowledgement obtained at a time reasonably practicable after the emergency treatment situation is resolved.

b. Make the Notice of Privacy Practices available at the service delivery site upon request.

c. Post the Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect individuals seeking service from the health care provider to be able to read the notice.

3. The Notice may be distributed by e-mail, if the patient agrees to the electronic notice and the agreement has not been withdrawn. All timing requirements still apply to electronic notices. If University Personnel know that the electronic transmission has failed, a hard copy must be provided. When electronic notice is provided, an acknowledgement of receipt must be obtained.

4. Health Care Components must ensure that health care providers with **indirect** treatment relationships with patients provide the Notice of Privacy Practices to individuals upon request.

5. The Notice of Privacy Practices for the Health Care Components must be posted and made available electronically on the web site of the University. Any Covered Component that maintains its own web site also must post the Notice of Privacy Practices on its web site or include a link to the Notice.

Amendment

If the Notice of Privacy Practices is amended, it must be made available upon request on or after the effective date.

Retention

The Notice of Privacy Practices must be retained by the Privacy Official for six years.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 43 (pg. 167-172).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82547–52, 82720-26 (December 28, 2000) and 67 Fed. Reg. 53238-53243 (August 14, 2002).

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Patient Access to Protected Health Information	**Coverage:** Health Care Components
Policy #: Privacy-05 (Patient Rights)	**Page:** 1 of 4
HIPAA Section: 164.524(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To permit patients access to their protected health information.

II. POLICY

Rights to Access

The University will permit patients to inspect and obtain a copy of protected health information about the patient included in a designated record set maintained by a Health Care Component(s), for as long as the protected health information is maintained in the designated record set. If the same information is kept in more than one designated record set or in more than one location, the University has to produce the information only once per request for access.

Unless an exception applies, a patient should be granted access to the entire medical record, including records received from other providers that were used to make treatment decisions.

The University may charge a fee for access to protected health information as long as the fee only includes the costs of copying and postage and is consistent with any limit set by State law.

The law of the District of Columbia does not contain any provision regarding the amount that can be charged for copying.

The University must provide the patient with access to protected health information in the form or format requested by the patient, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the University and the patient.

The University must arrange with the patient for a convenient time and place to inspect or obtain a copy of the protected health information, or mail a copy of the

information at the patient's request. A Health Care Component may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.

If the University does not maintain the protected health information that is the subject of the patient's request for access, and University Personnel knows where the requested information is maintained, the University must inform the patient where to direct the request for access.

Psychotherapy Notes

A patient does not have the right to access psychotherapy notes relating to him/herself except (i) to the extent the patient's treating professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access. See, definition of psychotherapy notes in Privacy-01, Definitions (number 23) and Privacy-24, Mental Health.

Denial of Right to Access

A patient may be denied access under the limited circumstances listed below. **The following exceptions should be narrowly construed and rarely used:**

1. Legal Information. The University may deny a patient access to information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. The advice of the Office of University Counsel should be obtained prior to denying a patient's request for access.

2. Inmate Information. The University, acting under the direction of a correctional institution, may deny, in whole or in part, an inmate's request to obtain a **copy** of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the patient or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

3. Research. The University may temporarily suspend a patient's access to protected health information created or obtained in the course of research that includes treatment. The suspension may last for as long as the research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the research, and the patient has been informed that the right of access will be reinstated upon completion of the research.

4. Information from Other Source. The University may deny a patient's access to protected health information if the information was obtained from someone other than a Health Care Provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

5. Endangerment. The University may deny a patient access in the event a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person. Access may not be denied on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm.

6. Reference to Other People. The University may deny a patient access if the protected health information makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment that the access requested is reasonably likely to cause substantial harm to such other person. Access can be denied if the release of such information is reasonably likely to cause substantial physical, emotional or psychological harm to the other person.

7. Personal Representative. The University may deny access if the request is made by a patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

8. Psychotherapy Notes. See, preceding section of this policy.

The University must, to the extent possible, give the patient access to any other protected health information requested, after excluding the protected health information as to which access is being denied.

Review of Denied Access

If access is denied for the reasons set forth in Number 5, 6 and 7 above, the patient must be given the opportunity to have the denial reviewed by the director or manager of the Health Care Component that received the request or some other appropriate person designated by the Health Care Component that maintains the records requested ("Reviewer"). The Reviewer cannot have participated in the original denial.

III. PROCEDURES

Rights to Access

1. Patients must make their requests for access in writing using the form attached hereto as Form-05.A. Patients making their request for access by telephone or e-mail should be forwarded a copy of the form. **Verification of the requester's identity must be obtained prior to granting access.** The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a request for access should provide the patient with the form attached hereto as Form-05.A. If a patient indicates that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request should immediately forward a copy of the request to the Privacy

Official who will coordinate the processing of the request with the other Health Care Components designated by the patient. If the patient does not request access from any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form and a copy of the denial letter, if applicable, to the Privacy Official.

3. A patient's request for access to protected health information must be acted upon as soon as reasonably possible, but in not more than thirty (30) days after receiving the request.

4. Each Health Care Component must designate and document the titles of persons responsible for receiving and processing requests for access by individual. A copy of the designations must be provided to the Office of University Counsel and the Privacy Official. The Health Care Components must update the lists as changes are made and provide an updated list to the Office of University Counsel and the Privacy Official. The Privacy Official must maintain a copy of the designations for a minimum of six (6) years.

The health care provider that treated the patient should be notified if a patient requests access to his/her protected health information for litigation or some other unusual purpose.

5. Any questions regarding a patient's right of access should be forwarded to the Office of University Counsel.

Denial of Right to Access

If a patient's request for access is denied, the individual must be provided with a written denial using the form attached hereto as Form-05.B. The denial form must be maintained in the patient's medical record for a minimum of six (6) years. The copies forwarded to the Privacy Official also should be maintained for six (6) years.

Review of Denied Access

Health Care Components are required to promptly forward requests for review to the Reviewer and the Reviewer is required to review the denial within a reasonable period of time, but no later than thirty (30) days after receiving the request for review. Access must be provided to the patient in accordance with the determination of the Reviewer who reviewed the request. The patient making the request should be notified promptly, in writing, of the Reviewer's decision.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 45 (pg. 175).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82554, 82731 (December 28, 2000).

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Accounting of Disclosures	**Coverage:** Health Care Components
Policy #: Privacy-06 (Patient Rights)	**Page:** 1 of 4
HIPAA Section: 164.528(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To permit patients to request an accounting of the disclosures of their protected health information.

II. POLICY

The University will permit patients to request an accounting of disclosures of protected health information made by the Health Care Components of the University. The accounting must include disclosures made by a Health Care Component in the six (6) years prior to the date of the request (unless limited at the request of the patient), including disclosures to or by business associates.

Accounting Requirements – General

The accounting must include all disclosures, **except** for disclosures:

1. to carry out treatment, payment and health care operations;

2. to patients of protected health information about them;

3. incident to a use or disclosure otherwise permitted or required by the Privacy Regulations;

4. pursuant to the patient's authorization;

5. for a facility directory or to persons involved in the patient's care;

6. for national security or intelligence purposes;

7. to correctional institutions or law enforcement officials to provide them with information about a person in their custody;

8. as part of a limited data set; or

9. that occurred prior to the compliance date.

Examples of disclosures subject to the accounting requirement include disclosures for, or pursuant to: (1) research, unless authorized by patient; (2) subpoenas, court orders or discovery requests; (3) abuse and/or neglect reporting; (4) communicable disease reporting; or (5) other reports to local health departments.

Accounting Requirement – Research Involving More than 50 Participants

If, during the period covered by the accounting, a Health Care Component had made disclosures of protected health information for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the patient may have been included, provide:

1. the name of the protocol or other research activity;

2. a description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

3. a brief description of the type of protected health information that was disclosed;

4. the date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

5. the name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

6. a statement that the protected health information of the patient may or may not have been disclosed for a particular protocol or other research activity.

If a Health Care Component provides an accounting for research disclosures as provided above, and if it is reasonably likely that the protected health information of the patient requesting the accounting was disclosed for such research, the Health Care Component shall, at the request of the patient, assist in contacting the entity that sponsored the research and the researcher.

The research accounting provision above permits the University to meet the requirement for research disclosures if it provides patients with a list of all protocols for which their PHI may have been disclosed for research purposes pursuant to a waiver of authorization by the IRB. To use this method of accounting the disclosure must involve at least 50 records.

Suspension of Accounting

A patient's right to receive an accounting of disclosures may be suspended at the request of a health oversight agency or law enforcement official if certain conditions are satisfied. If a Health Care Component receives a request to suspend patient's right to receive an accounting from a health oversight agency or law enforcement official, Legal Counsel should be contacted to determine if the appropriate conditions have been satisfied.

III. PROCEDURE

1. A patient must request an accounting for disclosure in writing using the form attached hereto as Form-06.A. **Verification of the requester's identity must be obtained prior to granting the request for an accounting.** Patients making their request for an amendment by telephone or e-mail should be forwarded a copy of the form. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a request for an accounting of disclosures should provide the patient with the form attached hereto as Form-06.A. If a patient indicates that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request should immediately forward a copy of the request to the Privacy Official who will coordinate the processing of the request with the other University Health Care Components designated by the patient. If the patient does not request an accounting from any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form and a copy of the accounting of disclosure form to the Privacy Official.

3. Health Care Components should designate an individual or individuals who will be responsible for processing requests for accounts of disclosures.

4. For each disclosure that must be recorded, the accounting must include the following information:

   a. the date of the disclosure;

   b. the name of the entity or person who received the protected health information and, if known, the address of such entity or person;

   c. a brief description of the protected health information disclosed; and

   d. a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.

5. The form attached hereto as Form-06.B must be used to record disclosures and must be maintained in a patient's medical record for a period of at least six (6) years from that date of the last accounting.

6. The Accounting Request Form and any copies of the request form and the accounting form forwarded to the Privacy Official also should be maintained for six (6) years.

7. If, during the period covered by the accounting, a Health Care Component has made multiple disclosures of protected health information to the same person or entity for a single purpose, or pursuant to a single authorization, the accounting may, with respect to such multiple disclosures, provide:

a. the information set forth in section 2 above for the first disclosure during the accounting period;

b. the frequency, periodicity, or number of the disclosures made during the accounting period; and

c. the date of the last such disclosure during the accounting period.

8. The University will act on the patient's request for an accounting, no later than sixty (60) days after receipt of such a request.

9. The first accounting to a patient in any twelve (12) month period must be provided at no charge. The University may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the twelve (12) month period, provided that the University informs the patient in advance of the fee and provides the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 47 (pg. 185).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82559, 82739 (December 28, 2000), 67 Fed. Reg. 53237, 53243, 53247 (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Communication by Alternative Means	**Coverage:** Health Care Components
Policy #: Privacy-07 (Patient Rights)	**Page:** 1 of 2
HIPAA Section: 164.522(b)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To permit patients to request communication of protected health information by alternative means or at alternative locations.

II. POLICY

The University will permit patients to request, and will accommodate reasonable requests by patients, to receive communications of protected health information by alternative means or at alternative locations.

If a request for communication by alternative means is granted, Health Care Components of the University must communicate with the patient in accordance with the patient's request.

The University **cannot** require an explanation from the patient as to the basis for the request as a condition of considering or granting the request.

The University can condition the provision of an alternative means of communication on: (a) information as to how payment will be handled, if applicable and (b) the specification of an alternative address or other method of contact.

III. PROCEDURE

1. A patient must request communication by alternative means or at alternative locations in writing by using the sample form attached hereto as Form-07.

2. Any Health Care Component that receives a request for communications by alternative means or at alternative locations should provide the patient with the form attached hereto as Form-07. If a patient indicates that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request should immediately forward a copy of the request to the Privacy Official who will coordinate the processing of the request with the other University Health Care

Components designated by the patient. If the patient does not request an alternative means of communication from any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form and the denial form, if applicable, to the Privacy Official.

3. Health Care Components should designate an individual or individuals who will be responsible for determining if a particular request for alternative means of communication is reasonable in light of the expense and administrative burden involved with complying with the request. Questions regarding the reasonableness of a particular request should be forwarded to the Privacy Official.

4. Health Care Components should, if possible, notify the patient making the request in writing at the time of his/her visit if the request is denied by providing the patient with a copy of the form attached hereto as Form-07 with the reason for the denial noted. If the patient cannot be notified of the denial at the time of his/her visit, the form for requesting an alternative means of communication, with the denial noted, should be sent to the patient. **In order to protect the patient, the denial should be sent to the alternative address, if specified.**

5. Requests for alternative means of communication, and documentation of any denials of such requests, should be maintained in a patient's medical record for a minimum of six (6) years.

6. Health Care Components must ensure that agreed upon alternative means of communication are communicated to the billing department and other departments and providers and business associates who may be sending the patient communications on behalf of the Health Care Provider who agreed to the request.

7. If a request for communication by alternative means is granted, a Health Care Component must place or affix a clear indication of the communication by alternative means on the patient's medical record, whether it be paper or electronic.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 44 (pg. 173).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82553, 82730 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Right to Amend Records	**Coverage:** Health Care Components
Policy #: Privacy-08 (Patient Rights)	**Page:** 1 of 3
HIPAA Section: 164.526(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To permit patients to request amendments to their protected health information.

II. POLICY

The University will permit patients to request amendments to their protected health information, or a particular record, contained in a designated record set.

The University may deny a patient's request for amendment, if it determines that the protected health information or record that is the subject of the request:

1. Was not created by University Personnel, unless the patient provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

2. Is not part of the designated record set;

3. Is not available for inspection by the individual pursuant to Privacy-05, Individual Access Policy;

4. Is accurate and complete.

Patients requesting an amendment to their protected health information must provide a reason to support a requested amendment.

III. PROCEDURE

1. Patients must request amendments to their protected health information in writing by using the form attached hereto as Form-08.A. Patients making their request for an amendment by telephone or e-mail should be forwarded a copy of the form. Verification of the requester's identity must be obtained prior to considering the amendment request. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a request for an amendment should provide the patient with the form attached hereto as Form-08.A. If a patient indicates that

he/she has been treated by more than one Health Care Component, the Health Care Component that received the request should immediately forward a copy of the request to the Privacy Official who will coordinate the processing of the request with the other University Health Care Components designated by the patient. If the patient does not request an amendment from any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form to the Privacy Official.

3. Health Care Components should designate an individual or individuals who will be responsible for processing a particular amendment request. The specific provider responsible for recording the protected health information or originating the record must be consulted, if possible, prior to making an amendment decision and should sign the amendment form.

4. Health Care Components must act on the patient's request, no later than sixty (60) days after receipt of a request, as set forth below:

a. Accepting the Amendment. If the Health Care Component accepts the requested amendment, in whole or in part, the Health Care Component must: (i) Make the appropriate amendment by identifying the records in the designated record set that are affected by the amendment and appending the amendment to such record; (ii) Inform the patient, in writing, that the amendment is accepted by sending the patient a copy of the form attached hereto as Form-08.A with the acceptance noted; (iii) Obtain the patient's identification of and agreement to have the Health Care Component notify the relevant persons with whom the amendment needs to be shared by using the form attached hereto as Form-08.B; and (iv) Make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the patient as having received protected health information about the patient and needing the amendment; and persons, including business associates, that the Health Care Component knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the patient.

b. Denying the Amendment. If the Health Care Component denies the requested amendment, in whole or in part, the Health Care Component must: (i) Inform the patient, in writing, that the amendment is denied by sending the patient a copy of the form attached hereto as Form-08.A; (ii) Permit the patient to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement; (iii) Identify, as appropriate, the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment, the Health Care Component's denial of the request, the patient's statement of disagreement, if any, and the Health Care Component's rebuttal, if any, to the designated record set. A Health Care Component may, but is not required to, prepare a written rebuttal to the patient's statement of disagreement. If a rebuttal statement is prepared, a copy of it must be provided to the patient who submitted the statement of disagreement.

5. If a statement of disagreement has been submitted by the patient, a Health Care Component must include the material set forth in subsection (iii) of the preceding paragraph, or, at the election of the Health Care Component, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement related.

6. If the patient has not submitted a written statement of disagreement, the Health Care Component must include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information **only if the patient has requested such action**.

7. A Health Care Component that is informed by another covered entity of an amendment to a patient's protected health information must amend the protected health information in designated record sets.

8. Requests for amendments, and documentation of the response to such requests, must be maintained in a patient's medical record for a minimum of six (6) years.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 46 (pg. 181).

2.HIPAA Privacy Regulations, 65 Fed. Reg. 82558, 82736 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Right to Request Restriction on Disclosures	**Coverage:** Health Care Components
Policy #: Privacy-09 (Patient Rights)	**Page:** 1 of 3
HIPAA Section: 164.522(a)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To permit patients to request certain restrictions on the use and disclosure of their protected health information.

II. POLICY

The University will permit patients to request restrictions on the use and disclosure of their protected health information: (a) to carry out treatment, payment or health care operations and/or (b) to people involved in their care or for notification purposes as described in § 164.510(b) of the Privacy Regulations. **However, the University is <u>not</u> required to agree to any request to restrict the use and disclosure of protected health information.**

If the University agrees to a restriction, it may not use or disclose protected health information in violation of the restriction, except in emergency situations when the protected health information is needed to treat the patient. If restricted protected health information is disclosed to a health care provider for emergency treatment, the Health Care Component disclosing the information must request that the health care provider that received the information not further use or disclose the information.

Any agreed to restriction will not be effective to prevent uses and disclosures to the patient or required by law.

The University must adhere to any agreed to restriction until the restriction is terminated according to the procedures set forth below.

University Personnel may not use or disclose protected health information subject to a restriction, except to provide emergency treatment or unless required by law.

III. PROCEDURE

1. Patients must request restrictions on the use and disclosure of their protected health information in writing by using the sample form attached hereto as Form-09. Patients making their restriction requests by telephone or e-mail should be forwarded a copy of the form. Verification of the requester's identity must be obtained prior to considering the request. The request form must be maintained in the patient's medical record for a minimum of six (6) years.

2. Any Health Care Component that receives a restriction request should provide the patient with the form attached hereto as Form-09. If a patient indicates that he/she has been treated by more than one Health Care Component, the Health Care Component that received the request should immediately forward a copy of the request to the Privacy Official who will coordinate the processing of the request with the other Health Care Components designated by the patient. If the patient does not request a restriction on the use of protected health information created or maintained by any other Health Care Components, the Health Care Component that received the initial request should process the request and send a copy of the request form to the Privacy Official.

Requests for restrictions should only be granted in rare instances in which the facts and circumstances indicate such a restriction is necessary to protect the patient.

3. The Privacy Official should be contacted prior to considering any restriction request.

4. Health Care Components should designate an individual or individuals who will be responsible for determining if a particular restriction will be permitted.

5. Health Care Components must notify the patient making the request in writing at the time of his/her visit if the request is denied by providing the patient with a copy of the form attached hereto as Form-09 with the reason for the denial noted. If the patient cannot be notified of the denial at the time of his/her visit, the form for requesting a restriction, with the denial noted, should be sent to the patient.

6. Requests for restrictions, and documentation of any denials of such requests, should be maintained in a patient's medical record for a minimum of six (6) years.

7. Health Care Components must ensure that agreed upon restrictions on the use and disclosure of protected health information are communicated to the billing department and other departments, providers and business associates who may be sending the patient communications on behalf of the University and/or Health Care Provider who agreed to the request.

8. A restriction on the use and disclosure of protected health information can be terminated if: (a) the patient requests the termination in writing; (b) the patient orally agrees to or requests the termination and the oral request or agreement is documented in the patient's medical record and communicated to the Privacy Official; or (c) the University and/or the Health Care Component informs the patient that it is terminating its

agreement to a restriction in which case the termination only will apply to protected health information created or received after the patient has been notified of the termination.

9. If a restriction request is granted, a Health Care Component must place or affix a clear indication of the restriction on the patient's medical record, whether it be paper or electronic.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 11 (pg. 96).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82552, 82726 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Privacy Official – Contact Information	**Coverage:** Health Care Components
Policy #: Privacy-10 (Admin.)	**Page:** 1 of 1
HIPAA Section: 164.530(a)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To provide for the designation of a Privacy Official and to set forth contact information as required by the Privacy Regulations.

II. POLICY

The Senior Vice President and Chief Administrative Officer of the University will designate a Privacy Official who is responsible for the development and implementation of the University's Privacy Policies for its Health Care Components and who will be responsible for answering questions regarding the content of the University's Privacy Policies and Notice of Privacy Practices. The Privacy Official also will be responsible for receiving complaints regarding compliance with the Policies and the Notice.

III. PROCEDURE

1. Documentation regarding the designation of the Privacy Official and his/her contact information must be retained, in written or electronic format, for at least six (6) years by the Privacy Official.

2. The contact information for the Privacy Official is set forth on Form-10 and will be revised in the event a new Privacy Official is designated or the contact information changes.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 48 and 49 (pg. 190-193).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82561, 82744-45 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Privacy Complaint Reporting and Tracking	**Coverage:** Health Care Components
Policy #: Privacy-11 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(d)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish the procedures for individuals to submit complaints regarding the University's Privacy Policies and the failure to comply with such Policies by the University's Health Care Components and/or University Personnel.

II. POLICY

All complaints regarding the University's Privacy Policies and compliance with such Policies, regardless of the form in which it was received, will be documented, reviewed, and acted upon, if necessary, by the University's Privacy Official.

Documentation regarding complaints received and the resolution of such complaints will be retained, in written or electronic format, for at least six (6) years.

III. PROCEDURE

1. Each Health Care Component must develop and implement a process for receiving privacy complaints and reporting them to the University's Privacy Official. Such process can be as simple as notifying employees that each individual submitting a privacy related complaint should be instructed to contact the University's Privacy Official. A sample complaint form is attached as Form-11. The contact information for the University's Privacy Official is located on Form-10. However, if a particular University Health Care Component would like to keep track of privacy complaints received for quality assurance purposes, the Health Care Component can develop an alternative process, as long such process involves the notification of the University's Privacy Official of each complaint received so that the Privacy Official can record and track the response to each complaint and can participate in the resolution of such complaints.

2. The Privacy Official will document each complaint received and maintain such documentation for the minimum retention period stated above.

3. The Privacy Official will investigate each complaint, in conjunction with the applicable Health Care Component and, if necessary, in conjunction with other affiliated

entities, and will document the resolution of the investigation and any corrective actions taken.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 52 (pg. 198).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82562, 82746-47 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Documentation	**Coverage:** Health Care Components
Policy #: Privacy-12 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(j)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish documentation requirements as required by the Privacy Regulations.

II. POLICY

The University will maintain, for at least six (6) years, the following:

a. Written or electronic copies of its Privacy Policies;

b. Written or electronic copies of any communication that is required by the Privacy Regulations to be in writing; and

c. Written or electronic records of any action, activity or designation that is required by the Privacy Regulations to be documented.

III. PROCEDURE

1. Documentation of Privacy Policies. Written or electronic copies of the University's Privacy Policies will be maintained by the Privacy Official for at least six (6) years from the date any such Policy or Policies were created or were last in effect, whichever is later.

2. Documentation of communications required by the Privacy Regulations. Such documentation will be retained for a period of at least six (6) years from the date of creation and will be maintained in the location specified in the particular Privacy Policy in which such communication is specifically addressed. For example: The policy addressing the right of patients to have access to their protected health information (Privacy-05) states that the Access Request Form must be maintained in a patient's medical record for a minimum of six (6) years.

3. Documentation of any action, activity or designation required by Privacy Regulations. Such documentation will be retained for a period of at least six (6) years from the date of creation and will be maintained in the location specified in the particular privacy Policy in which such action, activity or designation is specifically addressed. For example: The policy addressing the appointment of a Privacy Official (Privacy-10)

specifies that the designation of the Privacy Official will be maintained by the Privacy Official, in written or electronic format, for at least six (6) years.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 59 (pg. 211-212).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748–50 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Non-Retaliation	**Coverage:** Health Care Components
Policy #: Privacy-13 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(g)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To prohibit retaliation against individuals and others who exercise their rights under the Privacy Regulations.

II. POLICY

Neither the University, its Health Care Components, or University Personnel, will intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by the Privacy Regulations;

2. Individuals and Others. Any individual or other person for:

   a. Filing a complaint with the Secretary of the Department of Health and Human Services as permitted by the Privacy Regulations;

   b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by a government enforcement agency; or

   c. Opposing any act or practice made unlawful by the Privacy Regulations, 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 protected health information in violation of the Privacy Regulations or the University's Privacy Policies.

For purposes of this policy, the term "person" is not limited to natural persons, but includes any type of organization, association or group such as other covered entities, health oversight agencies, and advocacy groups.

III. PROCEDURE

1. Any person who believes that some form of retaliation is occurring, or has occurred, should report the incident to the Privacy Official.

2. If the Privacy Official receives a report of retaliation or intimidation, the Privacy Official will conduct an investigation to determine if retaliation has occurred. If the report is substantiated, sanctions will be imposed.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 55 (pg. 204-205).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Mitigation	**Coverage:** Health Care Components
Policy #: Privacy-14 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(f)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish procedures regarding the mitigation of harmful effects of inappropriate disclosures of protected health information.

II. POLICY

The University will mitigate, to the extent practicable, any harmful effect that is known to the University of a use or disclosure of protected health information in violation of the University's Privacy Policies or the Privacy Regulations by the University, one of its Health Care Components, University Personnel, or a business associate of the University.

III. PROCEDURE

1. Health Care Components must take all practicable steps to mitigate the harmful effects of a confirmed inappropriate use or disclosure. The type of mitigation that occurs will be based on the facts and circumstances of each case based on the following factors:

   a. knowledge of where the information has been disclosed;
   b. how the information might be used to cause harm to the patient or another individual; and
   c. what steps can actually have a mitigating effect under the facts and circumstances of any specific situation.

2. Health Care Components must investigate the cause of the inappropriate use and/or disclosure and take corrective actions to prevent such uses and/or disclosures from re-occurring.

3. Health Care Components should notify the Privacy Official of inappropriate uses and disclosures, the mitigation efforts and the results of the investigation. The Privacy Official will assist with the investigation and provide advice regarding mitigation efforts if requested to do so. If legal action is threatened, or is a distinct possibility, Legal Counsel must be notified.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 54 (pg. 202-203).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82562-63, 82747-48 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Amendment of Privacy Practices and Policies	**Coverage:** Health Care Components
Policy #: Privacy-15 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(i)(2)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To outline the requirements for changes to the University's Notice of Privacy Practices and amendment of its Privacy Policies.

II. POLICY

The University will promptly change its privacy practices and amend its Privacy Policies as necessary and appropriate to comply with changes in the law, including the Privacy Regulations, or to accommodate changes in the structure or operations of the University or its Health Care Components.

The University has reserved, in its Notice of Privacy Practices, the right to change its privacy practices and amend its Privacy Policies. Therefore, any such changes or amendments will be effective for protected health information created or received by the University or its Health Care Components prior to the effective date of the amendment.

III. PROCEDURE

1. Changes to Privacy Practices and Policies Addressed in the Notice of Privacy Practices. In order to effectuate changes to privacy practices and policies addressed in the Notice of Privacy Practices, the University will:

   a. Ensure that the Privacy Policies, if revised to reflect a change in the University's privacy practices, comply with the Privacy Regulations and applicable state laws that are not preempted.

   b. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.

   c. Revise the University's Notice of Privacy Practices as required by § 164.520(b)(3) of the Privacy Regulations to state the changed practice and make the revised Notice available as required by § 164.520(c) and Privacy-03. The University may not implement an amendment to a Privacy Policy addressed in the Notice of Privacy Practices prior to the effective date of the revised Notice.

2. Amendments to Privacy Policies Not Addressed in the Notice of Privacy Practices. The University may amend, at any time, a Privacy Policy that does not materially affect the content of its Notice of Privacy Practices. In order to effectuate such an amendment, the University will:

   a. Ensure that the Privacy Policy, as amended, complies with the Privacy Regulations; and

   b. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 58 (pg. 208-210).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82748-82750 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Waiver of Rights	**Coverage:** Health Care Components
Policy #: Privacy-16 (Admin.)	**Page:** 1 of 1
HIPAA Section: 164.530(h)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To prohibit requiring patients to waive their rights under the Privacy Regulations.

II. POLICY

The University will not require patients to waive: (a) their right to file a complaint with the Secretary of the Department of Health and Human Services or any other enforcement agency regarding the University's compliance with the Privacy Regulations or (b) any other rights under the Privacy Regulations as a condition of treatment or payment.

III. PROCEDURE

1. Any person with knowledge of a violation of this policy should report the incident to the Privacy Official.

2. If the Privacy Official receives a report of a violation of this policy, the Privacy Official will conduct an investigation to determine if a violation has occurred. If the report is substantiated, sanctions will be imposed pursuant to Privacy-19, Sanctions.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 56 (pg. 206).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82563, 82748 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Training	**Coverage:** Health Care Components
Policy #: Privacy-17 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(b)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish a method for providing training regarding the University's Privacy Policies.

II. POLICY

The University will train University Personnel associated with its Health Care Components regarding the Privacy Policies and the manner in which such Policies relate to their function within the University. Health Care Components can rely on training regarding the Privacy Regulations that volunteer faculty received from another Covered Entity as long as the volunteer faculty provides evidence of such training.

III. PROCEDURE

1. The University, through the Privacy Official, will designate the methods and manner in which training will be accomplished and will develop a Training Plan and Instructions. The Training Plan and Instructions will be attached to this Policy as Form-17.

2. Training materials must include some mechanism to demonstrate understanding of the information presented which must be completed according to the standards set forth in the Training Plan and Instructions in order for the training requirement to be satisfied.

3. It will be the responsibility of each Health Care Component, in coordination with the Privacy Official and/or Human Resources, to ensure that its employees receive training. Each Health Care Component will be solely responsible for training volunteers that provide assistance to them.

4. If required by the Training Plan and Instructions, a Privacy Training Coordinator, or Coordinators, will be designated by each Health Care Component to liaison with the Privacy Official and/or Human Resources to ensure that training is accomplished.

5. Training will be tracked by each Health Care Component. If required by the Training Plan and Instructions, the University's Human Resources and Student Admissions offices will provide periodic reports to the Privacy Official indicating the

names of new employees and students and the Health Care Component and department, if applicable, with which they will be associated.

6. Employees, volunteers and students must be trained no later than the compliance date of the Privacy Regulations.

7. After compliance date, employees, volunteers and students must receive some type of annual refresher training, as specified in the Training Plan and Instructions attached as Form 17.

8. After the compliance date of the Privacy Regulations, each new employee, volunteer and student must receive training within a reasonable period of time after the person becomes an employee, volunteer or student. The failure of an employee, volunteer or student to complete the required training within 30 days of becoming an employee, volunteer or student will be referred to Human Resources or the appropriate academic supervisor, and such failure to complete training will subject such employee, volunteer or student to sanctions within the applicable faculty, staff or student code.

9. Each employee, volunteer or student whose job or academic functions are affected by a material change in the University's Privacy Policies should receive training regarding the material change within a reasonable period of time after the change becomes effective.

10. Existing employees who fail to complete the training will be subject to sanctions pursuant to Privacy-19, Sanctions. Students who fail to complete training will be subject to sanctions under the Student Code of Conduct. Volunteers, including volunteer faculty, who fail to complete training, or provide evidence of training, whichever is applicable, will not be permitted to provide volunteer services to the University.

11. Documentation regarding training must be maintained by the Privacy Official, in written or electronic format, for at least six (6) years or for as long as required by other applicable University policies.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV.50 (pg. 194-195)

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82561, 82745 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: Safeguards	**Coverage:** Health Care Components
Policy #: Privacy-18 (Admin.)	**Page:** 1 of 5
HIPAA Section: 164.530(c)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish safeguards that must be implemented by the University's Health Care Components to protect the confidentiality of protected health information.

II. POLICY

The University, through its Health Care Components, will implement appropriate administrative, technical, and physical safeguards which will reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the University's Privacy Policies and/or the Privacy Regulations.

University Personnel must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

Health Care Components may not disclose PHI to other components of the University that are not designated Health Care Components without patient authorization. University Personnel who perform services for Health Care Components and other components of the University must not use or disclose PHI created or received in the course of or incident to their work for the Health Care Component to other components of the University and must use their best efforts to segregate the PHI.

Set forth below are policies establishing minimum administrative and physical standards regarding the protection of protected health information that each Health Care Component must enforce, if applicable. Health Care Components may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the protection of protected health information in light of the unique circumstances of a particular Health Care Component. The development and implementation of policies and procedures in addition to those stated herein must be approved by the University's Privacy Official.

Technical safeguards regarding the protection of Protected Health Information maintained in electronic form will be developed as part of the efforts to implement security best practices (and the HIPAA Security Regulations when they become effective) and will be incorporated into this Policy by reference.

1. Administrative Safeguards.

Oral Communications. University Personnel must exercise due care to avoid unnecessary disclosures of protected health information through oral communications. Conversations in public areas should be avoided, unless necessary to further patient care, research or teaching purposes. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary disclosures of protected health information. Patient identifying information only should be disclosed during oral conversations when necessary to further treatment, payment, teaching, research or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones only should be used in secure areas.

Cellular Telephones. Digital or landline telephones should be used if the conversation will involve the disclosure of Particularly Sensitive Health Information.

"Particularly Sensitive Health Information" means protected health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information. See Privacy-01, number 24.

Telephone Messages. Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested an alternative means of communication pursuant to Privacy-07, Communication by Alternative Means. However, each provider and/or clinic should limit the amount of protected health information that is disclosed in a telephone message. Telephone messages should never be left that include Particularly Sensitive Health Information. The content of appointment reminders should not reveal Particularly Sensitive Health Information, directly or indirectly. Telephone messages regarding test results or that contain information that links a patient's name to a particular medical condition should be avoided.

Faxes. The following procedures must be followed when faxing protected health information:

- Only the protected health information necessary to meet the requester's needs should be faxed.

- Particularly Sensitive Health Information should not be transmitted by fax, except in emergency situations or if required by a government agency. If Particularly Sensitive Health Information must be faxed, the recipient should be notified immediately

prior to the transmission and the sender should immediately confirm that the transmission was completed, if possible.

• Each Health Care Component should designate employees who can fax, or approve the faxing of, protected health information. Unauthorized employees, students and volunteers should never fax protected health information.

• Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing protected health information to third parties (including faxes to University departments that are not designated Health Care Components) for purposes other than treatment, payment or health care operations as provided in Privacy-23, Authorization. Protected health information may be faxed to an individual if the individual requests access to their own protected health information in accordance with Privacy-05, Patient Access to Protected Health Information.

• All faxes containing protected health information must be accompanied by a cover sheet that includes a confidentiality notice. A sample fax cover sheet is attached hereto as Form-18.

• Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be preprogrammed into fax machines or computers to avoid misdialing errors. Preprogrammed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.

• Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing protected health information should not be left sitting on or near the machine.

• Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.

• All instances of misdirected faxes containing protected health information should be investigated and mitigated pursuant to Privacy-14, Mitigation.

Mail. Protected health information should be mailed within the University in sealed envelopes. Protected health information mailed outside the University should go via first class mail and should be concealed. Appointment reminders may be mailed to a patient, unless the patient has requested an alternative means of communication pursuant to Privacy-07, Communication by Alternative Means.

Copying. Copies only should be made by authorized persons designated by a Health Care Component. Photocopying protected health information should be done only when necessary for treatment, payment or health care operations, when authorized by the patient or the patient's legal representative or when required by law. Photocopying of Particularly Sensitive Health Information should be strictly monitored. Protected health information should be reviewed on-site by internal auditors associated with the

University's Department of Internal Auditing when possible and should not be copied for convenience.

All copies provided to the patient or another third party in response to a request for access should be date stamped in a color other than black, or bear some other unique identifying mark or symbol, so that a copy can be distinguished from the original.

Date stamping or marking records provided to patients will protect the University in the event there is a dispute as to how certain records were acquired or disclosed.

Sign-in Sheets. Sign-in sheets in Health Care Components, departments or clinics which primarily see and treat patients with mental health, substance abuse, communicable disease, or other particularly sensitive conditions should structure the sign-in sheets in a manner so that subsequent signers cannot identify previous signers.

Destruction Standards. Protected health information must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing protected health information should be destroyed or shredded. Magnetic media and diskettes containing protected health information should be overwritten or reformatted.

2. Physical Safeguards.

Paper Records. Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access. Paper records and medical charts on desks, counters or treatment areas must be placed face down or concealed to avoid access by unauthorized persons. Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

Original paper records and medical charts should not be removed from University premises unless necessary to provide care or treatment to a patient or required by law. University employees should not remove paper records or medical charts for their own convenience. Any paper records and medical charts removed from University premises should be checked out according to any applicable Health Care Component policies and procedures and should be returned as quickly as possible. The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out or removed them.

Paper records and medical charts that are removed from University premises must not be left unattended in places in which unauthorized persons can gain access. Paper records and medical charts must not be left in unlocked automobiles or in view of passers-by.

The theft or loss of any paper record or medical chart should be reported to the Privacy Official and any person designated by a Health Care Component so that mitigation options can be considered.

Escorting Visitors and Patients. Visitors and patients must be appropriately monitored when on University premises where protected health information is located to ensure they do not access protected health information about other patients without permission.

This means that persons that are not employed by the University should not be in areas in which patients are being seen or treated or where PHI is stored without appropriate supervision. This includes pharmaceutical representatives and device salespeople.

Computer/Work Stations. Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. The screens on unattended computers must be returned to the main menu or at a password protected screen saver.

III. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 510 (pg. 196-197).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82561-62, 82745-46 (December 28, 2000).

Related polices:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: Sanctions	**Coverage:** Health Care Components
Policy #: Privacy-19 (Admin.)	**Page:** 1 of 2
HIPAA Section: 164.530(e)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish a process for imposing sanctions in the event the University's Privacy Policies are violated.

II. POLICY

The University will apply appropriate sanctions against University Personnel and its business associates who fail to comply with the University's Privacy Policies and/or the Privacy Regulations.

The University will not impose sanctions against University Personnel or business associate for: (a) engaging in whistleblower activities; (b) submitting a complaint to the Secretary of the Department of Health and Human Services; (c) participating in an investigation; or (d) registering opposition to a violation of the Privacy Regulations.

III. PROCEDURE

1. Employees. A violation of the University's Privacy Policies by faculty or staff will be subject to sanction. The sanction imposed for a violation of the Privacy Policies will depend on the severity of the violation and will be imposed in accordance with the University's Human Resources Manual or the Faculty Handbook, whichever is applicable.

2. Students. Students who violate the University's Privacy Policies will be subject to sanctions. The type of sanction imposed will depend on the severity of the violation. Sanctions will be imposed on students in accordance with the Georgetown University Code of Conduct.

3. Volunteers. Volunteers who materially violate the University's Privacy Policies will not be permitted to provide further assistance to the University as a volunteer.

4. Business Associates. If the University knows of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under his/her/its contract with the University, the University will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful: (a) terminate the contract, if feasible; or (b) report the problem to

the Secretary of the Department of Health and Human Services or other applicable government agency.

5. Documentation regarding any sanction imposed for a violation of the Privacy Policies should be retained in the sanctioned person's personnel or student file, whichever is applicable, in written or electronic format, for at least six (6) years. Copies of such documentation should be forwarded to the Privacy Official who also should maintain such documentation for the minimum retention period. Documentation of any sanction imposed against a business associate should be retained by the Privacy Official for the minimum retention period.

6. When imposing sanctions for the inappropriate use and disclosure of protected health information, consideration should be given to whether the use or disclosure was made as a result of (a) carelessness or negligence, (b) curiosity or concern, or (c) the desire for personal gain or malice.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 53 (pg. 200-201).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82562, 82747 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Uses and Disclosures - General	**Coverage:** Health Care Components
Policy #: Privacy-20 (Uses & Disclosures)	**Page:** 1 of 1
HIPAA Section: 164.502	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To set forth outline of required and permitted uses and disclosures.

II. POLICY

The University cannot use or disclose protected health information, except as permitted by the Privacy Regulations and these Policies.

Required Disclosures

The University will use or disclose protected health information: (a) to a patient, when requested under, and as required by Privacy-05, Patient Access to Protected Health Information, and Privacy-06, Accounting of Disclosures; and (b) when required by the Secretary of the Department of Health and Human Services to investigate the University's compliance with the Privacy Regulations.

Permitted Uses and Disclosures

The University, and University Personnel, are permitted to use or disclose protected health information as follows: (a) for treatment, payment or health care operations, as permitted by and in compliance with Privacy-22, Treatment, Payment and Health Care Operations; (b) incident to a use or disclosure otherwise permitted or required by the Privacy Regulations as long as the minimum necessary (Privacy-21) and safeguard (Privacy-18) policies have been followed; (c) pursuant to an authorization as permitted by Privacy-23, Authorization and Privacy-28, Marketing; (d) pursuant to an agreement under, or as otherwise permitted by Privacy-26, Disclosures to Family and Others Involved in Patient's Care and Privacy-33, Facility Directory; and (e) as permitted by and in compliance with Privacy-24, Mental Health Records; Privacy-25, Required by Law; Privacy-27, Business Associate; Privacy-29, Fundraising; Privacy-30, Research; and Privacy-31, Limited Data Set.

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Minimum Necessary Rule	**Coverage:** Health Care Components
Policy #: Privacy-21 (Uses & Disclosures)	**Page:** 1 of 3
HIPAA Section: 164.502(b) and 164.514(d)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To describe the application of the minimum necessary rule to uses, disclosure and requests for protected health information.

II. POLICY

University Personnel must make reasonable efforts to limit the Use, Disclosure of, and requests for protected health information to the *minimum necessary* to accomplish the intended purpose of the use, disclosure or request.

The minimum necessary rule does not apply to:

a. Disclosures to or requests by a Health Care Provider for treatment;
b. Uses or Disclosures made to the patient or his/her legal representative (See, Privacy-02, Personal Representatives, or Privacy-05, Patient Access to Protected Health Information.);
c. Uses or disclosures made pursuant to an authorization (See, Privacy-23, Authorization);
d. Disclosures made to the Secretary of the Department of Health and Human Services for compliance and enforcement of the Privacy Regulations;
e. Uses and Disclosures required by law (See, Privacy-25, Required by Law);
f. Uses and Disclosures required by compliance with HIPAA standardized transactions.

University Personnel may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose for the use, disclosure, or request.

Each Health Care Component must designate the University Personnel associated with that Health Care Component who need access to protected health information to carry out their duties **and** must designate the level of access needed and the conditions appropriate to such access.

III. PROCEDURE

1. The Role Based Access Worksheet, or similar form as approved by the Privacy Official, attached hereto as Form-21, must be completed for each employee and volunteer. The Health Care Component in which the employee works will be responsible for completing the Worksheet. A copy of the Worksheet must be sent to Human Resources. The original should be maintained by the Health Care Component.

University Personnel who are directly involved in a patient's treatment and care (e.g., physicians, clinicians, and nurses) may have access to all of the patient's protected health information. University Personnel who are not directly involved in a patient's treatment may not have unlimited access to a patient's protected health information. It is a violation of the minimum necessary rule for a health care provider to access the protected health information of protected health information of patients with whom the provider has no treatment relationship, unless for research purposes as permitted by the Privacy Regulations and these Policies.

2. The access granted to students must be determined on a case-by-case circumstance depending on the educational activity. A student's access must be determined by, and monitored by, the instructor.

Disclosures

3. Routine Disclosures: Health Care Components should implement standard protocols, when appropriate, to limit the protected health information disclosed on a routine or recurring basis. Copies of such protocols should be forwarded to the Privacy Official.

4. Non-Routine Disclosures: All non-routine disclosures (those that do not occur on a day-to-day basis as part of treatment, payment or health care operation activities or which are required by law on a regular basis) must be reviewed by the Office of University Counsel. When considering non-routine disclosures, the Office of University Counsel should consider the following criteria: (a) the purpose of the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the disclosure; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

University Personnel may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (a) making disclosures to public officials as required by law, if the public official represents that the information requested is minimum necessary for the stated purpose; (b) the information is requested by another covered entity; (c) the information is requested by a professional who is an employee of the University or is a business associate of the University providing professional services, if the professional or business associate represents that the information is the minimum necessary for the stated purpose(s); or (d) documentation submitted by a researcher that the information is preparatory to research, related to research on a decedent, or the disclosure has been approved by the IRB or Privacy Board.

Requests

5. Routine Requests: Health Care Components should implement standard protocols, when appropriate, to limit the protected health information requested on a routine or recurring basis. Copies of such protocols should be forwarded to the Privacy Official.

6. Non-Routine Requests: Each Health Care Component must designate who will be responsible for reviewing all non-routine requests (those that do not occur on a day-to-day basis as part of treatment, payment or health care operation activities). Any questions regarding the propriety of a particular request must be submitted to the Office of University Counsel. When considering non-routine disclosures, the following criteria must be considered: (a) the reason for the request; (b) any potential harm that would result to the patient, the University, or any other third party as a result of the request; (c) the relevancy of the information requested; and (d) other applicable state and federal laws and regulations.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 39 (pg. 154).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82712-82716 (December 28, 2000) and 67 Fed. Reg. 53195-53199 (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Treatment, Payment and Health Care Operations	**Coverage:** Health Care Components
Policy #: Privacy-22 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.506	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish consent requirements and permitted uses and disclosures for treatment, payment and health care operations.

II. POLICY

Due to ambiguities regarding consent requirements under local law and the Federal Education Rights Privacy Act ("FERPA"), which pertains to student records, Health Care Components must include language consenting to the use of a patient's protected health information for treatment, payment and health care operations purposes with the acknowledgement of receipt of the University's Notice of Privacy Practices. **The recommended consent language is set forth in Privacy-04, Notice of Privacy Practices.**

Health Care Components may use or disclose protected health information for their own treatment, payment or health care operations.

Health Care Components may disclose protected health information:

a. for treatment activities of another health care provider;

b. to another covered entity or a health care provider for the payment activities of the entity that receives the information; and

c. to another covered entity for **certain enumerated** health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the patient who is the subject of the protected health information being requested, the health information pertains to such relationship.

PHI can be exchanged between two covered entities for the following health care operations: (1) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; (2) population-based activities relating to improving health or reducing health care costs; (3) protocol development, (4) case management and care coordination; (5) contacting of health care providers and patients with information about treatment alternatives; (6) reviewing the competence or qualifications of health care professionals; (7) evaluating practitioner and provider performance; (8) conducting training programs in which students, trainees, or practitioners in areas of health care, learn under supervision to practice or improve their skills as health care providers; (9) training of non-health care professionals; and (10) accreditation, certification, licensing or credentialing activities.

Health Care Components that participate in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for **any** health care operations activities of the organized health care arrangement.

For uses and disclosures of a patient's protected health information other than for treatment, payment activities and health care operations of a Health Care Component or another health care provider, an authorization of the patient pursuant to Privacy-23 must be obtained unless disclosure pursuant to another Policy is permitted and/or required.

Except for limited circumstances if a record is covered by FERPA, a patient authorization is required for exchanges of PHI between Health Care Components and University departments that have <u>not</u> been designated as Health Care Components.

III. REFERENCES

1. HIPAA Privacy Regulations, 67 Fed. Reg. 53208-53219 (August 14, 2002).

<u>Related policies:</u>

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Authorization	**Coverage:** Health Care Components
Policy #: Privacy-23 (Uses & Disclosures)	**Page:** 1 of 3
HIPAA Section: 164.508	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish authorization requirements for uses and disclosures other than for treatment, payment and health care operations.

II. POLICY

Health Care Components cannot use or disclose protected health information, for purposes **other** than treatment, payment and health care operations, without a valid written authorization from the patient, except as otherwise permitted by these Policies. When a Health Care Component obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with the authorization.

Information released pursuant to this authorization may include alcohol and/or drug abuse records protected under federal and/or local law. Re-disclosure of such alcohol and/or drug abuse records by the recipient may require an additional specific authorization.

An authorization is required to disclose information to third parties for purposes other than treatment, payment or health care operations and for use by or disclosures to departments of the University that are not designated Health Care Components.

Psychotherapy Notes

University Personnel must obtain an authorization for any use or disclosure of psychotherapy notes, except in certain circumstances. See, Privacy-24, Mental Health Records.

Marketing

Health Care Components must obtain an authorization for any use or disclosure of protected health information for marketing, except in certain circumstances. See, Privacy-28, Marketing.

Conditioning of Authorizations

Generally, Health Care Components may not condition the provision of treatment to a patient on the provision of an authorization, except in the context of research involving treatment. See, Privacy-30, Research.

One exception to the prohibition on conditioning authorization relates to health care services provided at the request of a third party. For example, Health Care Components can require an authorization as a condition to providing a drug screening test or physical requested by an employer.

Revocation of Authorizations

Health Care Components must permit patients to revoke their authorizations, except to the extent the Health Care Component has taken action in reliance on the authorization.

III. PROCEDURES

1. A valid authorization must contain all of the elements required by the Privacy Regulations. A sample authorization form is attached hereto as Form-23**.**

2. Prior to using or disclosing protected health information pursuant to an authorization, University Personnel must review the authorization to determine if it is valid. An authorization is not valid, if it contains any of the following defects:

   a. the expiration date has passed or the expiration event is known to have occurred;
   b. the authorization has not been filled out completely,
   c. University Personnel have knowledge that the authorization has been revoked;
   d. University Personnel have knowledge that some material information in the authorization is false;
   e. the authorization was obtained by improperly conditioning treatment upon its receipt; or
   f. if the authorization is for psychotherapy notes, it is improperly combined with another type of authorization or document.

3. If a Health Care Component seeks an authorization from a patient for a use or disclosure of protected health information, the Health Care Component must provide the patient with a copy of the signed authorization.

4. Health Care Components must keep copies of authorizations for at least six (6) years.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 10 (pg. 90)

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82650-82662 (December 28, 2000) and 67 Fed. Reg. 53219-53226

3. 42 C.F.R. § 2.31.

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Mental Health Records	**Coverage:** Health Care Components
Policy #: Privacy-24 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.508	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish permitted uses and disclosures of mental health records, including psychotherapy notes.

II. POLICY

Mental Health Records – General

A patient generally has the right to access his/her mental health records **other than psychotherapy notes**. See, the definition of psychotherapy notes set forth in Privacy-01, number 33. A patient can be denied access to his/her mental health records for one of the reasons set forth in Privacy-05, Patient Access to Protected Health Information.

Remember: Psychotherapy notes have a very limited definition. They are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Mental health records, other than psychotherapy notes may be used and disclosed by University Personnel for treatment, payment and health care operations to the same extent, and subject to the same limitations, applicable to other types of protected health information as set forth in these Policies.

Persons or entities not covered by the Privacy Regulations who desire access to a patient's mental health records for purposes other than treatment, payment or health care operations must obtain an authorization as required by Privacy-23, Authorization, unless otherwise permitted by these Policies.

An authorization for the use or disclosure of psychotherapy notes cannot be combined with another authorization.

Psychotherapy Notes

A patient does not have a right to access psychotherapy notes relating to him/herself except (i) to the extent the patient's treatment professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access.

A patient authorization must be obtained for ***any*** use or disclosure of psychotherapy notes, except for the following purposes:

1. Use by the *originator* (the creator) of the psychotherapy notes for treatment purposes;

2. Use or disclosure of psychotherapy notes by University Personnel for conducting University-related training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;

3. Use by or disclosure to the Office of University Counsel to defend the University in a legal action or other proceeding brought by the patient;

4. Use or disclosure of psychotherapy notes to the Secretary of Health and Human Services, or any other officer or employee of the Department of Health and Human Services to whom the authority has been delegated, to conduct enforcement activities;

5. Use or disclosure needed for oversight of University Personnel who created the psychotherapy notes;

6. Use or disclosure needed by a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or

7. When University Personnel, in good faith, believe 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.

The Privacy Regulations do not permit a health plan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining a patient's authorization to use or disclose psychotherapy notes.

III. REFERENCES

1. HIPAA Privacy Regulations, 65 Fed. Reg. 82652-82655 (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Required by Law	**Coverage:** Health Care Components
Policy #: Privacy-25 (Uses & Disclosures)	**Page:** 1 of 8
HIPAA Section: 164.512	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To set forth requirements pertaining to uses and disclosures required by law.

II. POLICY

University Personnel may disclose protected health information without the patient's consent, authorization or the opportunity to agree or object as required by applicable state and federal laws, including those listed below.

Questions regarding whether a particular use or disclosure is required by law must be submitted to the Office of University Counsel.

III. PROCEDURE

1. Abuse or Neglect of Children.

a. Reporting Child Abuse or Neglect. All University Personnel who have reason to believe that a child under the age of 18 is a victim of abuse or neglect must promptly notify the Department of Public Safety/Metropolitan Police Department of the District of Columbia or the Child Protective Services Division of the Department of Human Services of the District of Columbia. Health Care Components may establish procedures for facilitating and coordinating reporting requirements.

"Abuse" for purposes of this section means harm or threatened harm to the child's health, safety or welfare by a parent, legal guardian, custodian, foster parent, adult residing in the home of the child, the owner, operator, or employee of a child care facility, or an agent or employee of a private residential home, institution, facility or day treatment program.

"Neglect" for purposes of this section means a failure to provide (i) adequate food, clothing, shelter, medical care, and supervision; (ii) special care

which is necessary because of the physical or mental condition of the child; or (iii) abandonment.

Reports of abuse or neglect may be made by telephone, in writing, or in person. A written record of each such report and the circumstances surrounding such report shall be maintained by the Health Care Component making the report. The report must contain the following:

- The names and addresses of the child and the child's parents or other persons responsible for the child's health, safety or welfare;
- The child's age;
- The nature and extent of the abuse or neglect, including any evidence of previous injuries; and
- Any other information that may be helpful in establishing the cause of the injuries and the identity of the person or persons responsible.

Health Care Components must also provide copies of the results of the examination or copies of the examination on which the report was based and any other clinical notes, x-rays, photographs, and other previous or current records relevant to the case to law enforcement officers conducting a criminal investigation into the case and to employees of the Child Protective Services Division conducting an investigation of alleged abuse or neglect in the case, upon written verification by the applicable agency of a pending investigation.

b. Reporting Criminally Inflicted Injuries. University Personnel examining, attending, or treating a child suffering from what appears to be criminally injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury or death, or child physical or sexual abuse, shall promptly report the matter to the local police department. The report may require the disclosure of protected health information relevant to the investigation. Health Care Components may establish procedures for facilitating and coordinating reporting requirements.

c. Notification. To the extent a report is made pursuant to this provision, University Personnel must promptly notify the personal representative of the child who is the subject of the report, unless University Personnel, in the exercise of professional judgment, believes such personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the child.

2. Adult Victims of Abuse, Neglect, Domestic Violence or Criminally Injurious Conduct.

a. Abuse, Neglect and Domestic Violence. University Personnel who have reasonable cause to believe that a Vulnerable Adult is suffering from abuse, neglect, or exploitation shall promptly report the matter to the Department of Public Safety, who shall confer with the Office of University Counsel as to the required reporting obligations under the law of the District of Columbia.

A "Vulnerable Adult" is a patient who is incapacitated or who, because of physical or mental disability, incapacity, or other disability, is substantially impaired in the ability to provide adequately for the care or custody of him or herself, is unable to manage his or her property and financial affairs effectively, is unable to meet essential requirements for mental or physical health or safety, or is unable to protect him or herself from abuse, neglect, or exploitation without assistance from others.

"Abuse" for purposes of this section means causing or permitting: (i) the infliction of physical pain, injury, sexual abuse, sexual exploitation, unreasonable restraint or confinement, or mental anguish, or (ii) the deprivation of nutrition, clothing, shelter, health care, or other care or services without which serious physical or mental injury is likely to occur to a Vulnerable Adult by a caretaker or other person providing services to a Vulnerable Adult.

"Neglect" for purposes of this section means: (i) the failure to provide protection for a Vulnerable Adult who is unable to protect his or her own interest; (ii) the failure to provide a Vulnerable Adult with adequate shelter, nutrition, health care, or clothing; or (iii) the causing or permitting of harm or the risk of harm to a Vulnerable Adult through the action, inaction, or lack of supervision by a caretaker providing direct services.

The report must contain the name and address of the Vulnerable Adult, the name and address of the caretaker, if any, and a description of the current location and current condition of the Vulnerable Adult and of the situation which may constitute abuse, neglect or exploitation of the Vulnerable Adult.

b. Reporting Criminally Inflicted Injuries. Any University Personnel examining, attending, or treating a patient of what appears to be criminally injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury or death, shall promptly report the matter to the Department of Public Safety/local police department. The report may require the disclosure of protected health information relevant to the investigation. Health Care Components may establish procedures for facilitating and coordinating reporting requirements.

c. Notification. To the extent a report is made pursuant to this provision, University Personnel must promptly notify the personal representative of the child who is the subject of the report, unless University Personnel, in the exercise of professional judgment, believes such personal representative is responsible for the

abuse, neglect or other injury, and that informing such person would not be in the best interests of the victim.

3. Court Orders. A court order is a direction of the court which directs a party to produce certain specified documents. Upon the receipt of a court order requesting the disclosure of medical records containing protected health information and meeting all legal requirements, University Personnel or the recipient of the order must immediately forward the court order to the Office of University Counsel. Upon determining that the court order is valid and meets all legal requirements, the University should release the information pursuant to the court order. The patient whose records are being requested is not required to provide an authorization to disclose the records pursuant to a court order.

4. Subpoenas. A subpoena is a unilateral request of a party for the production of documents. A subpoena is not generally approved by a judge. Therefore, it is important for the University to determine whether the patient's authorization or a court order is required for the release.

Upon receipt of a subpoena, University Personnel or the recipient of the subpoena must immediately forward the subpoena to the Office of University Counsel to determine if PHI can be released pursuant to the subpoena.

5. Other Disclosures to Law Enforcement Officials.

a. Certain limited protected health information may be disclosed regarding a patient to a law enforcement official who requests such information to identify or locate a suspect, fugitive, material witness, or missing person. Absent a request, such information may not be disclosed. A request may be made orally or in writing and may include a general request seeking the public's assistance in identifying a suspect, fugitive, material witness, or missing person. A "law enforcement official" means an officer or employee of any agency or authority of the United States, State, Indian tribe, county, city, town or municipality, who is empowered by law to (i) investigate or conduct an official inquiry into a potential violation of law; or (ii) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

If a request is made by a law enforcement official for a patient's protected health information, the Office of University Counsel shall be immediately contacted to authenticate the request for disclosure and to determine whether the official is authorized to make such a request. Upon determining if the request is valid, the Office of University Counsel shall direct the appropriate person(s) to provide the limited information set forth below.

The disclosure of protected health insurance pursuant to this section**,** is limited only to the following:

- Name and address
- Date and place of birth
- Social security number
- ABO, blood type and rh factor
- Type of injury, if applicable
- Date and time of treatment
- Date and time of death, if applicable
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

Do not disclose any of the following information: DNA data and analyses, dental records, or typing samples or analyses of tissues or bodily fluids other than blood.

b. The University may disclose protected health information to law enforcement officials pursuant to an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by Federal, State or local law, so long as (i) the information sought is relevant and material to a legitimate law enforcement inquiry; (ii) the request is specific and limited in scope to the extent reasonably possible; and (iii) de-identified information cannot be reasonably used. University Personnel should consult with the Office of University Counsel before making any disclosures pursuant to this provision.

c. In addition to other disclosures regarding potential victims of a crime discussed in this policy, the University may disclose to law enforcement officials information about a patient who is suspected to be a victim of a crime, if (i) the patient consents to the disclosure; or (ii) if the patient is unable to provide consent, all of the following requirements are met: (a) the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the patient has occurred, and such information is not intended to be used against the patient and that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the patient is able to consent; and (b) the disclosure is in the best interest of the patient as determined by University Personnel, in the exercise of professional judgment. University Personnel should consult with the Office of University Counsel before making any disclosures pursuant to this provision.

d. The University may disclose to a law enforcement official PHI that University Personnel believe in good faith constitutes evidence of criminal conduct that occurred on University property. University Personnel should consult with the Office of University Counsel before making any disclosures pursuant to this provision.

e. University Personnel providing emergency health care in response to a medical emergency, other than an emergency on University property, may disclose PHI to a law enforcement official if the disclosure appears necessary to alert law enforcement to: (i) the commission and nature of a crime; (ii) the location of such crime or that of the victim(s) of such crime; and (iii) the identity, description, and location of the perpetrator of such crime. University Personnel should consult with the Office of University Counsel before making any disclosures pursuant to this provision.

6. Uses or Disclosures to Avert Serious Threats to Health and Safety. University Personnel may, consistent with applicable law and ethical standards, use or disclose protected health information if University Personnel, in good faith, believe such use and disclosure (i) is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or (ii) is necessary for law enforcement authorities to identify or apprehend an individual who (a) has made a statement admitting participation in a violent crime that University Personnel reasonably believes may have caused serious physical harm to the victim (provided that no disclosure may be made under this circumstance if the disclosure is made during the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or actual counseling or therapy, or if the disclosure is made during a request to initiate such treatment); or (b) escaped from a correctional institution or from lawful custody. The Office of University Counsel should be consulted before any disclosures of PHI are made pursuant to this Section.

7. Uses and Disclosures for Special Government Functions.

a. The University may use and disclose protected health information of patients in the United States and foreign armed forces for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The Office of University Counsel should be consulted to confirm that the requirements of this disclosure are met.

b. The University may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act, and to protect the President of the United States and certain other public officials as authorized by law. The Office of University Counsel should be consulted to confirm that the requirements of this disclosure are met.

c. The University may disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual, and the correctional institution or law enforcement official may use protected health information about such individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for: (i) the provision of health care to such individuals; (ii) the health and safety of such individual or other inmates; (iii) the health and safety of the officers or employees of or others at the correctional institution or other persons responsible for the transporting of inmates; (iv) law enforcement on the premises of the

correctional institution; and/or (v) the administration and maintenance of the safety, security, and good order of the correctional institution. The Office of University Counsel should be consulted to confirm that the requirements of this disclosure are met.

8. Public Health. University Personnel may disclose protected health information without the written authorization of the patient to the appropriate state or federal health authority conducting public health surveillance, public health investigations, public health interventions and the Food and Drug Administration regulatory oversight. Such permitted disclosures shall specifically include the following:

a. Statistical Reports. The Registrar appointed by the Director of the Department of Human Services is charged with tracking health information within the District of Columbia. The Department may request University Personnel to provide to the Registrar certain health care information for the purpose of statistical and other similar reports. The University may disclose the requested information without the patient's written authorization. This includes discharge data including, but not limited to, complete discharge data sets or comparable information for each patient discharged.

The Office of University Counsel must be notified upon the receipt of a request from the Registrar for such information to ensure appropriate reporting. The release of information must be limited to that information which is specified in the request.

b. Birth Certificates. If a birth occurs in a University facility, a birth certificate must be prepared and filed by one of the following University Personnel in the indicated order of priority:

- The physician in attendance at or immediately after the birth; or
- Any other person in attendance at or immediately after the birth.

This University Personnel must obtain the personal data, prepare the certificate, secure the signatures required by the certificate and file the certificate with the local registrar. The physician in attendance must certify to the facts of birth and provide the medical information required by the certificate within five (5) days after the birth. No patient authorization is necessary to disclose the information used to prepare and file the birth certificate.

c. Death Certificates. A death certificate for each death which occurs in the District of Columbia must be filed with the local registrar of the district in which the death occurred, within five (5) days after the death and prior to the disposition of the body. The University Personnel responsible for the patient's care or the medical examiner must then complete and sign the certificate of death within forty-eight (48) hours after death. If the University Personnel in charge of the patient's care is not in attendance at the time of the death, the medical certificate must be completed and signed within forty-eight (48) hours after death by other University Personnel in attendance at the time of death. In this instance, the

alternative physician must note on the face of the certificate, the name of the attending physician and that the information shown is only as reported.

The authorization of the patient's personal representative is not required to disclose information necessary to complete the certificate of death for filing.

d. Other reportable events. The University will not be required to seek an authorization from a patient for such other mandatory disclosures of information as may be enacted from time to time.

9. Workers' Compensation. Under the laws of the District of Columbia, an employer must provide to an injured employee medical, surgical or other attendance or treatment, nurse and hospital service, medicine, crutches, and apparatus as may be necessary after an injury which occurred during the course of his employment.

The Workers' Compensation Act contemplated that an employee who participates in the benefits of this Act is deemed to consent to the treating physician in making these reports. Thus, the patient authorization is not required. However, uses and disclosures made under this section must be limited only to that protected health information which is relevant to the injury for which benefits are sought.

Related Policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Disclosures to Family and Others Involved in Patient's Care	**Coverage:** Health Care Components
Policy #: Privacy-26 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.510(b)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To articulate conditions under which family and friends can be notified of patient's condition.

II. POLICY

University Personnel may disclose protected health information to a patient's family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, as long as the protected health information disclosed is **relevant** to the person's involvement with the patient's care or payment related to the patient's health care.

University Personnel may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the patient, or another person responsible for the care of the patient of the individual's location, general condition, or death.

University Personnel may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The protected health information that may be released is limited to the individual's location, general condition, or death.

III. PROCEDURES

1. Patient is Present – If the patient is present for, or otherwise available prior to, a use or disclosure to a family member or friend as described above and has the capacity to make health care decisions, University Personnel may use or disclose the protected health information if he/she:

   a. Obtains the patient's agreement and documents the agreement in the patient's medical record;

   b. Provides the patient with the opportunity to object to the disclosure, and the patient does not express an objection and documents the lack of objection in the patient's medical record; or

c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.

2. Patient is **not** Present – If the patient is not present, or the opportunity to agree or object to the use of disclosure cannot practicably be provided because of the patient's incapacity or an emergency circumstance, University Personnel may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the patient and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the patient's health care.

University Personnel may use professional judgment and his/her experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

3. The following criteria should be considered when determining whether it is in the patient's best interest to disclose the protected health information to a family member or friend:

a. Whether the potential disclosure is common practice;

b. The nature of the relationship between the parties;

c. The sensitive nature of the information being disclosed;

d. The ability of the patient to manage necessary tasks (i.e., pick up prescriptions, medical supplies, x-rays, or other forms of protected health information); and

e. Whether the incapacitated patient is a suspected victim of domestic violence and whether the person seeking information about the patient may have abused the patient. In these instances University Personnel should not disclose information to the suspected abuser if there is reason to believe that such a disclosure could cause the patient harm.

4. University Personnel are not required to verify the relationship of relatives or other individuals involved in the patient's care. University Personnel may simply inquire into the individual's relationship with the patient. The patient's act of involving the other person in his/her care also may suffice as verification of their identity.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 23 (pg. 119).

2. HIPAA Privacy Regulations, 45 C.F.R.§164.510.

Related policies:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: Business Associates	**Coverage:** Health Care Components
Policy #: Privacy-27 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.502(e), 164.504(e) and 164.532	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish requirements regarding uses and disclosures of protected health information to business associates.

II. POLICY

A Health Care Component may disclose protected health information to a business associate, and may allow a business associate to create or receive protected health information on its behalf, if the Health Care Component ensures that the University has executed an agreement with the business associate which contains language requiring the business associate to appropriately safeguard the protected health information.

A Business Associate is a person or entity who provides certain functions, activities, or services on behalf of the University, that involves the use and/or disclosure of protected health information. See, the Business Associate Decision Tree attached hereto as Form-27.

If the University or a Health Care Component knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under the business associate agreement, the University and/or the Health Care Component must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the business associate agreement must be terminated or, if termination is not possible, the problem with the Business Associate must be reported to the Secretary of the Department of Health and Human Services.

III. PROCEDURE

1. The University's Office of University Counsel will be responsible for drafting and implementing the appropriate business associate language and/or agreements. All contracts must be reviewed in accordance with University policies. Questions regarding the status of a vendor or independent contract should be forwarded to the Office of University Counsel.

2. Health Care Components must identify Business Associates and bring the need for contractual language to the attention of the Office of University Counsel.

The business associate language must be included in new or renewing contracts. The University has until April 14, 2004 to include the appropriate language into existing agreements.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 03 and .16 (pg. 70 and 108).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82475-76, 82499 (December 28, 2000) and 67 Fed. Reg. 53248-53254 and 53264-53266 (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Marketing	**Coverage:** Health Care Components
Policy #: Privacy-28 (Uses & Disclosures)	**Page:** 1 of 1
HIPAA Section: 164.508(a)(3)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish requirements pertaining to the use and disclosure of protected health information for marketing purposes.

II. POLICY

Health Care Components must obtain an authorization for any use or disclosure of protected health information for marketing, **except** if the communication is in the form of: (a) a face-to-face communication made by University Personnel to an individual; or (b) a promotional gift of nominal value provided by the Health Care Component. See, Privacy-23, Authorization, for the requirements of a valid authorization.

"Marketing" does not include communications about medical services or products provided by the University or one of its Health Care Components.

If the marketing involves direct or indirect payment to the University or a Health Care Component from a third party, the authorization must state that payment is involved.

University Personnel are prohibited from selling patient lists to third parties, or from disclosing protected health information to a third party for the independent marketing activities of the third party, without obtaining an authorization from every patient on the list.

III. PROCEDURE

Authorizations for marketing should be kept in a patient's medical record for at least six (6) years from the date it was signed.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 24 (pg. 121).

2. HIPAA Privacy Regulations, 65 Fed. Reg. (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Fundraising	**Coverage:** Health Care Components
Policy #: Privacy-29 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.514(f)(1)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish requirements pertaining to the use and disclosure of protected health information for fundraising purposes.

II. POLICY

Health Care Components may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization: (a) demographic information relating to an individual; and (b) dates of health care provided to an individual.

Any use or disclosure for fundraising purposes beyond demographic information requires the patient's authorization. Demographic information includes the patient's name, address, age and gender. It does not include the use or disclosure of any information about a patient's illness or treatment. See, Privacy-23, Authorization, for requirements of a valid authorization.

A patient's demographic information and dates of receipt of health care services may not be used or disclosed without the patient's authorization for fundraising purposes unless the following requirements are met:

1. The University's Privacy Notice must contain a statement that the University may contact the patient to raise money for the University; and

2. The Privacy Notice and all fundraising materials must describe the procedures for a patient to opt out of receiving any additional fundraising communications.

III. PROCEDURE

1. All fundraising materials directed to patients, as well as the Notice of Privacy Practices, must indicate that a patient can opt out of receiving fundraising materials from the University, or a Business Associate or related foundation on the University's behalf, by sending a letter or e-mail to the University's Privacy Official.

2. The University's Health Care Components must get the approval of the Privacy Official prior to initiating any fundraising campaigns directed at patients of the Health Care Components to ensure patients are not solicited who have indicated that they do not want to receive fundraising materials.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 25 (pg. 123).

2. HIPAA Privacy Regulations, 65 Fed. Reg. (December 28, 2000) and 67 Fed. Reg. (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Research	**Coverage:** Health Care Components
Policy #: Privacy-30 (Uses & Disclosures)	**Page:** 1 of 1
HIPAA Section:	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To require that the University conduct human subject research in accordance with applicable HIPAA requirements.

II. POLICY

All research based, in whole or in part, on PHI, whether obtained initially from a University Health Care Component or another entity subject to HIPAA shall be in compliance with the requirements of the covered entity from which PHI was obtained.

III. PROCEDURES

With regard to PHI obtained from MedStar, the University IRBs will follow the procedures of, and adapt the forms contained on the MedStar HIPAA website, www.medstarresearch.org/departments/orp/HIPAA/hipaaintro.htm.

With regard to PHI obtained from a University Health Care Component, the adapted MedStar procedures and forms shall be utilized.

With regard to PHI obtained from a non-MedStar or University Health Care Component source, guidance shall be sought from the University's IRB coordinator of the University's Director of Research Compliance.

Related policies:

See: http://www.georgetown.edu/grad/IRB/

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: Limited Data Sets	**Coverage:** Health Care Components
Policy #: Privacy-31 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.514(e)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish permitted uses of limited data sets and the method for creating them.

II. POLICY

A Health Care Component may use and disclose a limited data set without patient authorization only for the purposes of research, public health or health care operations if the Health Care Component enters into a data use agreement with the intended recipient of the limited data set.

A Health Care Component may use protected health information to create a limited data set, or disclose protected health information to a business associate to create a limited data set on behalf of the Health Care Component.

If a Health Care Component knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or end the violation, as applicable. If such steps are unsuccessful, the Health Care Component must discontinue disclosure of protected health information to the recipient and report the problem to the Secretary of the Department of Health and Human Services.

A limited data set is protected health information that does not directly identify the patient, but which contains certain potentially identifying information.

III. PROCEDURE

1. Limited Data Set. In order to create a limited data set, the following direct identifiers of the patient or of relatives, employers or household members of the patient must be removed:

a. Names
b. Postal address information, other than town, city, state, and zip codes
c. Telephone numbers
d. Fax numbers
e. Electronic mail addresses

f. Social security numbers
g. Medical record numbers
h. Health plan beneficiary numbers
i. Account numbers
j. Certificate/license numbers
k. Vehicle identifiers and serial numbers, including license plate numbers
l. Device identifiers and serial numbers
m. Web Universal Resource Locators (URLs)
n. Internet Protocol (IP) address numbers
o. Biometric identifiers, including finger and voiceprints
p. Full-face photographs and comparable images

The patient's birth date should only be disclosed if the University and the recipient of the information agree that it is needed for their purpose.

2. Data Use Agreements. All data use agreements must be approved by the Office of University Counsel prior to execution. A Data Use Agreement must:

a. Establish the permitted uses and disclosures of the limited data set.

b. Establish who is permitted to use or receive the limited data set.

c. Provide that the recipient of the information will:

- Not use or further disclose the information other than as permitted by the agreement
- Use appropriate safeguards to prevent use or disclosure other than as permitted by the agreement
- Report to the University any uses or disclosures the recipient is aware of that is not provided for by the agreement
- Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient
- Not identify the information or contact the patients

IV. REFERENCES

1. HIPAA Privacy Regulations, 67 Fed. Reg. 53234, 53240 (August 14, 2002).

Related policies:

GEORGETOWN UNIVERSITY

HIPAA Privacy Policies

Subject: De-Identified Information	**Coverage:** Health Care Components
Policy #: Privacy-32 (Uses & Disclosures)	**Page:** 1 of 3
HIPAA Section: 164.502(d) & 164.514(a)&(b)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish the method for de-identifying health information.

II. POLICY

De-Identified Information

Health Care Components can use and disclose de-identified health information without regard to the policies, as long as the code or other means of identification designed to permit re-identification is not disclosed.

Health Care Components may use protected health information to create information that is not individually identifiable health information or disclose protected health information to a Business Associate to de-identify health information on behalf of the Health Care Component. If de-identified information is re-identified, its use and disclosure becomes subject to regulation under the Policies.

Health information that does not identify the patient and in which there is no reasonable basis to believe that the health information can be used to identify the patient, or "de-identified information" is not considered protected health information and is not subject to the requirements of this Policy.

III. PROCEDURE

Health information can be de-identified by using one of the two methods listed below:

1. Safe Harbor. The following identifiers of the patient or of the relatives, employers, or household members of the patient are removed:

   a. Names

   b. Geographic subdivision, such as street address, city, county, and zip code

c. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and if it has fewer than 20,000 the zip code is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate).

d. All elements of dates (except year) for dates directly related to the patient, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age.

e. Telephone numbers

f. Fax Numbers

g. E-mail addresses

h. Social security numbers

i. Medical record numbers

j. Health plan beneficiary numbers

k. Account numbers

l. Certificate/license numbers

m. Vehicle identifiers, serial numbers, license plate numbers

n. Device identifiers and serial numbers

o. Web Universal Resource Locators (URLs)

p. Internet Protocol address numbers (IP)

q. Biometric identifiers, including finger and voiceprints

r. Full face photographic images and other comparable images

s. All other unique identifying number, characteristic, or code.

2. Alternative Method of De-Identification. A biostatician or some other person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, must apply such principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information. The person making this determination must document the methods and results of the analysis that justify the determination.

Re-Identification

A Health Care Component may assign a code or other means of record identification to allow de-identified information to be re-identified, provided that:

1. Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

2. Security. The code, and/or mechanism for re-identification, is not used or disclosed for any other purpose.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV-15 (pg. 107).

2. HIPAA Privacy Regulations, 65 Fed. Reg. 82499 (December 28, 2000).

Related policies:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: PDA's and Personal PC's	**Coverage:** Health Care Components
Policy #: Privacy-33 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.510(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To establish safeguards on the use of Portable Digital Assistants (PDA's) and other personal computers. This category includes both privately owned and University owned devices.

II. POLICY

University Personnel may use PDA's and personal computers for the collection, storage, and dissemination of PHI only when both are properly safeguarded to prevent an unauthorized disclosure. The University policies on confidentiality and security of information assets owned by or in the custody of University personnel apply regardless of the medium of data capture and/or storage. Use of a Portable Digital Assistant (PDA) or personal computer (PC), regardless of purchaser or ownership, does not alter the individual's responsibility to uphold the confidentiality of University data. Current technology makes portable devices 'at risk devices' with respect to security issues. Hence, the user assumes the responsibility for the physical control and security of the device and the information it stores.

III. PROCEDURES.

Definitions:

For the purposes of this policy, the following definitions apply:

Portable Digital Assistant (PDA): Include, but are not limited to, hand held devices (e.g. Palm, Handspring, Compaq, TRG, Pocket PCs, Tablet PCs), pen pads, cell phones and pagers that store data. Portable Digital Assistants are battery operated (though they may support direct connection to utility power), free-standing devices used for the purposes of data storage, retrieval, analysis and exchange.

Personal Computer (PC): Any desktop or notebook computer, whether owned by the university or by the individual, that is used by University Personnel and may not necessarily be located on the University's premises.

A. Security Requirements

1. All University Personnel are responsible for the protection from improper use or disclosure of all PHI contained on their PDAs and personal computers. Security of data maintained and stored on PCs and PDAs is subject to the provisions of relevant local, state and federal statutes and regulations, and the provisions of these HIPAA privacy policies.

2. Health Care Components must acknowledge that PDAs and/or personal PCs will be used by University Personnel, and incorporate specific training on the protection of PHI into their HIPAA training. This training plan must be include training on the "Security Procedures" below and be approved by the Privacy Official and Security Officer. .

B. Security Procedures

The following procedures must be included by a Health Care Component in their procedures and training about the use and storage of PHI:

1. PHI stored on PDAs and PCs shall be protected from unauthorized access through the use of effective and necessary measures. These shall include, but are not limited to the following:

a. Password protection

b. Encryption.

c. Personal PCs shall have up-to-date virus protection and scanning software.

d. Appropriate hardware or software firewall protection , if the PDA or Personal PC containing PHI is connected to the Internet via an "always on" broadband connection.

2. Prior to disposal or transfer to a new owner, all PHI on that device must be permanently destroyed unless the new owner has a right to access that PHI.

Related Policies:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: Use of E-Mail	**Coverage:** Health Care Components
Policy #: Privacy-34 (Uses & Disclosures)	**Page:** 1 of 4
HIPAA Section:	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To protect Patient Privacy should PHI be communicated via e-mail.

II. POLICY

The University's Health Care Components shall not use e-mail as a form of communication for messages containing PHI unless the communication is protected by appropriate security and other measures designed to protect patient privacy.

III. PROCEDURES

A. Prohibited Use of Electronic Mail

The following are some specific examples of prohibited usage of e-mail systems. This list is not to be considered all-inclusive. Further questions regarding appropriate use of electronic mail should be directed to the Georgetown University Privacy Official.

E-mail is not to be used for urgent or time-sensitive communications.

E-mail addresses are not to be used for marketing purposes except as described in the University marketing policy and as may be authorized by a patient.

B. General Procedures for Ensuring Confidentiality of All Electronic Mail Containing PHI, whether to patients or other recipients

Users of e-mail may have the capacity to forward, print and circulate any message. Therefore:

- Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

- PHI received or transmitted via electronic mail must be protected. Refer to the information security policies, the University's personnel policies regarding confidential information, and departmental requirements.

- Printers must be operated in a secure manner to protect information confidentiality in an area that is accessible to staff only and not to patients or visitors.

Basic e-mail communication systems are not inherently secure; mail sent via the Internet or other external systems can be intercepted and read by individuals other than the intended recipient. Even internal e-mail may make its way to the Internet. Therefore, when e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information. Specific safeguard measures are as follows:

a) The recipient address should be confirmed. Obtaining an email address from a directory is not proof that the email will go to the proper recipient. If the sender is unsure of the accuracy of the recipient's address, contact should first be made (by any means, including email) to confirm that the address is correct.

b) All electronic communications containing PHI **must be encrypted**. This can be accomplished by an approved encryption system and/or service (further questions regarding encryption should be directed to the Georgetown University Security Officer.) **If encryption is not available, then communications containing PHI cannot be sent via e-mail unless the Security Officer and Privacy Official approve the means proposed for protecting the security of the electronic communication.**

c) Additional security and confidentiality protections may be achieved on external networks by utilizing some form of authentication, e.g., user identification and password, digital signature, biometrics, etc., in conjunction with encryption methods to accomplish more secure transmission of electronic communication. Contact the Georgetown University Security Officer for details of authentication and encryption policies and procedures.

d) A notation referring to the confidential or sensitive nature of the information should be made in the subject line to further safeguard the confidentiality of electronically submitted data.

e) Use a banner at the top of each e-mail message stating: ``This is a CONFIDENTIAL medical communication. If you have received this e-mail in error please notify sender, do not read any further, and destroy."

f) PHI may be distributed to multiple recipients; however, the use of distribution lists is prohibited.

g) Double-check all address fields prior to sending messages, including ``to'', ``cc'', and ``bcc''.

C. Use of E-mail for Communicating with Patients

Obtain patient's written authorization for use of e-mail. Authorization forms, to be approved by the Security Officer and the Privacy Official should contain, at a minimum:

a) Itemized communication guidelines, e.g., establish turnaround time for messages (do not use e-mail for urgent matters), inform patients about privacy issues, establish types of transactions and categorize e-mail messages by transaction type, etc. (see sample communication guidelines.)

b) Instructions for when and how to escalate to phone calls and office visits.

c) Indemnification of the University for information loss due to technical failures.

d) Information that patient that e-mail communication is included as part of the medical record.

e) Instructions of use of e-mail option requesting read receipt.

D. Extended Absences

For extended absences, a clinician shall either forward email to another clinician at Georgetown University or have an autoreply message stating that the clinician cannot answer the email at this time and providing instruction on alternative methods of contacting Georgetown University. Even when a clinician has another Georgetown University employee access his/her email account (see A.3, above), the intended recipient or a designated provider with the appropriate credentials must handle any email sent from a patient that contains health information.

E. Documentation of E-mail

Electronic mail used in a clinical setting constitutes a form of progress note or encounter documentation. In the absence of an electronic patient record that allows inclusion of e-mail messages, each e-mail message should be printed in full and a copy and placed in the patient's paper record. Efficient archiving can be accomplished by:

a) Including the full text of the patient's query in the e-mail reply.

b) Copying (cc:) the reply to the sender.

c) Printing the sender's copy (which includes the initial message and reply) and file it in the patient record unless an acknowledgement is expected. When such an acknowledgement has been requested, e.g., when important medical advice has been given, the printed (chart) copy should not be filed until this confirmation is received.

Electronic mail used in a non-clinical setting containing PHI needs to be archived. Efficient archiving can be accomplished by:

a) Including the full text of the patient's query in the e-mail reply.

b) Copying (cc:) the reply to the sender.

c) Printing the sender's copy (which includes the initial message and reply) and filing it in the appropriate part of the designated record set. All e-mail correspondence will be retained in accordance to applicable record retention policy in a secure system.

Related policies:

GEORGETOWN UNIVERSITY
HIPAA Privacy Policies

Subject: Media	**Coverage:** Health Care Components
Policy #: Privacy-35 (Uses & Disclosures)	**Page:** 1 of 2
HIPAA Section: 164.510(a)	**Approved:**
Effective Date: April 12, 2003	**Revised:**

I. PURPOSE

To describe the circumstances under which patient information can be disclosed to the media.

II. POLICY

It is the policy of the University to ensure the privacy and security of PHI of patients and to ensure that release of PHI to the media is disclosed along the guidelines set forth in this policy and in the best interest of the patients served. Except under limited circumstances, it is the policy of the University not to release PHI to the media.

III. PROCEDURES

In General

1. All requests for patient PHI made by the media shall be forwarded to the Privacy Official for review and response.

2. The University may only respond to a request for specific patient information from the media when the inquiry specifically contains the patient's name, and the patient has specifically permitted the release of information.

3. The organization is not responsible for addressing inquiries that are made as a result of "public record." Matters of public record refer to situations that are reportable by law to public authorities, such as law enforcement agencies, the medical examiner/coroner or public health officer. Inquiries made from media citing access as a matter of public record should be referred to the appropriate public authority.

Disaster/Mass Casualty Situations

4. When appropriate in disaster or mass casualty situations, the University may release general information to the media to help dispel public anxiety.

5. The University shall select a spokesperson to handle media inquiries to restrict and control information shared with the public.

6. In disaster or mass casualty situations, the organization shall strive to work effectively with the media balancing the release of general information with privacy rights. A location may be provided for the media to be contained, so that information can be released in a press conference format that does not compromise patient privacy or the facility's need for added security in disaster situations.

References:

- "Guidelines for Releasing Information on the Condition of Patients," AHA Media Advisory, November, 2002.
- "Privacy/HIPAA Related Questions and Answers Pertaining to Release of PHI to News Reporters," Bricker & Eckler, LLP, Ohio State Medical Association, 2002.
- "Select a Spokesperson When Dealing With the Media," HCPRO, August 2002.

Related policies:

FORMS

FORM-04

HIPAA Document –
Retain for Minimum of 6 years

GEORGETOWN UNIVERSITY
NOTICE OF PRIVACY PRACTICES

***Effective Date*: _____**

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.

If you have any questions about this notice, please contact the Georgetown University Privacy Official, Georgetown University, 202 Healy Hall, 37th & O Streets, N.W., Washington, DC 20057-1246 (202) 687-6457, or by e-mail to _____.

WHO MUST FOLLOW THIS NOTICE:
This notice describes the privacy practices of the Georgetown University Health Care Components [Medicare Demonstration Project, ISIS, Counseling and Psychiatric Center (CAPS), Health Benefit Plans, and designated administrative offices.]

OUR OBLIGATIONS:
We are required by law to:

- Maintain the privacy of protected health information;
- Give you this notice of our legal duties and privacy practices regarding health information about you; and
- Follow the terms of our notice that is currently in effect.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION:
The following categories describe ways that we may use and disclose health information that identifies you ("Health Information"). Some of the categories include examples, but every type of use or disclosure of Health Information in a category is not listed. Except for the purposes described below, we will use and disclose Health Information only with your written permission. If you give us permission to use or disclose Health Information for a purpose not discussed in this notice, you may revoke that permission, in writing, at any time by contacting the University Privacy Official.

- ***For Treatment***. We may use Health Information to treat you or provide you with health care services. We may disclose Health Information to doctors, nurses, technicians, or other personnel, including people outside our facility who may be involved in your medical care. For example, we may tell your primary physician about the care we provided you or give Health Information to a specialist to provide you with additional services.

- ***For Payment***. We may use and disclose Health Information so that we or others may bill or receive payment from you, an insurance company or a third party for the treatment and services you received. For example, we may give your health plan information about your treatment so that they will pay for such treatment. We also may tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.

- ***For Health Care Operations***. We may use and disclose Health Information for health care operations purposes. These uses and disclosures are necessary to make sure that all of our patients receive quality care and for our operation and management purposes. For example, we may use Health Information to review the treatment and services we provide to ensure that the care you receive is of the highest quality.

- ***Appointment Reminders, Treatment Alternatives, and Health-Related Benefits and Services***. We may use and disclose Health Information to contact you as a reminder that you have an appointment with us. We also may use and disclose Health Information to tell you about treatment options or alternatives or health-related benefits and services that may be of interest to you.

- ***Fundraising Activities***. We may use Health Information to contact you in an effort to raise money. We may disclose Health Information to a related foundation or to our business associate so that they may contact you to raise money for us.

- ***Facility Directory***. We may list your name, general condition, and location in our directory. We may disclose this information to anyone who asks for you by name. We also may provide this information and your religious affiliation to members of the clergy.

- ***Individuals Involved in Your Care or Payment for Your Care***. We may release Health Information to a person who is involved in your medical care or helps pay for your care, such as a family member or friend. We also may notify your family about your location or general condition or disclose such information to an entity assisting in a disaster relief effort.

- ***Research***. Under certain circumstances, we may use and disclose Health Information for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication or treatment to those who received another, for the same condition. Before we use or disclose Health Information for research, though, the project will go through a special approval process. This process evaluates a proposed research project and its use of Health Information to balance the benefits of research with the need for privacy of Health Information. Even without special approval, we may permit researchers to look at records to help them identify patients who may be included in their research project or for other similar purposes, so long as they do not remove or take a copy of any Health Information.

SPECIAL CIRCUMSTANCES

- ***As Required by Law***. We will disclose Health Information when required to do so by international, federal, state or local law.

- ***To Avert a Serious Threat to Health or Safety***. We may use and disclose Health Information when necessary to prevent or lessen a serious threat to your health and safety or the health and safety of the public or another person. Any disclosure, however, will be to someone who may be able to help prevent the threat.

- ***Business Associates***. We may disclose Health Information to our business associates that perform functions on our behalf or provide us with services if the information is necessary for such functions or services. For example, we may use another company to perform billing services on our behalf. All of our business associates are obligated, under contract with us, to protect the privacy of your information and are not allowed to use or disclose any information other than as specified in our contract.

- ***Organ and Tissue Donation***. If you are an organ donor, we may release Health Information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary, to facilitate organ or tissue donation and transplantation.

- ***Military and Veterans***. If you are a member of the armed forces, we may release Health Information as required by military command authorities. We also may release Health Information to the appropriate foreign military authority if you are a member of a foreign military.

- ***Workers' Compensation***. We may release Health Information for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

- ***Public Health Risks***. We may disclose Health Information for public health activities. These activities generally include disclosures to prevent or control disease, injury or disability; report births and deaths; report child abuse or neglect; report reactions to medications or problems with products; notify people of recalls of products they may be using; track certain products and monitor their use and effectiveness; notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and conduct medical surveillance of the hospital in certain limited circumstances concerning workplace illness or injury. We also may release Health Information to an appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence; however, we will only release this information if you agree or when we are required or authorized by law.

- ***Health Oversight Activities***. We may disclose Health Information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

- ***Lawsuits and Disputes***. If you are involved in a lawsuit or a dispute, we may disclose Health Information in response to a court or administrative order. We also may disclose Health Information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

- ***Law Enforcement***. We may release Health Information if asked by a law enforcement official for the following reasons: (1) in response to a court order, subpoena, warrant, summons or similar process; (2) limited information to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement; (4) about a death we believe may be the result of criminal conduct; (5) about criminal conduct on our premises; and (6) in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description, or location of the person who committed the crime.

- ***Coroners, Medical Examiners and Funeral Directors***. We may release Health Information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We also may release Health Information to funeral directors as necessary for their duties.

- ***National Security and Intelligence Activities***. We may release Health Information to authorized federal officials for intelligence, counter-intelligence, and other national security activities authorized by law.

- ***Protective Services for the President and Others***. We may disclose Health Information to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

- ***Inmates or Individuals in Custody***. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release Health Information to the appropriate correctional institution or law enforcement official. This release would be made only if necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.

YOUR RIGHTS:

You have the following rights regarding Health Information we maintain about you:

- ***Right to Inspect and Copy***. You have the right to inspect and copy Health Information that may be used to make decisions about your care or payment for your care. To inspect and copy this Health Information, you must make your request, in writing, to the University Privacy Official.

- ***Right to Amend***. If you feel that Health Information we have is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for us. To request an amendment, you must make your request, in writing, to the University Privacy Official.

- ***Right to an Accounting of Disclosures***. You have the right to request an accounting of certain disclosures of Health Information we made. To request an accounting of disclosures, you must make your request, in writing, to the University Privacy Official.

- ***Right to Request Restrictions***. You have the right to request a restriction or limitation on the Health Information we use or disclose for treatment, payment, or

health care operations. In addition, you have the right to request a limit on the Health Information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not share information about your surgery with your spouse. To request a restriction, you must make your request, in writing, to the University Privacy Official. ***We are not required to agree to your request.*** If we agree, we will comply with your request unless we need to use the information in certain emergency treatment situations.

- ***Right to Request Confidential Communications***. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we contact you only by mail or at work. To request confidential communications, you must make your request, in writing, to the University Privacy Official. Your request must specify how or where you wish to be contacted. We will accommodate reasonable requests.

- ***Right to a Paper Copy of This Notice***. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice.

You may obtain a copy of this notice at our web site,
www.georgetown.edu/policies/hipaa

To obtain a paper copy of this notice, contact:

University Privacy Official
Georgetown University
202 Healy Hall, 37th & O Streets, N.W.
Washington, D.C. 200576

CHANGES TO THIS NOTICE:

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for Health Information we already have as well as any information we receive in the future. We will post a copy of the current notice at the hospital. The notice will contain the effective date on the first page, in the top right-hand corner.

COMPLAINTS:

If you believe your privacy rights have been violated, you may file a complaint with us or the Secretary of the Department of Health and Human Services. To file a complaint with us, contact the University Privacy Official. All complaints must be made in writing. You will not be penalized for filing a complaint**.**

FORM-05.A

HIPAA Document –
Retain for Minimum of 6 years

INDIVIDUAL'S REQUEST FOR PROTECTED HEALTH INFORMATION

NOTICE TO PATIENT: Your request for access to your protected health information **only** is applicable to the information maintained by Georgetown University. If you would like access to your protected health information maintained by any other Health Care Provider, a separate request must be submitted to that provider.

Name:_____ **Date of Birth**:_____

Address:_____
_____

Phone Number:_____

I hereby request access of the protected health information in my designated record set from _____ to _____ maintained or created by the following providers associated with Georgetown University:

Name of Physician or Other Provider	Department

I hereby request access to the following information maintained or created by the providers listed above: [Note: You will be charged $.25 per page for paper records and $5.00 per film for radiology films.]

☐ Lab Reports ☐ Radiology Reports

☐ Pathology Reports ☐ Patient History

☐ X-rays ☐ Entire Designated Record Set

☐ Billing Records ☐ Other_____

Information created or received from other providers (Specify which ones or "all")
_____

☐ I will pick up the copies of my records.

☐ Please mail copies of my records to:

☐ Myself ☐ Legal Representative

Address:_____
_____

Signature:_____ Date:_____
(of Patient or Legal Representative)

☐ Access granted or copy sent on (circle one):_____

FORM-05.B

HIPAA Document –
Retain for Minimum of 6 years

DENIAL OF INDIVIDUAL'S REQUEST FOR PROTECTED HEALTH INFORMATION

The request you submitted for access to your protected health information maintained in a designated record set by _____ has been **denied,** in whole or in part, for the reason indicated below:

☐ Information Not Available. We do not have the information you requested. The information you requested can be obtained from: _____. (*Alternative location will be indicated, if known.)*

☐ Legal Information. All, or a portion of, the information you requested has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

☐ Inmate Information. Releasing a **copy** to you would jeopardize the health, safety, security, or rehabilitation of you or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or who is responsible for your transportation.

☐ Research. As you agreed by signing a research participation consent form, your access to the protected health information created or obtained in the course of the research has been temporarily suspended. The suspension will last for as long as the research is in progress.

☐ Information from Other Source. The information you are requesting was obtained from someone under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

☐ Endangerment. A licensed health care professional has determined that the access you requested is reasonably likely to endanger the life or physical safety of you or another person. *You may request a review of a denial for this reason.*

☐ Reference to Other People. The information you requested makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person. *You may request a review of a denial for this reason.*

☐ Personal Representative. A licensed health care professional has determined that the provision of access to the information you requested is reasonably likely to cause substantial harm to the individual or another person. *You may request a review of a denial for this reason.*

☐ Psychotherapy Notes. Your treating health care provider has not approved the release of your psychotherapy notes.

Information that is not subject to one of the reasons for denial listed above will be provided to you as you requested.

Right to Review

If a right to review is available as indicated in the fifth, sixth, and seventh (5th, 6th, and 7th) reasons set forth above, you may request a review of the denial from the health care provider who denied your initial request. Your request will be reviewed by the manager of the Covered Health Component to which you submitted the request or another person designated by the clinic or provider within thirty (30) days after receiving the request for review. The determination of the manager will be final. You will be notified promptly, in writing, of the Medical Director's decision.

Complaints

You may file a complaint regarding the University's compliance with the HIPAA Privacy Regulations with the Secretary of the Department of Health and Human Services or any other agency that has been delegated the responsibility to enforce the Privacy Regulations. You may also submit a complaint to the University's Privacy Official by calling (202) 687-6457 or by sending an e-mail to hipaaprivacy@georgetown.edu, or by sending a written complaint to:

Georgetown University Privacy Official
202 Healy Hall
37th & Streets, N.W.
Washington, D.C. 20057-1246

Retain for minimum of 6 years.

FORM-06.A

REQUEST FOR ACCOUNTING OF DISCLOSURES

---------- ----------

Patient Name Patient Birth Date

Address where you want the accounting sent

NOTICE TO PATIENT: Your request for an accounting of disclosures of your protected health information **only** is applicable to the information maintained by Georgetown University. If you would like to request an accounting of disclosures of your protected health information maintained by any other Health Care Provider,, a separate request must be submitted to that provider.

REQUEST FOR ACCOUNTING OF DISCLOSURES:

I request an accounting of disclosures of the protected health information in my designated record set from _____ to _____ (not to exceed 6 years) maintained or created by the following providers associated with Georgetown University:

Name of Physician or Other Provider	Department

I understand that the first accounting in a twelve (12) months period is free of charge, but that I can be charged a reasonable fee for any additional accountings.

I understand that that the accounting must include all disclosures, **except** for disclosures:

1. to carry out treatment, payment and health care operations;
2. to individuals of protected health information about them;
3. incident to a use or disclosure permitted by the Privacy Regulations;
4. pursuant to the individual's authorization;
5. to persons involved in the individual's care or for a facility directory;
6. for national security or intelligence purposes;
7. to correctional institutions or law enforcement officials to provide them with information about a person in their custody;
8. as part of a limited data set; or
9. that occurred prior to the compliance date.

Signature Title, if legal representative* Date

*May be requested to submit evidence of representative status.

Retain for a minimum of 6 years

Notice: Check with Legal Counsel prior to making any non-routine disclosures.

FORM-06.B

ACCOUNTING FOR DISCLOSURES FORM

Date of Disclosure	Name and Address Of Entity Receiving PHI	Description of PHI Disclosed	Statement of Purpose of Disclosure

Retain for minimum of 6 years.

FORM-07

REQUEST FOR ALTERNATIVE MEANS OF COMMUNICATION

---------- ----------

Patient Name Patient Birth Date

NOTICE TO PATIENT: Your request for communication by alternative means **only** is applicable to the information maintained by Georgetown University. If you would like communications maintained by any other Health Care Provider, a separate request must be submitted to that provider.

My request for alternative means of communication applies to the following providers associated with the University of Oklahoma:

Name of Physician or Other Provider	Department

REQUESTED ALTERNATIVE MEANS OF COMMUNICATION:

□ Alternative Phone Number:_____

□ Alternative Mailing Address: _____

City State Zip

□ Other Alternative Means of Communication _____

My request applies:
□ to communications about this date of service only (indicate date)_____ **or**
□ from this date of service (indicate date) _____ until I indicate otherwise **or**
□ from _____ to _____.

Signature Title, if legal representative* Date

*May be requested to submit evidence of representative status.

REQUEST APPROVED: □
REQUEST DENIED: □

By: _____
Signature Title Date

Reason for Denial: □ Too expensive to accommodate request
□ Administratively impractical to accommodate request
□ You failed to provide information as to how payment, if applicable, will be handled
□ You failed to specify an alternative address or method of contact.

Additional explanation: _____

Retain for minimum of 6 years.

FORM-08.A

REQUEST FOR AMENDMENT OF PROTECTED HEALTH INFORMATION

---------- ----------

Patient Name Patient Birth Date

Address where you want the amendment response sent

NOTICE TO PATIENT: Your request for an amendment to your protected health information **only** is applicable to the information maintained by Georgetown University. If you would like to request amendments to your protected health information maintained by any other Health Care Provider, a separate request must be submitted to that provider.

REQUESTED AMENDMENT:

I request that you amend (describe the information you would like amended):_____

_____

_____

I request the amendment described above to be made to the protected health information in my designated record set maintained or created by the following providers associated with Georgetown University.

Name of Physician or Other Provider	Department

Date of record or information you would like amended:_____

I would like this information amended because (state specific reason for amendment):_____

_____

_____

_____

Signature Title, if legal representative* Date

*May be requested to submit evidence of representative status.

REQUEST APPROVED: □

If we approve your request for amendment, please complete the attached form, and return it to us, to identify any persons or entities that we need to notify of the amendment to your protected health information.

REQUEST DENIED: □

By: _____
Signature Title Date

Reason for Denial:
□ The information was not created by the physician or clinic to which you submitted the request;
□ The information is not part of your Designated Record Set;
□ The information is not available for your inspection pursuant to the University's Policy regarding individual access because _____;
□ The information is accurate and complete.

If your request for an amendment to your protected health information is denied, you may submit a written statement of your disagreement with the denial. Send the statement of disagreement to:

_____
_____.

If you do not submit a written statement disagreeing with the denial, you may request, in writing, that we provide your request for amendment and our denial with any future disclosures of the protected health information that is the subject of your request. This request should be submitted to us within sixty (60) days of receiving the notice of denial.

You may make a complaint to the University's Privacy Official regarding the denial of your amendment. The contact information for the University's Privacy Official is:

Privacy Official
Georgetown University
202 Healy, 37th & O Streets, N.W.
Washington, D.C. 20057
(202) 687-6457
hipaaprivacy@georgetown.edu

You also may submit a complaint to the Secretary of the Department of Health and Human Services regarding the denial of your amendment. The complaint must be written, but can be submitted either on paper or electronically. A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the HIPAA Privacy Regulations. You must submit the complaint within 180 days of when you knew or should have known that the act or omission complained of occurred.

FORM-08.B

Amendment Acceptance – Notification Form

I request and authorize _____[insert name of clinic/department/provider]_____ to notify the health care providers or entities listed below of the amendment(s) to the medical records of _____.
[Indicate name of patient.]

Signed: _____
Name Title, if legal representative Date

List of Providers/Entities that Need to be Notified of Amendment

_____
Name
_____
_____
Address

_____
Name
_____
_____
Address

_____
Name
_____
_____
Address

_____
Name
_____
_____
Address
_____
Name
_____
_____
Address

Retain for minimum of 6 years.

FORM-09

REQUEST FOR RESTRICTIONS ON USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

---------- ----------

Patient Name Patient Birth Date

Address:_____

NOTICE TO PATIENT: Your request for a restriction on the use and disclosure of your protected health information **only** is applicable to the information maintained by Georgetown University. If you would like to request a restriction on the use and disclosure of your protected health information maintained by any other Health Care Provider, a separate request must be submitted to that provider.

I hereby request on the use and/or disclosure of my protected health information maintained or created by the following providers associated with Georgetown University:

Name of Physician or Other Provider	Department

REQUESTED RESTRICTION: Check the box to indicate the type of restriction and then describe the specific restriction.

Note: Even if a requested restriction is granted, it cannot prevent complete disclosures to the individual or as required by law.

□ Treatment:_____

□ Payment: _____

□ Health Care Operations/Administrative Purposes_____

□ Disclosures to family members or others involved in my care _____

My request applies: □ to communications about this date of service only (indicate date)_____ **or** □ from this date of service (indicate date) _____ until I indicate otherwise **or** □ from _____ to _____.

Signature Title, if legal representative* Date

*May be requested to submit evidence of representative status.

REQUEST APPROVED: □
REQUEST DENIED: □

By: _____
Signature Title Date

Reason for Denial: □ Too expensive to accommodate request
□ Administratively impractical to accommodate request
□ May prevent effective treatment

Additional explanation: _____

FORM-10

Privacy Official – Contact Information

Privacy Official
Georgetown University
Office of University Counsel
202 Healy; 37th & O Streets, N.W.
Washington, D.C. 20057-1246
(202) 687-6457

hipaaprivacy@georgetown.edu

Form-11

Health Information Privacy Complaint Form

Patient Name: _____ Date: _____

Patient Identification Number: _____

Street Address: _____

City: _____ State: _____ Zip: _____

Please describe the nature of the complaint: _____

Date of Occurrence: _____ Information Affected: _____

Please list possible recipients of protected health information:

Name	Organization:
_____	_____
_____	_____
_____	_____

Patient Signature: _____ Date: _____

Please mail this form to the University's Privacy Official at the following address:

Privacy Official
Georgetown University
Office of University Counsel
202 Healy; 37th & O Streets, N.W.
Washington, D.C. 20057-1246
hipaaprivacy@georgetown.edu

You may also contact the Privacy Official at (202) 687-6457.

FORM-18

FAX COVER SHEET

Confidential Health Information Enclosed. Health care information is personal and sensitive. It is being faxed to you after appropriate authorization from the patient or under circumstances that do not require patient authorization. You, the recipient, are obligated to maintain this information in a safe, secure and confidential manner. Re-disclosure without additional patient consent or authorization or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain the confidentiality of this information could subject you to penalties under Federal and/or State law.

Date Transmitted: _____ Time Transmitted: _____
Number of Pages (including cover sheet):_____
Intended Recipient: _____
Facility: _____
Address: _____
Telephone #: _____ Fax #: _____

Documents being faxed: Clinic Records PT
Lab X-Ray
Other

Confidentiality Statement:

The information contained in this facsimile transmission is privileged and confidential and is intended only for the use of the recipient listed above. If you are neither the intended recipient or the employee or agent of the intended recipient responsible for the delivery of this information, you are hereby notified that the disclosure, copying , use or distribution of this information is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone to arrange for the return of the transmitted documents to us or to verify their destruction.

Please contact _____ at _____ to verify receipt of this Fax or to report problems with the transmission.

Verification of Transmission of Particularly Sensitive Health Information:

I verify the receiver of this Fax has confirmed its transmission:
Name:_____ Date:_____ Time:_____

I verify that I have confirmed the receipt of this Fax transmission by phone:
Name:_____ Date:_____ Time:_____

FORM-21

SAMPLE

EMPLOYEE ROLE BASED ACCESS WORKSHEET

Name:_____ **Date:**_____

Social Security Number:_____

College/Department/Clinic:_____

Supervisor:_____

Type of Information	Create	Edit	Use	View	Disclose	Transport	Destroy
None							
Entire Designated Record Set							
Progress Notes							
Directory							
Demographics							
Financial							
Medication Orders							
Lab Orders							
Radiology Orders							
Ancillary Orders							
Lab Results							
Radiology Results							
Ancillary Results							
Physician Dictation							

I understand that my access to, and use of, protected health information created, obtained, or maintained by the university is limited to the types and uses indicated in this worksheet. I agree to seek permission from my supervisor prior to using protected health information in any manner not permitted by this worksheet. I understand that if

I use or disclose protected health information in violation of this worksheet, the University's Privacy Policies, or the federal or state privacy laws, I will be subject to sanctions, up to and including termination.

Signature:_____ **Witnessed by:**_____

Type of Use:

Create:	**Primary source of documentation.**
Edit:	**Changing incorrect data.**
Use:	**Read to make decisions appropriate for your position.**
View:	**Employee position requires them to view information but is not expected to make decisions.**
Disclose:	**Conveyance of the information to persons or entities outside of the practice.**
Transport:	**Moving Information from one place to another.**
Destroy:	**Final legal disposition of the records.**

HIPAA Document –
Retain for 6 years

FORM-23

SAMPLE AUTHORIZATION FORM

Name:_____ **Date of Birth**:_____

I hereby authorize ___[Insert the specific name of the Health Care Component or University Personnel] to release the protected health information indicated below to:

Name Phone Number

Address

Requested Information

I authorize the disclosure of the following types of records created from _____ to_____: **[NOTE: You will be charged $.25 per page for paper records and $5.00 per film for radiology films.]**

☐ Billing Records ☐ Lab Reports

☐ Pathology Reports ☐ Radiology Reports

☐ X-rays ☐ Other_____

☐ Information created or received from other providers (Specify which ones or "all")_____

☐ Entire designated record set

Purpose of the Requested Use or Disclosure

The purpose of the use or disclosure is: ☐ at the request of the patient or ☐ other_ _____.

[Indicate specific reason.]

Expiration Date

This authorization will automatically expire:

☐ ___/____/____ (May not exceed 12 months from the date of the signature below.) or

☐ when the following event occurs: _____.

Please Note the Following:

1. You may refuse to sign this authorization. Your refusal will *not* affect your ability to obtain treatment or payment.

2. If the persons or entities who are authorized to receive the information above are *not* health care providers or health plans covered by federal health privacy laws, they may re-disclose the information and those laws would no longer protect the disclosed health information.

3. Once you sign this authorization, we can rely on it until you revoke it or, if you have not revoked it, until it expires. You can *revoke* this authorization by delivering a dated and signed letter to our clinic addressed to [insert title or name of person, i.e., business manager] at the following address: _____
_____.

4. ☐ If checked, we will receive compensation for our use/disclosure of the information that is the subject of this authorization.

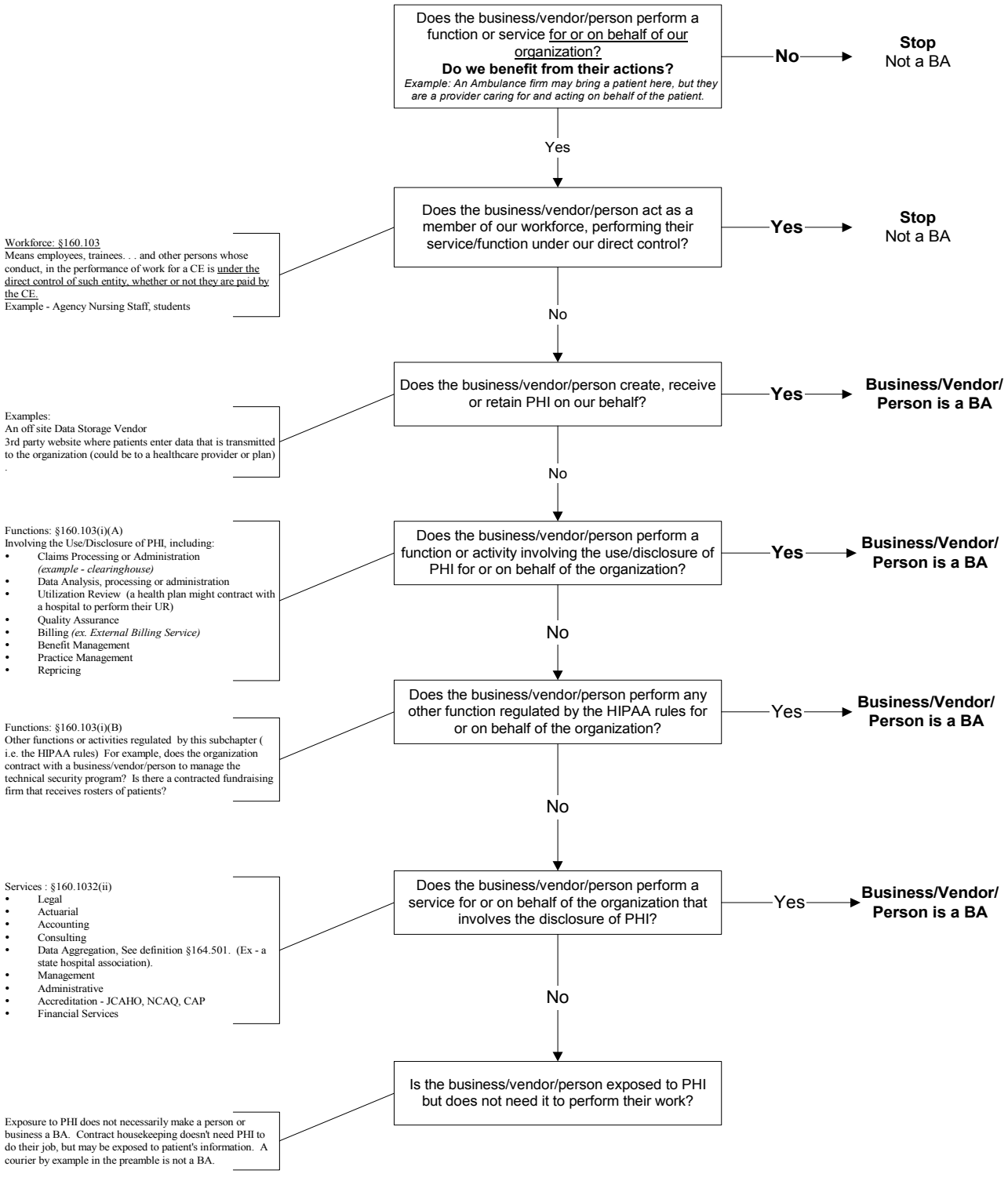
Signature:_____ Date:_____
(of Patient or Legal Representative)

Capacity of Legal Representative (if applicable)*:_____

*May be requested to provide verification of representative status.

BUSINESS ASSOCIATE (BA) DECISION CHART - correction 4/10/02

Name - Business/Vendor/Person: _____



FORM 27-A

BUSINESS ASSOCIATE ADDENDUM

HIPAA BUSINESS ASSOCIATE ADDENDUM

*** * * ***

This Addendum ("Addendum") amends and is hereby incorporated into the existing agreement known as _____ ("Agreement"), entered into by and between _____ (hereinafter "Business Associate") and Georgetown University (hereinafter "Covered Entity") on _____.

Covered Entity and Business Associate mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and HIPAA's implementing regulations, Title 45, Parts 160 and 164 of the Code of Federal Regulations ("Privacy Rule"), dealing with the confidentiality of health or health-related information. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:
    a. Protected Health Information (PHI) means any information, whether oral or recorded in any form or medium, that: (i) relates to the past, present or future physical or mental condition of any Individual; the provision of health care to an Individual; or the past, present or future payment of the provision of health care to an Individual; and (ii) identifies the Individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. PHI includes demographic information unless such information is de-identified according to the Privacy Rule.

    b. Individual means the person who is the subject of PHI, and shall include a person who qualifies under the Privacy Rule as a personal representative of the Individual.

    c. Capitalized terms used in this Agreement, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule.

2. Prohibition on Unauthorized Use or Disclosure of PHI: Business Associate shall not use or disclose any PHI received from or on behalf of Covered Entity except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by Covered Entity.

3. Use and Disclosure of Protected Health Information: Except as described in Section 4, Business Associate may use or disclose PHI only for the following purpose(s):
    a. *[Enumerate BA's permitted uses and disclosures here, or incorporate by reference an attached Exhibit where the uses and disclosures are described.]*

4. Use of PHI for Certain of Business Associate's Operations: Business Associate may use and/or disclose PHI it creates for, or receives from, Covered Entity to the extent

necessary for Business Associate's proper management and administration, or to carry out Business Associate's legal responsibilities, only if:

a. The disclosure is required by law; or
b. Business Associate obtains reasonable assurances, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:
   (i) hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization, or as required by law; and
   (ii) notify Business Associate, who shall in turn promptly notify Covered Entity, of any instance which the person or organization becomes aware of in which the confidentiality of such PHI was breached.

Business Associate's proper management and administration does not include the use of disclosure of PHI by Business Associate for Marketing purposes, or to support Marketing.

5. Safeguarding of PHI: Business Associate shall develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to prevent the improper use or disclosure of all PHI, in any form or media, received from or created or received by Business Associate on behalf of, Covered Entity. Business Associate shall document and keep these security measures current. [INCLUDE IF DEEMED NECESSARY: Attached to this Addendum as Exhibit ___ is a description of Business Associate's safeguards which shall be considered a part of this Addendum. Business Associate shall promptly inform Covered Entity in writing of any updates or modifications to Exhibit ___ made during the term of this Agreement.]

6. Subcontractors and Agents: If Business Associate provides any PHI which was received from, or created for, Covered Entity to a subcontractor or agent, then Business Associate shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Business Associate by this Addendum.

7. Maintenance of the Security of Electronic Information: Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Health Information received from, or on behalf of, Covered Entity which pertains to an Individual. Business Associate shall document and keep these security measures current and available for inspection, upon request. Business Associate's security measures must be consistent with HIPAA's Security regulations, Title 45, Part 142 of the Code of Federal Regulations ("Security Rule"), once such regulations are in effect.

8. Compliance with Electronic Transactions and Code Set Standards: If Business Associate conducts any Standard Transaction for, or on behalf, of Covered Entity, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in

connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

a. changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;

b. adds any Health Information elements or segments to the maximum defined Health Information Set;

c. uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or

d. changes the meaning or intent of the Standard's Implementations Specification(s).

9. Access to PHI: At the direction of Covered Entity, Business Associate agrees to provide access to any PHI held by Business Associate which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity . This access will be provided to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under the Privacy Rule.

10. Amendment or Correction to PHI: At the direction of Covered Entity, Business Associate agrees to amend or correct PHI held by Business Associate and which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity

11. Reporting of Unauthorized Disclosures or Misuse of PHI: Business Associate shall report to Covered Entity any use or disclosure of PHI not authorized by this Addendum or in writing by Covered Entity. Business Associate shall make the report to Covered Entity's Privacy Official not less than one (1) business day after Business Associate learns of such use or disclosure. Business Associate's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the PHI used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure. Business Associate shall provide such other information, including a written report, as reasonably requested by Covered Entity's Privacy Official.

12. Mitigating Effect of Unauthorized Disclosures or Misuse of PHI. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a misuse or unauthorized disclosure of PHI by Business Associate in violation of the requirements of this Addendum.

13. Tracking and Accounting of Disclosures: So that Covered Entity may meet its accounting obligations under the Privacy Rule,

(a) Disclosure Tracking. Starting April 14, 2003, for each disclosure not excepted under subsection (b) below, Business Associate will record for each disclosure of PHI it makes to Covered Entity or a third party of PHI that Business Associate creates or receives for or from Covered Entity (i) the disclosure date, (ii) the name and (if known) address of the

person or entity to whom Business Associate made the disclosure, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the disclosure. For repetitive disclosures which Business Associate makes to the same person or entity, including the Covered Entity, for a single purpose, Business Associate may provide (i) the disclosure information for the first of these repetitive disclosures, (ii) the frequency, periodicity or number of these repetitive disclosures, and (iii) the date of the last of these repetitive disclosures. Business Associate will make this log of disclosure information available to the Covered Entity within five (5) business days of the Covered Entity's request.

(b) Exceptions from Disclosure Tracking. Business Associate need not record disclosure information or otherwise account for disclosures of PHI that meet each of the following conditions:

(i) the disclosures are permitted under this Addendum, or are expressly authorized by Covered Entity in another writing; and,

(ii) the disclosure is for one of the following purposes:

a. Covered Entity's Treatment, Payment, or Health Care Operations;

b. in response to a request from the Individual who is the subject of the disclosed PHI, or to that Individual's Personal Representative;

c. made to persons involved in that individual's health care or payment for health care;

d. for notification for disaster relief purposes;

e. for national security or intelligence purposes; or,

f. to law enforcement officials or correctional institutions regarding inmates.

(c) Disclosure Tracking Time Periods. Business Associate must have available for Covered Entity the disclosure information required by this section for the six-year period preceding Covered Entity's request for the disclosure information (except Business Associate need have no disclosure information for disclosures occurring before April 14, 2003).

14. Accounting to Covered Entity and to Government Agencies. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or on behalf of, or created for, Covered Entity available to Covered Entity, or at the request of Covered Entity, to the Secretary of the Department of Health and Human Services (HHS) or his/her designee, in a time and manner designated by Covered Entity or the Secretary or his/her designee, for the purpose of determining Covered Entity's compliance with the Privacy Rule. Business Associate shall promptly notify Covered Entity of communications with HHS regarding PHI provided by or created by Covered Entity and shall provide Covered Entity with copies of any information Business Associate has made available to HHS under this provision.

15. Term and Termination:

a. This Addendum shall take effect [upon execution] [April 14, 2003].

b. In addition to the rights of the parties established by the underlying Agreement, if Covered Entity reasonably determines in good faith that

Business Associate has materially breached any of its obligations under this Addendum, Covered Entity, in its sole discretion, shall have the right to:

(i) exercise any of its rights to reports, access and inspection under this Addendum; and/or

(ii) require Business Associate to submit to a plan of monitoring and reporting, as Covered Entity may determine necessary to maintain compliance with this Addendum; and/or

(iii) provide Business Associate with a ten (10) day period to cure the breach; or

(iv) terminate the Agreement immediately.

c. Before exercising any of these options, Covered Entity shall provide written notice to Business Associate describing the violation and the action it intends to take.

16. Return or Destruction of PHI: Upon termination, cancellation, expiration or other conclusion of the Agreement, Business Associate shall:

a. Return to Covered Entity or, if return is not feasible, destroy all PHI and all Health Information in whatever form or medium that Business Associate received from or created on behalf of Covered Entity. This provision shall also apply to all PHI that is in the possession of subcontractors or agents of Business Associate. In such case, Business Associate shall retain no copies of such information, including any compilations derived from and allowing identification of PHI. Business Associate shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Business Associate shall certify on oath in writing to Covered Entity that such return or destruction has been completed.

b. If Business Associate believes that the return or destruction of PHI or Health Information is not feasible, Business Associate shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Business Associate shall extend the protections of this Addendum to PHI and Health Information received from or created on behalf of Covered Entity, and limit further uses and disclosures of such PHI, for so long as Business Associate maintains the PHI.

17. Miscellaneous:

a. Automatic Amendment: Upon the effective date of any amendment to the regulations promulgated by HHS with regard to PHI, this Addendum shall automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations.

b. Interpretation. Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

GEORGETOWN UNIVERSITY	BUSINESS ASSOCIATE
By: _____	By_____
Title: _____	Title: _____
Date: _____	Date: _____

FORM-29

HIPAA Document –
Retain for 6 years

Georgetown University Hospital
Georgetown University Medical Center

AUTHORIZATION FOR DISCLOSURE FOR PHILANTHROPY

Georgetown University Hospital is the national capital area's most recognized academic teaching hospital. With more than 1,100 physicians, our clinical services represent one of the largest and most geographically diverse and fully integrated healthcare delivery networks in the area. Since its founding in 1898, the hospital has been dedicated to promoting health through education, research, and patient care; and for 11 years in a row, the Hospital has been ranked among the best in the nation by *U.S. News and World Report* in a number of specialty areas. The Georgetown University Medical Center, an internationally recognized academic medical center and a part of Georgetown University, shares a three-part mission of research, teaching, and patient care in close partnership with the Hospital. This mission is carried out with a strong emphasis on community outreach, public service, and a dedication to the Jesuit principle of "cura personalis", or "care of the whole person."

By signing the form below, I agree that Georgetown University Hospital may disclose to the Georgetown University Medical Center Office of Development* my name and address and the name of my physician(s) from whom I received treatment, including her/his specialty. This means that if I sign the authorization form, the Office of Development may contact me with information, including fundraising information to support medical education, research, and clinical services that may be of interest to me after being treated at Georgetown. Georgetown University Hospital may not disclose to the Office of Development any information regarding my medical condition, diagnosis or treatment other than the name of my physician and specialty.

The Office of Development fully supports the protection of my health information and has pledged to maintain strict patient confidentiality in keeping with high ethical standards and in accordance with federal law. All development staff and business associates sign a confidentiality agreement or contract that states that no protected health information shall be improperly disclosed.

Georgetown University Hospital does not condition treatment, payment, benefit eligibility or enrollment activities on the signing of this form. Therefore, I am not required to sign this authorization. I may revoke this authorization at any time in writing by following the guidelines on this form. The revocation will be effective upon receipt, but will have no impact on uses or disclosures made while my authorization was valid.

This authorization shall expire 10 years from the date of signature. I will receive a copy of this authorization upon signature.

Patient Name:

_____

_____

(PLEASE PRINT) (First) (Middle Initial)
(Last)

Signature: _____
Date: _____

For Personal Representatives, please provide the following contact information.

I _____ represent that I am the healthcare agent/guardian/ surrogate/parent of the patient named above.
(circle one of the above)

Personal Representative Signature:

_____

(please print your name)

*The Office of Development is the department that helps to raise charitable gifts in support of medical education, biomedical research, and clinical care and services to support the missions of Georgetown University Hospital and Georgetown University Medical Center. Thank you for your willingness to let us contact you.

About Georgetown University Hospital and Georgetown University Medical Center:

- Georgetown University Hospital – a member of MedStar Health
- Georgetown University Medical Center
  - School of Medicine
  - Biomedical Research
  - School of Nursing and Health Studies
  - Lombardi Cancer Center

Frequently Asked Questions:

WHAT AM I SIGNING?

By signing the authorization form, the Office of Development may: tell you about the progress in medical treatments and discovery for the diseases and conditions that brought you to Georgetown; invite you to future seminars and meetings that include fundraising events; and offer you the opportunity to support the work of our exceptional physicians, nurses, and researchers in the areas that are of interest to you and your family.

WHY IS IT NECESSARY?

The Health Insurance Portability and Accountability Act (HIPAA) is a new federal law that protects the privacy of health information, and limits our ability to contact you. This means that if you sign the authorization form, you are giving us permission to contact you with information that may be of interest to you after being treated at Georgetown University Hospital. Signing the form does not obligate you in any way. The authorization form may be revoked at any time.

WHY IS IT IMPORTANT?

Georgetown University Hospital and Georgetown University Medical Center depend on gifts from individuals, foundations, corporations, and from the community to help us continue to search for better ways to diagnose, treat, and cure diseases. Those patients who make gifts tell us that it gives them a tremendous sense of satisfaction, knowing they are helping Georgetown physicians make progress in fighting diseases that have affected them or a family member.

The decision to make a gift is entirely up to you. Signing this form does not obligate you in any way. Thank you!

Georgetown University Hospital and the Georgetown University Medical Center greatly appreciate your willingness to allow us to contact you to discuss fundraising opportunities. Please return this completed authorization to your physician, his or her staff, the admissions office, or mail/fax it to:

Georgetown University Medical Center's Office of Development
P.O. Box 571404
Washington, DC 20057
Telephone: 202-687-4596
Fax: 202-687-4722

You have the right to revoke this authorization at any time by mailing or faxing a written request along with a copy of the original authorization to the address or fax listed above. If you are unable to provide a copy of the original authorization with your request to revoke, please provide:

Name	Medical Record Number
Address	Date of Birth
Phone Number	Date of Authorization

If the authorization was signed by your personal representative, please also include the representative's:

Name and Relationship, Address, and Phone Number

Please understand that if you are unable to provide all of the above information, Georgetown University Hospital and Georgetown University Medical Center may not be able to honor your revocation request.