POLICY #1: PRIVACY AND SECURITY RULES POLICIES AND PROCEDURES

DEFINITIONS

The following words shall have the meaning assigned to them below whenever used in the Case Western Reserve University ("CASE") Privacy and Security Rules Policies and Procedures:

Business associate means with respect to CASE a person who:

i. on behalf of CASE, but not as a member of CASE's workforce, performs, or assists in the performance of:

   (a) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
   (b) any other function or activity regulated by the requirements of 45 CFR, Subtitle A, Subchapter C (concerning the HIPAA administrative simplification requirements); or

ii. provides, other than as a member of CASE's workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to CASE, where the provision of the service involves the disclosure of individually identifiable health information from CASE, or from another business associate of CASE, to the person.

Case Western Reserve University or CASE shall refer solely and exclusively to the designated health care components of CASE, identified by CASE for HIPAA compliance purposes in accordance with the Privacy and Security Rules and as documented as required by the Privacy and Security Rules, unless the context requires otherwise, in which case, ***Case Western Reserve University*** or ***CASE*** shall mean the university as a whole.

Covered entity means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction for which standards have been promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996. CASE's designated health care components are "covered entities" for purposes of the Privacy and Security Rules.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered component, is under the direct control of the covered component, whether or not they are paid by the covered component.

Data use agreement means an agreement between CASE and the recipient of a limited data set which imposes certain requirements on that recipient as to the use of the limited data set and the confidentiality of PHI, as further described in the policy and procedures concerning research.

Designated health care component means any one of those departments, activities and/or functions, or any combination of departments, activities and/or functions of CASE which have been designated by CASE as health care components for purposes of compliance with the Privacy Rules; other than as provided in 45 CFR §164.504, the Privacy and Security Rules apply only to the designated health care components of CASE and not to any other departments, components, activities and/or functions of CASE.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside of CASE.

Health care operations means any of the following activities of CASE:

i. conducting quality assessment and improvement activities, 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 health care providers and individuals with information about treatment alternatives; and related functions that do not include treatment;
ii. 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 health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
iii. conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
iv. business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
v. business management and general administrative activities of CASE including, but not limited to:

(a) management activities relating to implementation of and compliance with the requirements of this subchapter;
(b) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
(c) resolution of internal grievances;
(d) the sale, transfer, merger, or consolidation of all or part of CASE with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(e) creating de-identified health information or a limited data set, and fundraising for the benefit of CASE, all as carried on as permitted by the HIPPA Privacy Rules.

Health information means any information, whether oral or recorded in any form or medium, that:

i. is created or received by a health care provider (including CASE), a health plan, a public health authority, an employer, a life insurer, a school or university, or a health care clearinghouse; and
ii. 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.

Hybrid entity means a single legal entity that is a covered entity for purposes of the Privacy Rules because it conducts certain activities which are subject to the Privacy and Security Rules and certain activities which are not, and which designates health care components as required by the Privacy and Security Rules; CASE is a hybrid entity and, as such, only its designated health care components are subject to and must comply with the Privacy and Security Rules.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

i. is created or received by a health care provider (including CASE), a health plan, an employer, or a health care clearinghouse; and
ii. 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

(a) that identifies the individual; or

(b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Institutional review board or IRB means the Case Western Reserve University Institutional Review Board, the Case Cancer Institutional Review Board, or any other similar body or board established in accordance with 45 CFR 46.102(g).

Limited data set means PHI from which certain direct identifiers of the individual and the individual's relatives, employer(s), and/or household members have been removed, as more fully described in CASE's Policies and Procedures concerning research.

Payment means the activities undertaken by CASE to obtain reimbursement for the provision of health care; such activities relate to an individual to whom health care is provided and include, but are not limited to:

i. determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
ii. risk adjusting amounts due based on enrollee health status and demographic characteristics;
iii. billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
iv. review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
v. utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
vi. disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(a) name and address;
(b) date of birth;
(c) social security number;
(d) payment history;
(e) account number; and
(f) name and address of the health care provider and/or health plan.

Policies and Procedures means collectively the written policies and procedures adopted by CASE concerning compliance with the Privacy and Security Rules.

Privacy Rules mean those standards, implementation specifications, rules and/or other requirements promulgated by the United States Department of Health and Human Services for the protection of individually identifiable health information, as set forth at

45 CFR Parts 160 and 164, as the same may be from time to time amended, modified and/or supplemented, and any successor rules or regulations dealing with substantially the same subject matter.

Protected health information or PHI means individually identifiable health information transmitted or maintained in any form or medium; ***protected health information*** excludes individually identifiable health information in:

i. education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
ii. records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
iii. employment records held by CASE in its role as an employer.

Security Rules mean those standards, implementation specifications, rules and/or other requirements promulgated by the United States Department of Health and Human Services for the protection of individually identifiable health information, as set forth at 45 CFR Parts 160, 162 and 164, as the same may be from time to time amended, modified and/or supplemented, and any successor rules or regulations dealing with substantially the same subject matter.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

POLICY #2: HYBRID ENTITY STATUS AND DESIGNATED HEALTH CARE COMPONENTS POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") has hybrid entity status for purposes of compliance with the Privacy and Security Rules. For most purposes, only the designated health care components of CASE are subject to the Privacy and Security Rules.

PURPOSE: The purpose of this policy is to: (1) explain CASE's hybrid entity status under the Privacy and Security Rules; (2) specify compliance obligations arising out of CASE's hybrid entity status; and (3) identify CASE's designated health care components.

I. HYBRID ENTITY STATUS

A. Hybrid entity election. CASE will comply with the Privacy and Security Rules as a hybrid entity. CASE qualifies as a hybrid entity because it performs both covered functions, i.e., functions which characterize CASE as health care provider under the Privacy and Security Rules, and non-covered functions.

B. Determination of Components. CASE will designate as health care components all those activities, components, departments and/or functions (collectively, "activities") of CASE, which, if a separate legal entity or treated as the sole activity(ies) of a single legal entity, would qualify such entity as a covered entity under the Privacy and Security Rules.

II. COMPLIANCE OBLIGATIONS

A. In General. Generally, the requirements of the Privacy and Security Rules apply only to the designated health care components of CASE.

B. Interpretation of the Privacy and Security Rules. Any reference in the Privacy and Security Rules to a covered entity shall be understood to refer to the designated health care components of CASE. Any reference in the Privacy and Security Rules to a "health plan" or a "covered health care provider" shall refer to a CASE designated health care component if such designated health care component performs the functions of a health plan or a health care provider. References in the Privacy and Security Rules to "protected health information" or "PHI" refer to PHI that is created or received by or on behalf of a designated health care component of CASE.

C. CASE Obligations. CASE, as opposed to just the designated health care components of CASE, has the following responsibilities under the Privacy and Security Rules:

1. compliance with those sections of the Privacy and Security Rules set forth in 45 CFR Subpart C, concerning compliance and enforcement;

2. adoption of policies and procedures to ensure compliance with the Privacy and Security Rules, including implementation of safeguard requirements protecting PHI held by designated health care components; and

3. designating its health care components and documenting such designation.

4. Provide training on CASE privacy and security policies and practices to all members of designated covered components at CASE.

5. Apply appropriate sanctions when violations of this policy occur.

D. Organizational Unit Responsibilities

Each covered component (e.g., department, clinic) within CASE is responsible for enforcing policies, standards, and practices set forth by CASE to comply with HIPAA Privacy and Security Standards. Management responsibilities shall include, but are not limited to, the following:

- Secure storage of patient information.
- Procedures for release of patient information (to third party payers, providers, etc.)
- Procedures for disposal of hard copy records.
- Secure transmission and storage of electronic records.
- Protection of confidential information from access, use, or dissemination by unauthorized persons.
- Report to the Privacy and/or Security Officer any known or suspected violation of this policy or other CASE privacy policies or any wrongful use or disclosure of protected health information.

E. Individual Responsibilities

All members of designated covered components at Case are responsible for adhering to this and related privacy and information security policies and standards and for

safeguarding all confidential patient information. These responsibilities shall include, but are not limited to, the following:

- Avoid access, retrieval, or use of any information on a current or former patient unless authorized for legitimate duties (i.e., assisting in care/treatment, providing a consultation, or approved educational/research or business purposes) within their organizational unit.
- Limit the access, use, and disclosure of protected health information to the minimum amount necessary to accomplish the intended purpose.
- Dictate patient notes and discuss patients and their care only in private areas (i.e., not in hallways, elevators, cafeteria lines,) to the extent practicable.
- Protect personal computerized data systems passwords from disclosure to others.
- Take special care to protect patient information (e.g., in hard copy charts or printouts or on computer screens) from view by unauthorized persons.
- Use secure methods for authorized storage, transmission, and disposal of confidential patient information.
- Report to the HIPAA Representative of the covered component AND the Privacy and/or Security Officer any known or suspected internal or external violation of this policy or other CASE privacy policies or any wrongful use or disclosure of PHI.

III. DESIGNATED HEALTH CARE COMPONENTS

A. Identification of Components. The following are CASE's designated health care components:

1. CASE School of Dental Medicine
2. CASE School of Dental Medicine Faculty Practice Plan
3. Center for Human Genetics Laboratory
4. CASE Student Self-Insured Health Plan
5. CASE Optional Dependent Medical Plan
6. CASE Employee Health Plan

B. Identification of Additional Components. If any changes in CASE's activities, or the addition of any activities to those currently undertaken by CASE occur, and such changes in or additions of activities require any changes in the designation of designated health care components of CASE, CASE will make changes to such designation in accordance with the Privacy and Security Rules and any additional health care components designated as a result of such changes will comply with

the Privacy and Security Rules.

IV. OTHER DEPARTMENTS/FUNCTIONS WITH ACCESS TO PHI

The designated health care components of CASE will enter into a memorandum of understanding with those departments and/or functions of CASE which provide services to the designated health care components or which otherwise might have access to PHI in the possession of the designated health care components. As of the date of the promulgation of these Policies and Procedures, a memorandum of understanding will be entered into between the designated health care components and those components or functions of the following departments which interact with the designated health care components:

1. CASE University Attorney's Office (now called the Office of General Counsel)
2. CASE Office of Audit Services
3. CASE Controller's Offices including all accounting functions
4. CASE Information Technology Services

If in the future any additional departments or functions of CASE have access to PHI maintained or disclosed by a designated health care component of CASE, the designated health care components will enter into a memorandum of understanding with such other department(s) or function(s).

V. SEPARATION CONTROLS

A. CASE will create adequate separation between its designated health care components and other components of CASE. These procedures for adequate separation are referred to as separation controls.

B. CASE shall implement the following separation controls in order to protect PHI used and/or maintained by its designated health care components:

1. designated health care components shall not disclose PHI to other components of CASE in circumstances under which the Privacy and Security Rules would prohibit such disclosure if the designated health care component and the other component were separate and distinct legal entities;

2. a designated health care component will disclose information to another component of CASE which would, if the components were separate entities, constitute a business associate of the designated health care component, only pursuant to a memorandum of understanding which requires that the other component not use or disclose PHI received from or on behalf of the

designated health care component in any way that is prohibited under the Privacy and Security Rules;

3. any person who performs duties or functions for both a designated health care component and another component of CASE, or for a department which performs functions on behalf of a designated health care component which would be business associate of the designated health care component if such department and the designated health care component were separate legal entities, will not use or disclose any PHI created or received in the course of or incident to performing such duties or functions for or on behalf of the designated health care component in any way prohibited by the Privacy and Security Rules; and

4. all employees of any CASE designated health care component or any function or department of CASE that has entered into a memorandum of understanding with a designated health care component shall be subject to the discipline procedures set forth in the policy entitled "Internal Enforcement" in CASE's Policies and Procedures.

HYBRID ENTITY: FREQUENTLY ASKED QUESTIONS

A. *Are all aspects of CASE's activities and operations subject to the Privacy and Security Rules?*

No. CASE is itself a covered entity for purposes of the Privacy and Security Rules because it carries on certain functions or activities which are subject to the Privacy and Security Rules. For example, CASE, through the CASE Dental School, provides health care to patients. However, the vast majority of CASE's activities and operations do not involve activities which are covered functions for purposes of the Privacy and Security Rules. While CASE itself has several obligations under the Privacy and Security Rules, such as adopting policies and procedures, cooperating in compliance efforts and designating its health care components, it is primarily CASE's designated health care components that are subject to the requirements and specifications of the Privacy and Security Rules.

B. *What does it mean to be a designated health care component?*

A designated health care component of CASE is a department, collection of activities or functions which if a separate legal entity, or if such activities or functions were performed by a separate legal entity, such separate entity would be a covered entity for purposes of the Privacy and Security Rules. CASE has listed its designated health care components in its Policies and Procedures concerning its hybrid entity status.

C. *Can a designated health care component of CASE disclose PHI to another department, or for the purposes of another function or operation of CASE?*

Yes, but that disclosure, must meet all requirements for a disclosure under the Privacy and Security Rules by a covered entity to a separate, unrelated entity, unless it is made pursuant to a memorandum of understanding entered into by the designated health care component with a department or activity of CASE that supports the designated health care component.

POLICY #3: GENERAL USE AND DISCLOSURE: POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will use and disclose PHI only as specifically permitted or required by the Privacy and Security Rules and in accordance with CASE's Policies and Procedures.

PURPOSE: The purpose of this policy is to specify when and how PHI may be used and disclosed.

I. INTRODUCTION

The Privacy and Security Rules restrict the use and disclosure of PHI. PHI may be used and disclosed only as permitted under the Privacy and Security Rules. Each use and disclosure of and each request for PHI must meet the "minimum necessary" standard. This policy describes permitted uses and disclosures of PHI and application of the minimum necessary standard to those uses and disclosures.

II. BASIC RULE

CASE will not use or disclose PHI except (a) as permitted or required by the Privacy and Security Rules, (b) in accordance with CASE's Notice of Privacy Practices, (c) as consistent with any agreed upon restrictions, as discussed in CASE's policy entitled "Requests for Additional Privacy" and (d) in compliance with the minimum necessary standard of the Privacy and Security Rules.

III. PERMITTED USES AND DISCLOSURES

A. Permitted uses and disclosures. Permitted uses and disclosures of PHI include:

1. to the individual;
2. incidental uses or disclosures, described below;
3. to carry out treatment, payment or health care operations;
4. pursuant to and in compliance with a valid authorization;
5. pursuant to a verbal agreement from an individual that permits disclosure to a caregiver;

6. for certain "priority" purposes such as disclosures required by law;

7. for various research purposes, pursuant to an appropriate waiver of authorization, as part of a limited data set and/or to create de-identified information (see policy on "Research");

8. for fund-raising, to the extent permitted under the Privacy and Security Rules; and

9. to business associates, as described below.

B. Incidental uses and disclosures. Incidental uses and disclosures that occur as a by-product of a use or disclosure otherwise permitted under the Privacy and Security Rules are explicitly permitted, so long as CASE has applied reasonable safeguards and implemented the minimum necessary standard, where applicable.

C. Business associates. The disclosure of PHI to CASE's business associates is permitted in accordance with the guidelines set forth in CASE's policy entitled "Business Associates."

D. Required disclosures. The Privacy and Security Rules require CASE to disclose PHI in the following instances:

1. when the individual requests access to information about himself or herself;

2. when the Department of Health and Human Services ("HHS") requests information to investigate or determine CASE's compliance with the rules; and

3. when required by law or other priorities, as discussed further in CASE's policy for Disclosures of Protected Health Information Without Authorizations or Prior Agreement.

IV. MINIMUM NECESSARY

A. The minimum necessary standard. When using or disclosing PHI, and when requesting PHI from another entity, CASE will make reasonable efforts to use, disclose or request the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request.

B. Exceptions. Among the uses, disclosures, and requests to which the minimum necessary standard does not apply are:

1. uses and disclosures for treatment purposes;

2. disclosures to the individual who is the subject of the information;

3. uses or disclosures made pursuant to an authorization;

4. uses or disclosures made in mandatory or situational fields of a HIPAA transactions standard;

5. disclosures to HHS when required by HHS for compliance and enforcement purposes; and

6. uses or disclosures that are required by other law.

C. Uses of PHI. With respect to CASE's use of PHI, CASE's privacy officer will identify: (1) the persons or classes of persons in CASE who need access to PHI to carry out their duties; (2) the categories of PHI that each person or class of persons needs; and (3) any conditions necessary for such access. It is CASE's policy to limit access to only the identified persons and to only the identified PHI.

D. Routine disclosures. For any type of disclosure of PHI that is made on a routine, recurring basis, it is CASE's policy to permit only the disclosure of the minimum amount of PHI that is reasonably necessary to achieve the purpose of the disclosure. For routine, recurring disclosures, CASE's privacy officer will identify the types of PHI to be disclosed and the conditions necessary for such access, and will distribute such information to the appropriate CASE personnel. Any such disclosures must be made in accordance with the Privacy and Security Rules.

For example, if a individual requests that his or her PHI be transmitted to a health care provider, CASE will comply with the request if it can determine that the disclosure is for treatment purposes or the individual provides an authorization.

E. Non-routine disclosures. For non-routine disclosures, it is CASE's policy to make such disclosures only in compliance with criteria designed to limit disclosure to only the minimum amount of PHI necessary to accomplish the purpose of the disclosure and review requests for such disclosures in accordance with those criteria. Among the factors that may be considered in making such a determination are:

1. What is the purpose of the disclosure? This could be relevant if the disclosure is not covered by the minimum necessary standard.

2. What is the minimum amount of PHI that can be disclosed to accomplish the purpose of the disclosure?

3. Are there standards in other industries or among health care providers as to what amount of information is sufficient to fulfill the intended purpose of the disclosure?

4. To what extent would the disclosure increase the number of persons with access to the PHI?

5. What is the likelihood of further disclosures?

6. Can substantially the same purpose be achieved using de-identified information?

7. Is there technology available to limit the amount of PHI disclosed?

8. What is the cost, financial or otherwise, of limiting the disclosure?

F. Requests for PHI. The minimum necessary standard applies to situations where CASE is requesting an individual's PHI from another entity.

1. For requests to other entities made on a routine and recurring basis, CASE will establish standard protocols describing the minimum amount of information reasonably necessary for purposes of a request, and limit its requests to only that information.

2. For non-routine requests, it is CASE's policy to make such requests only in compliance with criteria designed to limit a request to only the minimum amount of PHI necessary to accomplish the purpose of the request and review requests in accordance with those criteria. Among the factors that may be considered in making such a determination are:

   a. What is the purpose of the request? This could be relevant if the request is not covered by the minimum necessary standard.

   b. What is the minimum amount of PHI that can be disclosed to accomplish the purpose of the request?

c. Are there standards in other industries or among health care providers as to what amount of information is sufficient to fulfill the intended purpose of the request?

G. Reasonable reliance on requested disclosures. CASE may rely, if reasonable under the circumstances, on statements by public officials, other covered entities or their business associates that they are requesting the minimum PHI necessary to achieve the stated purpose of the request. CASE may also reasonably rely on the statements of its own business associates or professionals within its workforce that the information requested is the minimum necessary for such purposes, as well as on representations by researchers.

V. DISCLOSURES TO FRIENDS AND RELATIVES

A. Basic rule. CASE may disclose to a person involved in the current health care of an individual (such as a relative, close personal friend, or any other person identified by the individual) PHI directly related to the person's involvement in the current health care of the individual or payment for the individual's health care. Examples of persons who might be involved in the individual's care include, but are not limited to:

1. blood relatives;

2. spouses;

3. roommates;

4. girlfriends and boyfriends;

5. domestic partners; and

6. neighbors.

B. Disclosures of PHI when the individual is present. When the individual is present and has the capacity to make his or her own decisions, CASE may disclose PHI to the third party only if CASE:

1. obtains the individual's agreement to disclose to the third party involved in his or her care;

2. provides the individual with an opportunity to object to such disclosure and the individual does not express an objection; or

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

C. Disclosures of PHI when the individual is not present. When a individual is not present (*e.g.*, when a friend of the individual seeks to pick up a record of an individual's PHI from CASE) or when CASE cannot practically give the individual an opportunity to agree or object to the use or disclosure (*e.g.*, because of the individual's incapacity or an emergency circumstance), CASE may, in the exercise of professional judgment, determine whether the disclosure is in the individual's best interests. If so, CASE may disclose only PHI that is directly relevant to the person's involvement with the individual's health care. For example, CASE might disclose dental records to a person who it knows to be assisting an individual with his or her dental care. CASE personnel should follow these guidelines when deciding whether to disclose PHI when the individual is not present:

1. only disclose PHI that is directly related to the individual's current condition;

2. consider the individual's best interests and construe this opportunity narrowly, allowing disclosures only to those persons with close relationships with the individual, such as family members;

3. take into account whether the disclosure is likely to put the individual at risk of serious harm;

4. CASE is not required to verify the identity of relatives or other persons involved in the individual's care;

5. An individual's agreement to disclosure of PHI in one situation or on one occasion does not mean that the individual agrees to disclosures of PHI indefinitely in the future; use professional judgment to determine the scope of the person's involvement in the individual's care and the time period during which the individual agrees to the other person's involvement.

VI. VERIFICATION

A. Identity and Authority. CASE personnel must verify the identity of the person requesting PHI and the authority of such person to have access to the PHI under the Privacy and Security Rules, if the identity or the authority of the person is not known to the CASE personnel.

B. Documentation. CASE personnel should obtain documentation, statements, or representations, oral or written, from the person requesting the PHI, when such documentation is required under CASE's policy entitled "Disclosures of Protected Health Information Without Authorization or Prior Agreement."

C. Identity of Public Officials. CASE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or person acting on behalf of a public official: (1) an identification badge or other official credentials; (2) if a request is made in writing, the request is on the appropriate government letterhead; or (3) a written statement on appropriate government letterhead that the person to whom the disclosure will be made is acting under the government's authority, or other evidence or documentation of agency.

D. Authority of Public Officials. CASE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify the authority of a public official or person acting on behalf of a public official: (1) a written statement of the legal authority under which the information is requested, or an oral statement if a written statement is impracticable; or (2) if a request is made pursuant to legal process, a warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal.

E. Professional Judgment. CASE personnel may rely upon professional judgment when making a disclosure in accordance with public safety, as set forth in CASE's policy entitled "Disclosure of Protected Health Information Without Authorization or Prior Agreement."

VII. ORAL COMMUNICATIONS AND REASONABLE SAFEGUARDS

A. Applicability of privacy standards. The Privacy and Security Rules apply to PHI in all forms – electronic, written, oral, and any other form.

B. Use of PHI in oral communications. CASE personnel may orally coordinate CASE's services. CASE personnel may discuss a individual's PHI over the telephone with the individual, a physician, or a family member.

C. Documentation of oral communications. CASE is not required to document any information, including oral information, that is used or disclosed for treatment, payment, or health care operations. However, where the Privacy and Security Rules or CASE's Privacy and Security Policies require documentation of other types of disclosures, oral communications are included in such requirement. For example, oral disclosures of PHI for purposes other than treatment, payment, or

health care operations must be documented in order to provide an individual with a complete accounting of disclosures.

D. CASE's duty to safeguard PHI. It is CASE's policy to reasonably safeguard PHI, including oral information, from any intentional or unintentional uses or disclosures that are in violation of the Privacy and Security Rules or CASE's

privacy and security policies. This means that CASE will make reasonable efforts to prevent improper uses and disclosures of PHI. Such measures include, where practical:

IX. DECEASED INDIVIDUALS

It is CASE's policy to protect the PHI of deceased individuals in accordance with the Privacy and Security Rules and CASE's Privacy and Security Policies for as long as CASE maintains the information.

X. PERSONAL REPRESENTATIVES

CASE must treat a person as the personal representative of an individual if the person is, under applicable Ohio or federal law, authorized to act on behalf of the individual in making decisions related to health care. However, the representative must be treated as the individual only to the extent that PHI is relevant to the matters on which the personal representative is authorized to represent the individual. For instance, if the personal representative is authorized to act on the individual's behalf only with respect to the individual's treatment for a particular condition, then CASE may disclose to the personal representative only that information that is relevant to the individual's treatment for that condition. In addition, the personal representative's rights are limited by the scope of his or her authority under law.

XI. DE-IDENTIFICATION AND LIMITED DATA SETS

A. Basic standard. Health information is considered de-identified (*i.e.*, not individually identifiable) under the Privacy and Security Rules if it does not identify an individual and CASE has no reasonable basis to believe it can be used to identify an individual. De-identified information is not PHI and therefore the requirements of the rules do not apply to such information.

B. De-identifying information. CASE may de-identify information in two ways:

1. if a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination, and

documents the analysis, that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information; or

2. if CASE removes from the information all items on a list of specified identifying information about the individual or his or her relatives,

employers, or household members, and CASE has no actual knowledge that the information could be used alone or in combination to identify a subject of the information.

C. Use of PHI to create de-identified information. CASE may use PHI to create de-identified information, or may disclose PHI to a business associate for such purpose, whether or not the de-identified information will be used by CASE.

D. Re-identification. If de-identified information is re-identified at some point by CASE, it becomes subject to the Privacy and Security Rules again and may only be used or disclosed in compliance with the Privacy and Security Rules and CASE's Policies and Procedures.

E. Limited data set. CASE may use PHI, or disclose PHI to a business associate, for the creation of a limited data set. A limited data set may be used or disclosed only for the purposes of research, public health, or health care operations, so long as CASE enters into a data use agreement with the recipient of the limited data set.

1. A limited data set is PHI that excludes specified direct or "facial" identifiers of the individual or of relatives, employers, or household members of the individual.

2. A data use agreement between CASE and the limited data set recipient must:

a. establish the permitted uses and disclosures of such information by the limited data set recipient;

b. prohibit the limited data set recipient's use or disclosure of the information in a manner that would violate the Privacy and Security Rules if done by CASE;

c. establish who is permitted to use or receive the limited data set; and

d. provide that the limited data set recipient will:

i. not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

ii. use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

iii. report to CASE any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

iv. ensure that any agents, including a subcontractor, to whom it provides the limited data set, agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

v. not identify the information or contact the individuals.

GENERAL USE AND DISCLOSURE: FREQUENTLY ASKED QUESTIONS

A. *Can a individual have a friend or family member pick up an individual's PHI for delivery to a health care provider?*

Yes. CASE personnel may use professional judgment and experience with common practice to make reasonable inferences of an individual's best interests in allowing another person to pick up an individual's PHI. The fact that a friend arrives at CASE asking to pick up specific PHI for an individual effectively verifies that the friend is involved in the individual's care, so CASE personnel may give the PHI to the friend. The individual does not need to provide CASE with the names of such persons in advance.

B. *Do the minimum necessary requirements prohibit CASE trainees and interns from accessing individuals' PHI in the course of their training?*

No. CASE may give trainees and interns access to PHI if appropriate, so long as the access is the minimum necessary for such training.

C. *In limiting access to PHI, does CASE have to completely restructure workflow systems, including redesigns of space and upgrades of computer systems, in order to comply with the minimum necessary requirements?*

No. CASE is only required to limit access to PHI to those in the workforce who need access based on their roles in CASE. Facility redesigns are generally not necessary to meet the reasonableness standard for minimum necessary uses. CASE may need to make certain adjustments to its facilities, however, to minimize inappropriate access. Examples of such adjustments may include isolating and locking the file cabinets or records rooms, or providing additional security, such as passwords, on computers that contain PHI. CASE may configure record systems to allow access to only certain information, depending in part upon the feasibility of that reconfiguration.

D. *What if CASE believes that a request for PHI seeks more than the minimum necessary?*

CASE must limit the disclosure to the minimum necessary as it sees fit. The rules permit CASE to rely on the judgment of the requesting person in some situations. If such reliance is reasonable despite CASE's concerns, CASE may make the disclosure as requested.

POLICY #4: DISCLOSURES WITHOUT AUTHORIZATION OR PRIOR AGREEMENT POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") may release PHI without a valid authorization or other permission from an individual if the use or disclosure falls within one or more of the exceptions of the Privacy and Security Rules and CASE has complied with all of the conditions required by the exception.

PURPOSE: The purpose of this policy is to explain the situations where the Privacy and Security Rules allow CASE to use or disclose PHI without a written individual authorization or oral permission, and to describe the relevant procedures CASE must follow when using or disclosing PHI in such situations.

I. RELEASE OF PHI FOR PRIORITY PURPOSES

A. General rule. As discussed in CASE's other Policies and Procedures, in many circumstances CASE is allowed to use or disclose individuals' PHI without obtaining any form of permission (*i.e.*, authorization or verbal agreement) from the individual. In such situations CASE may use and disclose PHI to the extent permitted and/or for the purposes allowed under the Privacy and Security Rules.

B. Specific situations where individual permission is not required. Listed below are separate categories of uses and disclosures for which CASE is not required to obtain affirmative permission from the individual prior to disclosure. In any case where there is doubt as to whether a disclosure is permitted, the matter should be referred to CASE's privacy officer for review and handling.

1. Required by law. CASE may use or disclose PHI as required by law, if the use or disclosure complies with and is limited to the relevant requirements of such law.

2. Public health activities. CASE may disclose PHI for the following public health activities:

a. to a public health authority authorized by law to collect or receive information for (i) the purpose of preventing or controlling disease, injury, or disability (*e.g.*, reporting communicable diseases), (ii) the conduct of public health surveillance, investigations or

interventions, and (iii) the purpose of receiving reports of child abuse or neglect; and

b. to a person subject to Food and Drug Administration ("FDA") jurisdiction regarding FDA-regulated products and activities that are the responsibility of that person, for purposes related to the quality, safety or effectiveness of that product or activity, including but not limited to:

(i) collecting or reporting adverse events or product defects or problems such as drug use or labeling problems;

(ii) tracking FDA-regulated products;

(iii) enabling product recalls, repairs, replacement or lookback (including locating and notifying individuals who received products that have been recalled or withdrawn, or that are the subject of lookback); or

(iv) conducting post-marketing surveillance.

3. Health oversight activities. CASE may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, licensure or disciplinary actions; civil, administrative, or criminal proceedings; or other activities necessary for the oversight of the health care system, government benefit programs, or civil rights laws.

4. Judicial and administrative proceedings. CASE may disclose PHI in the course of judicial or administrative proceedings if the request for PHI is made pursuant to a court or administrative order or in response to a subpoena or discovery request (or other lawful process) from a party to the proceeding.

a. If the request is made pursuant to a court or administrative order, CASE may disclose the information requested without additional process. In such cases, CASE may disclose only the information expressly authorized by the order.

b. Without a court order or subpoena issued by a court, CASE must take additional steps to ensure the confidentiality of the information before it is permitted to disclose the minimum PHI necessary to fulfill the request. It is important to differentiate

between subpoenas issued by a court and subpoenas issued by an attorney or a notary public. CASE's privacy officer will determine what steps are required, such as written assurances or a protective order.

c. CASE may consult with its privacy officer and/or legal counsel to determine its obligation to disclose PHI with respect to judicial and administrative proceedings.

5. Law enforcement purposes. CASE may disclose PHI for law enforcement purposes to a law enforcement official as required by law (and not otherwise addressed in CASE's Policies and Procedures) and in compliance with a court ordered warrant, subpoena or summons, a grand jury subpoena, or, under certain circumstances, an administrative subpoena or summons.

If CASE receives an administrative subpoena or summons, CASE may disclose PHI if the PHI is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope to the extent possible, and de-identified information could not reasonably be used instead. CASE will make this assessment in consultation with its privacy officer and/or legal counsel.

In addition, under certain circumstances, CASE may disclose PHI to a law enforcement official:

a. to identify or locate a suspect, fugitive, material witness, or missing person;

b. in response to a request about an individual who is or may be a victim of a crime;

c. about an individual who has died as a result of criminal conduct;

d. where CASE believes that the information constitutes evidence of criminal conduct that occurred on CASE's premises; or

e. where CASE believes the disclosure is necessary to alert law enforcement to the commission and nature of a crime; the location of such crime or the intended victims of such crime; and the identity, description, and location of the perpetrator of the crime.

Under most of these circumstances, either only a limited amount of PHI may be disclosed or there are certain conditions that must be satisfied before the disclosure can be made.

6. Decedents. CASE may disclose PHI about a deceased person to a coroner or medical examiner as may be necessary to ascertain the cause of death or for similar purposes authorized by law.

7. Specialized government functions. Under limited circumstances, CASE may disclose the PHI of armed forces personnel if necessary for a military mission. CASE may also disclose PHI to federal officials for intelligence and national security activities, to federal officials for the provision of protective services to the President of the United States and/or certain other officials, or to a law enforcement or correctional institution official who has custody of the individual and needs the information to provide health care to the individual or to protect the health and safety of others.

8 Workers' compensation. CASE may disclose PHI as necessary to comply with laws relating to workers' compensation or similar programs.

9. Serious threat to health or safety. CASE may disclose PHI if it believes in good faith that the disclosure 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 reasonably able to prevent the threat, or is necessary for law enforcement authorities to identify or apprehend an individual who has committed a violent crime or escaped from a correctional institution.

10. Research. CASE may use or disclose PHI for research purposes pursuant to a waiver of authorization approved by an Institutional Review Board in accordance with all requirements of the Privacy and Security Rules. Any proposed use or disclosure of PHI for research shall be referred to CASE's privacy officer and/or Institutional Review Board. (See CASE's Policies and Procedures, "Research," for more information.)

II. VERIFICATION OF IDENTITY AND AUTHORITY

A. Identity and authority. With the exception of disclosures made pursuant to valid authorizations, prior to disclosing PHI, CASE must verify the identity of a person requesting PHI and the authority of such person to access PHI, if the identity and/or authority is not known.

B. Conditions on disclosures. CASE must obtain any documentation, statements or representations, whether oral or written, from the person requesting the PHI that are a condition of disclosure under the Privacy and Security Rules or other law (*e.g.*, when making certain priority disclosures).

C. Identity of public officials. CASE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

1. if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

2. if the request is in writing, the request is on the appropriate government letterhead;

3. if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

D. Authority of public officials. CASE may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

1. a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or

2. if a request is made pursuant to legal process, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.

III. DOCUMENTATION

A. Log of Disclosures. CASE will maintain a log of these disclosures for purposes of the accounting of disclosures requirement, except that CASE need not maintain a log of disclosures for national security or intelligence purposes or to correctional institutions, as set forth Section I above.

B. Information. CASE's log of these disclosures will include: (i) the name of the entity and/or person to whom the PHI was disclosed; (ii) the date of the disclosure; (iii) a description of the PHI disclosed; and (iv) the purpose of the disclosure.

PRIORITY DISCLOSURES:
FREQUENTLY ASKED QUESTIONS

A. *Do the Privacy and Security Rules require CASE to disclose individuals' PHI for government enforcement of the rules?*

Yes, in some cases. The HHS Office for Civil Rights ("OCR") has the authority to investigate complaints and conduct compliance investigations to ensure that CASE complies with the Privacy and Security Rules. Although the Privacy and Security Rules do not require CASE to send information to the government for a database or similar operation, the government does have the power to investigate allegations that the Privacy and Security Rules have been violated. This power authorizes the government to gain access to PHI, such as when an individual complains to OCR that he or she believes CASE has not properly handled his or her PHI.

The rules limit disclosures to OCR to information that is "pertinent to ascertaining compliance." What information would be needed by OCR depends on the circumstances and the alleged violations. In some cases, no PHI would be needed. For instance, OCR may need to review only a business associate contract to determine whether CASE included appropriate language to protect privacy when it hired an outside company to help with certain functions involving PHI.

Examples of investigations that may require OCR to have access to PHI include but are not limited to:

- allegations that CASE refused to note a request for amendment in a individual's designated record set, or did not provide the individual with appropriate access to his or her PHI;

- allegations that CASE used PHI for marketing purposes without first obtaining the individual's authorization when required to so by the rules. OCR may need to review information in the marketing department that contains PHI to determine whether a violation has occurred.

B. *May CASE disclose PHI to a state board of health that is conducting an investigation or inspection?*

Yes. A board of health would be considered a health oversight agency. Therefore, under the Privacy and Security Rules, CASE could disclose PHI to the board for oversight activities such as audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions where necessary to provide oversight of the health care system, government benefit

programs that have health-related eligibility criteria, and entities subject to government regulatory programs. It is important to note, however, that the rules do not create any new rights of access to health records by oversight agencies and cannot be used as authority to obtain records not otherwise legally available to the oversight agency.

POLICY #5: AUTHORIZATIONS FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will obtain a valid, signed authorization from an individual prior to using or disclosing the individual's PHI for purposes for which an authorization is required under the Privacy and Security Rules.

PURPOSE: The purpose of this policy is to explain: (1) when a written individual authorization is required; (2) the content of a valid authorization; and (3) the relevant procedures CASE will follow when using or disclosing PHI pursuant to a valid authorization.

I. WHEN AN AUTHORIZATION IS REQUIRED

A. An authorization is required before CASE uses or discloses PHI for purposes that are not "permitted purposes".

B. "Permitted purposes" are uses and disclosures of PHI for which an authorization is not required. These uses and disclosures include those made:

1. for treatment, payment, and health care operations;
2. for involvement in the individual's care and notification purposes (with an opportunity to agree or object, as required by the Privacy and Security Rules);
3. as required by law;
4. for public health activities;
5. about victims of abuse, neglect, or domestic violence;
6. for health oversight activities;
7. for judicial and administrative proceedings;
8. for law enforcement purposes;

9. about decedents to coroners, medical examiners and funeral directors;

10. for research purposes, where a waiver has been obtained;

11. to avert a serious threat to health or safety;

12. for specialized government functions;

13. for workers' compensation purposes;

14. to the individual;

15. to the Department of Health and Human Services for enforcement of the Privacy and Security Rules;

16. for marketing communications that are made face-to-face or that involve promotional products of nominal value;

17. to a business associate, if satisfactory assurances are obtained from the business associate;

18. in a limited data set;

19. incident to a permitted use or disclosure;

20. to permit a individual access to his or her own PHI; and

21. to provide an accounting to the individual of disclosures of his or her PHI;

II. CONTENT REQUIREMENTS OF AUTHORIZATION

A. Plain language. All authorizations must be written in "plain language." This means that CASE will make a reasonable effort to:

1. organize material to serve the needs of the reader;

2. write short sentences in the active voice, using "you" and other pronouns;

3. use common, everyday words in sentences; and

4. divide material into short sections.

B. Core elements. Authorizations must contain all of the following core elements:

1. a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

2. the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

3. the name or other specific identification of the person(s), or class of persons, to whom CASE will disclose the information;

4. a description of each purpose of the requested use or disclosure; if the individual is initiating the authorization, the purpose may be described as "at the request of the individual;"

5. an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; the authorization may expire on a specific date, after a specific time period (*e.g.*, 3 years from the date of the signature), or upon the occurrence of an event directly relevant to the individual or the purpose of the use or disclosure (*e.g.*, for the duration of the individual's participation in a drug study); authorizations for research disclosures may state that they expire at the end of the research study or have no expiration;

6. signature of the individual and date; and

7. if the authorization is signed by a personal representative of the individual, a description of the representative's authority to act for the individual.

C. Required notifications. In addition to the core elements, authorizations must contain all of the following notifications:

1. a statement that the individual has the right to revoke the authorization in writing and either a discussion of the exceptions to the right to revoke together with a description of how the individual may revoke the authorization, or, to the extent that this information is included in CASE's Notice of Privacy Practices, a reference to such notice;

2. for most authorizations, a statement that CASE will not condition benefits on the individual's provision of an authorization for the requested uses or disclosures; however, the rendering of research related treatment may be conditioned on the individual providing an authorization for uses and disclosures in connection with such research; and

3. a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by the Privacy and Security Rules.

D. Authorizations for marketing. If the authorization is for a marketing purpose, and the marketing involves any direct or indirect remuneration to CASE from a third party, the authorization must state this fact. For more information on the requirements governing marketing, see CASE's Marketing Policy.

E. Copy to the individual. If CASE requested the authorization, CASE must give the individual a copy of the signed authorization.

F. Non-required elements. Valid authorizations may also contain non-required elements, so long as those additional elements are not inconsistent with the required elements.

G. Defective authorizations. An authorization is not valid if it has any of the following defects:

1. the expiration date has passed or the expiration event is known by CASE to have occurred;

2. the required elements of the authorization have not been filled out completely;

3. the authorization is known by CASE to have been revoked;

4. the authorization lacks a required element.

5. the authorization is not for the use or disclosure of PHI for a research study and it violates the rule on compound authorizations (see Section II.H. below);

6. any material information in the authorization is known by CASE to be false; and

7. the authorization is conditioned upon CASE providing services to the individual, under circumstances where the Privacy and Security Rules do not permit the authorization to be so conditioned.

H. Combining documents. Generally, an authorization for use or disclosure of PHI may not be combined with any other types of documents (*e.g.*, the Notice of Privacy Practices) to create a compound authorization. However, if the authorization is for the use or disclosure of PHI for a research study, it may be

combined with any other type of written permission for the same research study, including a consent to participate in such research. Multiple authorizations for the use or disclosure of PHI may be combined, so long as CASE has not conditioned the provision of treatment or payment on obtaining the authorization.

III. REVOCATION OF AUTHORIZATIONS

A. An individual may revoke an authorization at any time by means of a written revocation, except to the extent that CASE has taken action in reliance upon the authorization.

B. When an individual revokes an authorization, CASE must stop making uses and disclosures pursuant to the authorization to the greatest extent practical, except as otherwise provided in these Policies and Procedures.

C. Despite an individual's right to revoke an authorization, CASE may continue using and disclosing PHI that was obtained prior to the time the individual revokes his or her authorization, as necessary to maintain the integrity of a research study. An individual may not revoke an authorization to the extent the CASE has acted in reliance on the authorization. Accordingly, CASE is permitted to continue to use and disclose PHI already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of a research study. For example, CASE could continue to use and/or disclose PHI in such circumstances to account for a subject's withdrawal from a research study, as necessary to incorporate the information as part of a marketing application submitted to the FDA, to conduct investigations of scientific misconduct, or to report adverse events. However, CASE would not be permitted to continue disclosing additional PHI or to use for its own research purposes PHI not already gathered at the time an individual withdraws his or her authorization.

IV. RECORD RETENTION REQUIREMENT

CASE will document and retain signed authorizations for six years after the date they were last in effect.

AUTHORIZATION: FREQUENTLY ASKED QUESTIONS

A. *Who may sign an authorization?*

The individual who is the subject of the PHI that will be used or disclosed, or a personal representative of the individual, may sign an authorization. If an authorization is signed by a personal representative of the individual, CASE must obtain a description of the representative's authority to act for the individual.

B. *Can CASE refuse to provide health care items or services to a individual who refuses to sign an authorization?*

Except for research related treatment, CASE may not refuse to provide treatment or other health plan benefits to individuals who refuse to sign an authorization. For example, CASE may not refuse to provide dental care services solely because an individual refuses to authorize a disclosure to a pharmaceutical dental care products manufacturer for the purpose of marketing a new product.

C. *Can CASE use or disclose PHI pursuant to an authorization that was obtained from the individual by a different person or entity?*

Yes. Authorizations for use or disclosure of CASE's individual records may be obtained by entities or persons other than CASE. For example, an attorney may obtain a individual's authorization for CASE to disclose PHI to the attorney for use in litigation. Whether the authorization is submitted to CASE by the individual or by another person on the individual's behalf, CASE may not use or disclose the PHI pursuant to an authorization unless the authorization meets the specified requirements set forth above.

D. *Is CASE required to disclose PHI to a third party pursuant to an authorization?*

No. CASE is not required to disclose PHI to a third party pursuant to a individual's authorization. The authorization permits, but does not require, CASE to disclose the requested PHI. For example, if CASE concludes that an authorized request for the individual's PHI is too burdensome (*e.g.*, it requires CASE to review the individual's record and select portions relevant to the request or redact portions not relevant), CASE may instead provide the entire individual record to the individual, who may redact and release more limited information to the third party.

AUTHORIZATION FORM – USE OR DISCLOSURE OF PHI
SAMPLE FORM

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the person or entity authorized to receive the information is not a health plan or health care provider, the released information may no longer be protected by federal privacy regulations.

Individual Name: _____

I.D. No.: _____

Person/entity authorized to provide the information: _____
_____

Person/entity authorized to receive the information: _____
_____

Specific description of information (including dates): _____
_____
_____

The purpose of the use or disclosure is: _____
_____

Will the person or entity requesting the authorization receive financial or in-kind compensation in exchange for using or disclosing the health information described above?

Yes _____ No _____

I understand that my health care and the payment for my health care will not be affected if I do not sign this form.

Initials _____

I understand that I may see and copy the information described on this form if I ask for it, and that I will receive a copy of this form after I sign it.

Initials _____

I understand that this authorization will expire on _____. Initials _____

I understand that I may revoke this authorization at any time by written notice to CASE Privacy Officer, at Case Western Reserve University, at 10900 Euclid Avenue, Cleveland, Ohio 44106. I also understand that if I revoke this authorization, the revocation will not have any effect on actions taken by CASE before CASE received the revocation. I also understand that more information regarding revocation of this authorization may be covered in CASE's Notice of Privacy Practices.

Initials _____

_____
Signature of Individual or Guardian or
Individual's Legal Representative

_____
Date

_____
Printed Name

_____
Relationship of
Legal Representative to Individual

YOU MAY REFUSE TO SIGN THIS AUTHORIZATION

POLICY #6: RESEARCH AND PROTECTED HEALTH INFORMATION POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will use and disclose PHI for research purposes only as permitted under the Privacy and Security Rules.

PURPOSE: The purpose of this policy is to explain: (1) how CASE will use and disclose PHI for research purposes; (2) the relevant procedures CASE will follow when using or disclosing PHI as a limited data set; (3) the rights of an individual with respect to access to PHI being used in clinical trials; and (4) how CASE might account for disclosures of PHI for research purposes.

I. USE AND DISCLOSURE FOR RESEARCH PURPOSES

A. Uses of PHI. PHI may be used in connection with research without an individual's authorization or a waiver of that authorization when used for purposes generally permitted under the Privacy and Security Rules. Accordingly, PHI can be used in the course of research for purposes of treatment, payment and/or health care operations without an individual's authorization or waiver of authorization. (See Policies and Procedures, Disclosures of Protected Health Information Without Authorization or Prior Agreement).

B. Disclosures of PHI. To the extent that CASE or any designated health care component of CASE is acting as a covered entity, it may only disclose PHI for research purposes as permitted under the Privacy and Security Rules. Permitted disclosures may be made as follows:

1. pursuant to a written authorization from the individual who is the subject of the PHI (see Authorization for Use and Disclosure of Protected Health Information);

2. pursuant to a waiver or alteration of the authorization requirements approved by an Institutional Review Board ("IRB");

3. for certain limited purposes preparatory to research; and

4. for certain limited purposes in connection with research concerning decedents.

C. Special Considerations. Research involving treatment of human subjects raises several issues concerning disclosures of PHI. Because CASE does not act as a

covered entity in most instances of research-related treatment, such disclosures of PHI will be made by an entity other than CASE. In such cases, it is the policy of

CASE that the covered entity making the disclosure of PHI is responsible for compliance with all Privacy and Security Rules requirements related to that disclosure.

D. Waiver of Authorization. The Privacy and Security Rules permit disclosure of PHI for research purposes without individual authorizations if an IRB or "privacy board" has waived the authorization requirement. CASE will recognize the IRBs of CASE, The Cleveland Clinic Foundation, MetroHealth System, The Louis Stokes Cleveland Department of Veterans Affairs Medical Center and University Hospitals of Cleveland, and other similarly organized and administered IRBs or privacy boards as competent to grant a waiver for disclosure of PHI without authorization if done so in accordance with their approved policies and in compliance with the Privacy and Security Rules. A waiver approved by any such IRB will be deemed to comply with the Privacy and Security Rules if there is documentation of the following with respect to such authorization or waiver:

1. the identification of the IRB or privacy board which approved the waiver and the date on which that approval was granted

2. that the IRB or privacy board determined that the alteration and waiver satisfied the following three (3) criteria:

a) that the use or disclosure of the PHI as proposed involved no more than a minimal risk of privacy to individuals, based on the presence of at least the finding that the research study included at least the following three (3) elements:

(1) an adequate plan to protect the identifiers from improper use and disclosure;

(2) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention as otherwise required by law; and

(3) adequate written assurances that the PHI will not be re-used or disclosed to any other person or entity except as required by law, or authorized oversight of the research study or for other research for which the use or disclosure of the PHI would be permitted by the Privacy and Security Rules;

b) that research could not practicably be conducted without the waiver or alteration; and

c) the research could not practicably be conducted without access to and use of the PHI.

3. a description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board;

4. a statement that alteration or waiver of authorization has been reviewed and approved under normal expedited review procedures; and

5. a signature of the chair or other member, as designated by the chair of the IRB or privacy board approving the waiver or alteration.

E. Disclosures Preparatory to Research. The Privacy and Security Rules recognize the importance of preparing research protocols as one of its first steps to effective research. For that reason, the Privacy and Security Rules permit a covered entity to disclose PHI to a researcher, without authorization or waiver, if the covered entity obtains from the researcher representations as follows:

1. use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

2. no protected health information is to be removed from the covered entity by the researcher in the course of the review; and

3. the protected health information for which use or access is sought is necessary for the research purposes.

If PHI is made available to a researcher under the above guidelines, no PHI may be removed from the premises where the PHI is reviewed and a researcher preparing the research protocol or reviewing potential research subjects may record only de-identified health information.

If a request for a disclosure of PHI preparatory to research is received by a designated health care component of CASE, CASE may comply with the disclosure request only if all requirements of the Privacy and Security Rules as to such request are satisfied.

F. Research Involving Decedents. The Privacy and Security Rules permit use or disclose of PHI for research without authorization or waiver of authorization

requirements in whole or in part in certain circumstances where research concerns decedents. In such cases, the covered entity making disclosure must obtain from the researcher:

1. a representation that the use or disclosure sought is solely for research on the protected health information of decedents;

2. documentation, at the request of the covered entity, of the death of such individuals; and

3. a representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

If a request for disclosure of PHI concerning decedents is received by a designated health care component of CASE, CASE may comply with the disclosure request only if all requirements of the Privacy and Security Rules as to such request are satisfied.

II. LIMITED DATA SETS

A. Disclosure of a Limited Data Set. The Privacy and Security Rules also permit disclosure of PHI in the form of a limited data set without authorization or waiver of authorization. However, disclosure of limited data set can only be made upon a receipt of a data use agreement by the party making disclosure.

B. Contents of a Limited Data Set. A limited data set is PHI from which the following direct identifiers of the individual or individual's relatives, employers or household members have been removed:

- names;
- postal address information, other than town or city, state, and zip code;
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- social security numbers;
- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;

- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- web universal resource locators (URLs);
- internet protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints; and
- full face photographic images and any comparable images.

C. Data Use Agreement. If CASE makes disclosure of a limited data set, CASE will require the recipient to enter into a data use agreement with CASE. The data use agreement will:

1. establish the permitted uses and disclosures of the PHI by the limited data set recipient, which must be limited to uses and disclosures for research purposes; the data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of the Privacy and Security Rules, if done by CASE;

2. establish who is permitted to use or receive the limited data set; and

3. provide that the limited data set recipient will:

a) not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

b) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

c) report to CASE any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

d) ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

e) not identify the information or contact the individuals.

III. ACCESS TO PHI USED IN RESEARCH

A. Right to Access Records. It is CASE's general policy to grant individuals access to their PHI as required under the Privacy and Security Rules. (See CASE Policies and Procedures, "Right to Access Records".)

B. Restrictions on PHI Used for Research. An exception to the rights of an individual to have access and to receive copies of their PHI applies with respect to PHI used in or related to research. Where PHI was obtained in the course of clinical trials and the individual who is the subject of the PHI agreed to denial of

access to that PHI when consenting to participate in the trial, access to that PHI may be denied for so long as the clinical trial is in process. When the clinical trial is completed, the individual will have the right to inspect and copy his or her PHI.

IV. ACCOUNTING FOR RESEARCH DISCLOSURES

A. General Policy. It is the general policy of CASE to provide an accounting of disclosures of PHI upon requests by an individual. (See CASE policy "Accounting for Disclosures")

B. Research Disclosures. In cases where PHI has been disclosed, pursuant to a waiver of authorization, as described above, the Privacy and Security Rules permit CASE to use an abbreviated method of accounting for such disclosures. CASE may choose to follow this method of accounting for disclosures of PHI for research purposes. These procedures apply where disclosures have been made involving fifty (50) or more individuals and the PHI of the individual requesting disclosure may have been included in such a disclosure. The abbreviated accounting for disclosure must include:

1. the name of the protocol or other research activity in connection with which the disclosure was made;

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

3. a brief description of the type of PHI that was disclosed;

4. the date or period of time during which 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 PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If CASE provides an accounting for research disclosures in accordance with the above procedures, and if it is reasonably likely that the PHI of the individual requesting an accounting was disclosed for the described research protocol or activity, CASE will, at the request of the individual,

assist the individual in contacting the entity that sponsored the research and/or the researcher.

V. COMPLIANCE WITH OTHER PRIVACY AND SECURITY RULE REQUIREMENTS.

A. It is the policy of CASE that all disclosures by a covered component for research purposes shall be conducted in full compliance with all requirements of the Privacy and Security Rules. In cases of research involving treatment, it is the policy of CASE and its IRB that the research protocol shall include satisfactory assurances that with respect to any treatment rendered as part of the research, the provider of such treatment has complied with all applicable requirements to the Privacy and Security Rules.

RESEARCH: FREQUENTLY ASKED QUESTIONS

A. *May PHI ever be used for research purposes without an individual authorization?*

Yes. A recognized IRB, following its own internal and certain procedures specified by the Privacy and Security Rules, is able to grant waivers of authorization requirements that generally apply to a disclosure of PHI.

B. *May I combine an authorization to disclose PHI created, maintained and/or used in the course of research involving human subjects with any other document?*

Yes. An authorization for a research related disclosure of PHI may be combined with an informed consent required under the Common Rule.

C. *May I have access to PHI without an authorization if such access in required to create or refine a research protocol?*

Yes. The Privacy and Security Rules permit certain disclosures of PHI that are preparatory to research if certain conditions are met. These include that the party making disclosure obtain from the researcher representations as follows:

1. use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

2. no protected health information is to be removed from the covered entity by the researcher in the course of the review; and

3. the protected health information for which use or access is sought is necessary for the research purposes.

If PHI is made available to a researcher under the above guidelines, no PHI may be removed from the premises where the PHI is reviewed and a researcher preparing the research protocol or reviewing potential research subjects may record only de-identified health information.

D. *Where can I obtain additional information concerning research and the Privacy and Security Rules?*

Additional information concerning research, the Privacy Rule and the Security Rule is available from the CASE Privacy Officer and the CASE Office of Research Compliance (http://ora.ra.Case.edu/main_research_compliance_page.htm).

POLICY #7: NOTICE OF PRIVACY PRACTICES POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to provide individuals with a Notice of Privacy Practices as specified in the Privacy Rules ("Notice") upon their first receipt of health care items or services through CASE. In addition, in those circumstances where required to do so, CASE will post the Notice in a conspicuous location and will make the Notice available to all individuals upon request.

PURPOSE: The purpose of this policy is to explain: (1) an individual's right to a Notice; (2) the relevant procedures CASE must follow when providing its Notice to individuals; and (3) the requirements for documentation of and revisions to the Notice. Acknowledgment of receipt of the Notice is addressed in the following policy, entitled "Acknowledgment of Receipt of Notice of Privacy Practices."

I. CONTENT OF A NOTICE OF PRIVACY PRACTICES

The Notice shall provide adequate notice of:

1. the uses and disclosures of PHI that CASE may make;

2. the individual's rights with respect to PHI;

3. CASE's legal obligations regarding PHI; and

4. how and to whom to submit complaints or request further information about CASE's privacy policies.

II. PROVIDING THE NOTICE

A. General rules. CASE will follow these rules for providing a paper copy of the Notice to individuals and the public in general.

1. CASE will make the Notice available upon request to any person, even if such person is not receiving services from CASE.

2. CASE will provide the Notice to the individual no later than the date that CASE first provides health care services or items to the individual in a transaction that involves PHI. In emergency treatment situations, the

Notice will be provided as soon after the emergency as is reasonably practicable. CASE may send the Notice at one time to all persons to whom it provides services, give the Notice to each individual as he or she receives services or items from CASE, give the Notice to an individual when the individual contacts CASE electronically, or by any combination of these approaches.

3. CASE will have the Notice available for delivery to individuals upon request.

4. When required to do so by the Privacy Rules, CASE will post the Notice in a clear and prominent location in the Dental Clinic where individuals will be able to read it.

5. Any CASE group health plan obligated to do so under the Privacy Rules will provide a Notice to individuals covered by the plan as of April 14, 2003 and, thereafter, at the time of enrollment, to individuals who are new enrollees in the plan. Any such plan will also provide a revised Notice to all participants in such plan within (sixty) 60 days of a material revision to the Notice. In addition, no less frequently than once every three years, the plan will notify individuals then covered by the plan of the availability of the Notice and how to obtain the Notice. A plan may satisfy its obligation to deliver a Notice either by itself providing the Notice, or, when permitted under the Privacy Rules to do so, by having the Notice provided by an insurer that issues a contract of insurance which funds plan benefits.

B. Electronic notice. CASE may be required to provide its Notice electronically under certain circumstances.

1. If CASE maintains a web site that provides information about CASE's services or benefits, it must prominently post its Notice on the web site and make the Notice available electronically through the web site.

2. CASE may provide the Notice to an individual by e-mail, if the individual agrees to receive materials from CASE electronically and the individual has not withdrawn his or her agreement. If CASE knows that the e-mail transmission failed, CASE must provide a paper copy of the Notice to the individual.

3. If service is first delivered to an individual electronically, CASE must provide electronic notice automatically and contemporaneously with the individual's first request for service.

4. If an individual receives an electronic Notice from CASE, he or she still has the right to obtain a paper copy of the Notice from CASE upon request.

III. REVISIONS TO THE NOTICE

A. The right to change the Notice. In its Notice, CASE has reserved the right to change its privacy practices. If CASE will apply any such changes to PHI previously created or retained, it must make a statement to that effect in the Notice.

B. Making material changes to the Notice. CASE will revise its Notice whenever there is a material change to the uses or disclosures of PHI, the individuals' rights, CASE's legal obligations, or other privacy practices stated in the Notice.

1. Whenever the Notice is revised, CASE will make the Notice available upon request on or after the effective date of the revision, make the Notice available to patients of the Dental Clinic, and post the revised Notice in a clear and prominent location.

2. After giving an individual a copy of the Notice upon his or her first visit or delivery of a service or item, CASE is not required to further distribute the Notice to the individual. Except as described above with respect to health plans, even if CASE revises the Notice, it is not required to distribute the Notice to persons who have already received the Notice. Under such circumstances, CASE only has to make the Notice available upon request and post the information in a prominent location.

C. Implementation of revised privacy practices. In general, CASE may not implement a material change to any term of the Notice before the effective date of the Notice that reflects the material change. This means that CASE must revise its Notice accordingly and make it available to individuals before it may implement any new or different privacy practices.

IV. DOCUMENT RETENTION REQUIREMENTS

CASE must retain a copy of each Notice it issues for a period of six years from the date that the Notice was last in effect.

NOTICE OF PRIVACY PRACTICES: FREQUENTLY ASKED QUESTIONS

A. *Are CASE personnel required to explain the Notice to individuals?*

No. The Notice must be written in plain language so that the average reader will be able to understand it. Patients who have questions may be referred to the CASE contact person and telephone number listed in the Notice.

B. *Can CASE distribute the Notice to individuals as part of other publications or communications?*

Yes, in many circumstances. For example, the Notice and the individual acknowledgment form may be included in the same document. However, the Notice may not be combined in a single document with an authorization.

C. *Is CASE required to respond to requests for the Notice from the general public?*

Yes. In order to allow individuals to use the Notice to compare privacy practices and to select a provider, CASE must provide the Notice to any person who requests a copy, including members of the general public who are not patients of the CASE Dental Clinic.

FORM OF NOTICE -- GENERAL

CASE WESTERN RESERVE UNIVERSITY
NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice will tell you about the ways in which CASE WESTERN RESERVE UNIVERSITY ("CASE") protects, uses and discloses your protected health information ("PHI"). This Notice also describes your rights and certain obligations we have regarding the use and disclosure of PHI. If you have any questions about this Notice of Privacy Practices ("Notice"), please contact CASE's Privacy Officer, at CASE WESTERN RESERVE UNIVERSITY, 10900 Euclid Avenue, Cleveland, Ohio 44106.

PHI means any information, transmitted or maintained in any form or medium, which CASE creates or receives that relates to your physical or mental health, the delivery of health care services to you or payment for health care services and that identifies you or could be used to identify you. We maintain your PHI in a record we create of the services and items you receive from CASE. This Notice applies to all of those records created, received or maintained by CASE.

We are required by law to: make sure that PHI is kept private; give you this Notice of our legal duties and privacy practices with respect to your PHI; and comply with the currently effective terms of this Notice.

HOW WE MAY USE AND DISCLOSE PHI ABOUT YOU

The following paragraphs describe different ways that we use and disclose PHI.

Use for Treatment, Payment, or Health Care Operations

We are permitted to use and disclose your PHI (1) to provide treatment to you, (2) to be paid or request payment for our services, and (3) to conduct health care operations. This section of this Notice discusses each of these types of uses and disclosures of PHI.

- **For Treatment.** We may use PHI about you to provide you with health care treatment or services. For example, we may use your PHI when performing dental procedures. We may disclose PHI about you to CASE personnel, as well as to doctors, nurses, hospitals, clinics, or other health care providers who are involved in your care. For example, a doctor treating you for a medical condition may need to know the medications which have been prescribed for you, or the services and items that have been provided to you. CASE may also share PHI about you in order to coordinate health care services and items that you may need.

- **For Payment.** We may use and disclose PHI about you so that the services and items that you receive from CASE may be billed to and payment may be collected from you, an insurance company, or a third party payor. For example, we may need to give your health plan information about the services or items that you received so that your health plan will pay us or reimburse you for the services or items.

- **For Health Care Operations.** We may use and disclose PHI about you for health care operations. These uses and disclosures are necessary to make sure you receive quality care. For example, we may use PHI to review our treatment and services and to evaluate the performance of our staff in providing services to you. We may also disclose information to doctors, nurses, hospitals, clinics, and other health care providers, for review and learning purposes. We may remove information that identifies you from this set of PHI so others may use it to study health care and health care delivery without learning the names of the specific individuals.

Other Uses and Disclosures of PHI

Listed below are a number of other ways that CASE is permitted or required to use or disclose PHI. This list is not exhaustive.

Therefore, not every use or disclosure in a category is listed.

- **Appointment Reminders.** We may use and disclose protected health information to contact you as a reminder that you have an appointment with us.

- **Individuals Involved in Your Care or Payment for Your Care.** We may release PHI about you to a friend or family member who is involved in your medical care. We may share PHI about you with family members or friends who accompany you to the Dental Clinic. We may also give information to someone who helps pay for your care. In addition, we may disclose PHI about you to a person or entity assisting in an emergency so that your family can be notified about your condition, status and location.

- **As Required By Law.** We will disclose PHI about you when required to do so by federal, state, or local law.

- **Public Health Risks.** We may disclose PHI about you for public health activities, including to prevent or control disease or, when required by law, to notify public authorities concerning cases of abuse or neglect.

- **Health Oversight Activities.** We may disclose PHI to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure.

- **Lawsuits and Disputes.** If you are involved in a lawsuit or dispute, we may disclose PHI about you in response to a court or administrative order. We may also disclose PHI about you 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 PHI if asked to do so by a law enforcement official as permitted by law.

- **Coroners and Medical Examiners**. We may release PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death.

- **Research.** Under certain circumstances, we may use and disclose PHI about you for research purposes. For example, we might disclose PHI to be used in a research project involving the effectiveness of certain dental procedures. In some cases, we might disclose PHI for research purposes without your knowledge or approval. However, such disclosures will be made only if approved through a special process. This process evaluates a proposed research project and its use of PHI, trying to balance the research needs with an individual's need for privacy of their PHI.

- **To Avert a Serious Threat to Health or Safety.** We may use and disclose PHI about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.

- **Military and Veterans.** If you are a member of the armed forces, we may release PHI about you as required by military command authorities.

- **Health-Related Benefits and Services.** We may use and disclose PHI to tell you about health-related benefits or services that may be of interest to you.

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

- **Fundraising**. We may disclose PHI about you for fundraising purposes. Any such disclosure of PHI will be limited in scope and disclosed only to our business associates or to a charitable organization which is obligated to act for the benefit of CASE. If you do not want CASE to contact you about fundraising, you must notify the CASE Privacy Officer in writing. Further information about disclosures for fundraising purposes may be found in CASE's Policies and Procedures, "Fundraising."

Other uses and disclosures will be made only upon your written authorization. You also have the right to revoke such authorization, in writing, except where we have previously taken action in reliance on your prior authorization or if the authorization was a condition to obtaining insurance or health plan coverage and applicable law provides the insurer or health plan with the right to contest a claim under the policy.

Certain provisions of Ohio law may now, or in the future, impose greater restrictions on uses and/or disclosures of PHI or otherwise be more stringent than federal rules protecting the privacy of PHI. If such provisions of Ohio law apply to a use or disclosure of PHI or under other circumstances described in this Notice, CASE must comply with those provisions.

When required to do, the Plan will disclose only the minimum amount of PHI necessary to accomplish the intended purpose of a use, disclosure or request for PHI.

YOUR RIGHTS REGARDING PHI

You have the following rights with respect to your PHI:

- **Right to Inspect and Copy.** You have the right to inspect and copy your PHI maintained by CASE. Generally, this information includes health care and billing records. You do not have a right of access to (1) psychotherapy notes; (2) information prepared in anticipation of or for use in, a civil, criminal, or administrative action; and (3) PHI maintained by CASE that is (a) subject to the Clinical Laboratory Improvements Amendments ("CLIA") of 1988, 42 U.S.C. 263a, if access to the individual would be prohibited by law, or

(b) exempt from CLIA pursuant to 42 CFR 493.3(a)(2). Under certain circumstances, you also do not have a right of access to information created or obtained in the course of research involving treatment or received from someone other than a health care provider under a promise of confidentiality.

To inspect and copy PHI maintained by CASE, you must submit your request in writing to CASE's Privacy Officer. We may charge a fee for the costs of copying, mailing or other supplies associated with you request. We may deny your request to inspect and copy your PHI for the reasons set forth above or under certain other limited circumstances. If you are denied access to PHI other than for a reason stated above, you will receive a written denial. You may request that the denial be reviewed. Thereafter, a licensed health care provider chosen by CASE will review your request and the denial. The person conducting the review will not be the person who originally denied your request. We will comply with the outcome of the review.

- **Right to Request Amendment.** You may ask us to amend the PHI we have about you. You have the right to request an amendment for so long as the information is kept by or for CASE. To request an amendment to your PHI, your request must be made in writing and submitted to CASE's Privacy Officer. In addition, you must provide a reason that supports your request. We will generally make a decision regarding your request for amendment no later than 60 days after receipt of your request. However, if we are unable to act on the request within this time, we may extend the time for 30 more days but we will provide you with a written notice of the reason for the delay and the approximate time for completion. If we deny your requested amendment, we will provide you with a written denial.

  We have the right to deny your request for an amendment if it is not in writing or does not include a reason to support the request. We are not required to agree to your request if you ask us to amend PHI that: was not created by us, unless the person or entity that created the information is no longer available to make the amendment; is not part of the PHI kept by or for CASE; is not part of the PHI which you would be permitted to inspect and copy; or is already accurate and complete.

- **Right to an Accounting of Disclosures.** You have the right to request an "accounting of disclosures." This is a list of certain disclosures of PHI we have made about you. We do not have to list certain disclosures such as those made for the purposes of treatment, payment, or healthcare operations, pursuant to a prior authorization by you or for certain law enforcement purposes.

  To request this list or accounting of such disclosures, your request must be submitted in writing to CASE's Privacy Officer. Your request must also state a time period, which may not be longer than six (6) years and may not include dates before April 14, 2003. Your request should also specify the format of the list you prefer (i.e. on paper or electronically). The first list you request within a twelve (12) month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the costs involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restriction of Uses and Disclosures.** You have the right to request that we restrict the uses and disclosures of PHI about you to carry out treatment, payment or health care operations and/or to individuals involved in your care. We cannot restrict disclosures required by law or requested by the federal government to determine if we are meeting our privacy protection obligations. *We are not required to agree to your request;* however, if we do agree, we will comply with your request unless the information is needed to provide you emergency health care treatment. To request restrictions, you must make your request in writing to CASE's Privacy Officer. Your request must specify (1) what PHI you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply (i.e., disclosures to your spouse). We may terminate our agreement to the restriction if you orally agree to the termination and it is documented, you request the termination in writing, or we inform you that we are terminating our agreement with respect to any information created or received after receipt of our notice.

- **Right to Request Confidential Communications.** You also have the right to request that we communicate with you about health care matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make you request in writing to CASE's Privacy Officer. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- **Right to Receive Notice Electronically.** 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. To obtain a paper copy of this notice, please write to or call CASE's Privacy Officer.

CHANGES TO THIS NOTICE

We reserve the right to change our privacy practices that are described in this Notice. We reserve the right to make the revised or changed privacy practices applicable to PHI we already have about you as well as any information we receive in the future. A copy of our current notice will be posted at CASE. Prior to a material change to the uses or disclosures, your rights, our legal duties, or other privacy practices stated in this Notice, we will promptly revise the Notice. The Notice will contain the effective date on the first page.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with CASE or with the Secretary of the Department of Health and Human Services. To file a complaint with CASE, write to CASE's Privacy Officer. All complaints must be in writing. ***You will not be penalized or retaliated against for filing a complaint.***

OTHER USES OF PHI

Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you provide us permission to use or disclose PHI about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose PHI about you for the reasons covered by your written authorization. You understand that we are unable to retract any disclosures we have already made with your authorization, and that we are required to retain our records of the care that we provided to you.

ACKNOWLEDGMENT OF

RECEIPT OF NOTICE OF PRIVACY PRACTICES

I acknowledge receipt of CASE's Notice of Privacy Practices.

Date: _____

_____
Signature of Patient, Guardian or Legal Representative

_____
Printed Name of Patient, Guardian or Legal Representative

_____
Relationship of Guardian or Legal Representative to Patient

The individual or the individual's legal representative did not provide a written acknowledgment of receipt of this Notice of Privacy Practices. The following explains the good faith efforts to obtain the written acknowledgment and the reasons why the acknowledgment was not obtained: _____
_____
_____
_____
_____

FORM ON NOTICE BY GROUP HEALTH PLANS

CASE WESTERN RESERVE UNIVERSITY
EMPLOYEE WELFARE BENEFIT PLANS
NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003

THIS NOTICE OF PRIVACY PRACTICES DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice will tell you about the ways in which the CASE WESTERN RESERVE UNIVERSITY employee welfare benefit plans (collectively, the "Plan") protect, use and disclose your protected health information ("PHI"). This Notice also describes your rights and certain obligations we have regarding the use and disclosure of PHI. If you have any questions about this Notice of Privacy Practices ("Notice"), please contact CASE's Privacy Officer, at CASE WESTERN RESERVE UNIVERSITY, 10900 Euclid Avenue, Cleveland, Ohio 44106.

PHI means any information, transmitted or maintained in any form or medium, which the Plan creates or receives that relates to your physical or mental health, the delivery of health care services to you or payment for health care services and that identifies you or could be used to identify you. We maintain your PHI in records we create of claims submitted to or payments made by the Plan and related information. This Notice applies to all of those records created, received or maintained by the Plan.

We are required by law to: make sure that PHI is kept private; give you this Notice of our legal duties and privacy practices with respect to your PHI; and comply with the currently effective terms of this Notice.

HOW WE MAY USE AND DISCLOSE PHI ABOUT YOU

The following paragraphs describe different ways that we use and disclose PHI.

Use for Treatment, Payment, or Health Care Operations

We are permitted to use and disclose your PHI (1) to provide treatment to you, (2) to be paid or request payment for our services, and (3) to conduct health care operations. This section of this Notice discusses each of these types of uses and disclosures of PHI.

- **For Treatment.** We may use PHI about you in connection with health care treatment or services. We may disclose PHI to doctors, nurses, hospitals, clinics, or other health care providers who are involved in your care. For example, a doctor treating you for a medical condition may need to know the medications which have been prescribed for you, or the services and items that have been provided to you. We may also share PHI about you in order to coordinate health care services and items that you may need.
- **For Payment.** We may use and disclose PHI about to process payments for the services and items that you receive from health care providers For example, we may need to share your health information with a provider to verify the delivery of services or items that you received so that the Plan can pay the provider or reimburse you for the services or items.
- **For Health Care Operations.** We may use and disclose PHI about you for health care operations. These uses and disclosures are necessary to make sure you receive quality care. For example, we may use PHI to review treatment and services and to evaluate the performance of providers. We may also disclose information to doctors, nurses, hospitals, clinics, and other health care providers, for review and learning purposes. We may remove information that identifies you from PHI used for such purposes so others may use it to study health care and health care delivery without learning the names of the specific individuals.

Other Uses and Disclosures of PHI

Listed below are a number of other ways that the Plan is permitted or required to use or disclose PHI. This list is not exhaustive. Therefore, not every use or disclosure in a category is listed.

- **Individuals Involved in Your Care or Payment for Your Care.** We may release PHI about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose PHI about you to a person or entity assisting in an emergency so that your family can be notified about your condition, status and location.
- **As Required By Law.** We will disclose PHI about you when required to do so by federal, state, or local law.
- **Public Health Risks.** We may disclose PHI about you for public health activities, including to prevent or control disease or, when required by law, to notify public authorities concerning cases of abuse or neglect.
- **Health Oversight Activities.** We may disclose PHI to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure.
- **Lawsuits and Disputes.** If you are involved in a lawsuit or dispute, we may disclose PHI about you in response to a court or administrative order. We may also disclose PHI about you 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 PHI if asked to do so by a law enforcement official as permitted by law.
- **Coroners and Medical Examiners**. We may release PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death.
- **Research.** Under certain circumstances, we may use and disclose PHI about you for research purposes. For example, we might disclose PHI to be used in a research project involving the effectiveness of certain treatment. In some cases, we might disclose PHI for research purposes without your knowledge or approval. However, such disclosures will be made only if approved through a special process. This process evaluates a proposed research project and its use of PHI, trying to balance the research needs with an individual's need for privacy of their PHI.
- **To Avert a Serious Threat to Health or Safety.** We may use and disclose PHI about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.
- **Military and Veterans.** If you are a member of the armed forces, we may release PHI about you as required by military command authorities.
- **Health-Related Benefits and Services.** We may use and disclose PHI to tell you about health-related benefits or services that may be of interest to you.
- **Workers' Compensation.** We may release PHI about you for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.
- **Fundraising**. We may disclose PHI about you for fundraising purposes. Any such disclosure of PHI will be limited in scope and disclosed only to our business associates or to a charitable organization which is obligated to act for the benefit of CASE. If you do not want CASE to contact you about fundraising, you must notify the CASE Privacy Officer in writing. Further information about disclosures for fundraising purposes may be found in CASE's Policies and Procedures, "Fundraising."

Other uses and disclosures will be made only upon your written authorization. You have the right to revoke such authorization, in writing, except where we have previously taken action in reliance on your prior authorization or if the authorization was a condition to obtaining insurance or health plan coverage and applicable law provides the insurer or health plan with the right to contest a claim under the policy.

When required to do, the Plan will disclose only the minimum amount of PHI necessary to accomplish the intended purpose of a use, disclosure or request for PHI.

MORE STRINGENT LAWS

Certain provisions of Ohio law may now, or in the future, impose greater restrictions on uses and/or disclosures of PHI or otherwise be more stringent than federal rules protecting the privacy of PHI. If such provisions of Ohio law apply to a use or disclosure of PHI or under other circumstances described in this Notice, CASE must comply with those provisions.

YOUR RIGHTS REGARDING PHI

You have the following rights with respect to your PHI:

- **Right to Inspect and Copy.** You have the right to inspect and copy your PHI maintained by the Plan. Generally, this information includes health care and billing records. You do not have a right of access to (1) psychotherapy notes; (2) information prepared in anticipation of or for use in, a civil, criminal, or administrative action; and (3) PHI maintained by the Plan that is (a) subject to the Clinical Laboratory Improvements Amendments ("CLIA") of 1988, 42 U.S.C. 263a, if access to the individual would be prohibited by law, or (b) exempt from CLIA pursuant to 42 CFR 493.3(a)(2). Under certain circumstances, you also do not have a right of access to information created or obtained in the course of research involving treatment or received from someone other than a health care provider under a promise of confidentiality.

  To inspect and copy PHI maintained by the Plan, you must submit your request in writing to CASE's Privacy Officer. We may charge a fee for the costs of copying, mailing or other supplies associated with you request. We may deny your request to inspect and copy your PHI for the reasons set forth above or under certain other limited circumstances. If you are denied access to PHI other than for a reason stated above, you will receive a written denial. You may request that the denial be reviewed. Thereafter, a licensed health care provider chosen by CASE will review your request and the denial. The person conducting the review will not be the person who originally denied your request. We will comply with the outcome of the review.

- **Right to Request Amendment.** You may ask us to amend the PHI we have about you. You have the right to request an amendment for so long as the information is kept by or for the Plan. To request an amendment to your PHI, your request must be made in writing and submitted to CASE's Privacy Officer. In addition, you must provide a reason that supports your request. We will generally make a decision regarding your request for amendment no later than 60 days after receipt of your request. However, if we are unable to act on the request within this time, we may extend the time for 30 more days but we will provide you with a written notice of the reason for the delay and the approximate time for completion. If we deny your requested amendment, we will provide you with a written denial.

  We have the right to deny your request for an amendment if it is not in writing or does not include a reason to support the request. We are not required to agree to your request if you ask us to amend PHI that: was not created by us, unless the person or entity that created the information is no longer available to make the amendment; is not part of the PHI kept by or for the Plan; is not part of the PHI which you would be permitted to inspect and copy; or is already accurate and complete.

- **Right to an Accounting of Disclosures.** You have the right to request an "accounting of disclosures." This is a list of certain disclosures of PHI we have made about you. We do not have to list certain disclosures such as those made for the purposes of treatment, payment, or healthcare operations, pursuant to a prior authorization by you or for certain law enforcement purposes.

  To request this list or accounting of such disclosures, your request must be submitted in writing to CASE's Privacy Officer. Your request must also state a time period, which may not be longer than six (6) years and may not include dates before April 14, 2003. Your request should also specify the format of the list you prefer (i.e. on paper or electronically). The first list you request within a twelve (12) month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the costs involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Request Restriction of Uses and Disclosures.** You have the right to request that we restrict the uses and disclosures of PHI about you to carry out treatment, payment or health care operations and/or to individuals involved in your care. We cannot restrict disclosures required by law or requested by the federal government to determine if we are meeting our privacy protection obligations. *We are not required to agree to your request;* however, if we do agree, we will comply with your request unless the information is needed to provide you emergency health care treatment. To request restrictions, you must make your request in writing to CASE's Privacy Officer. Your request must specify (1) what PHI you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply (i.e., disclosures to your spouse). We may terminate our agreement to the restriction if you orally agree to the termination and it is documented, you request the termination in writing, or we inform you that we are terminating our agreement with respect to any information created or received after receipt of our notice.

- **Right to Request Confidential Communications.** You also have the right to request that we communicate with you about health care matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential communications, you must make you request in writing to CASE's Privacy Officer. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- **Right to Receive Notice Electronically.** 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. To obtain a paper copy of this notice, please write to or call CASE's Privacy Officer.

CHANGES TO THIS NOTICE

We reserve the right to change our privacy practices that are described in this Notice. We reserve the right to make the revised or changed privacy practices applicable to PHI we already have about you as well as any information we receive in the future. Prior to a

material change to the uses or disclosures, your rights, our legal duties, or other privacy practices stated in this Notice, we will promptly revise the Notice. The Notice will contain the effective date on the first page.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with CASE or with the Secretary of the Department of Health and Human Services. To file a complaint with CASE, write to CASE's Privacy Officer. All complaints must be in writing. ***You will not be penalized or retaliated against for filing a complaint.***

OTHER USES OF PHI

Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you provide us permission to use or disclose PHI about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose PHI about you for the reasons covered by your written authorization. You understand that we are unable to retract any disclosures we have already made with your authorization, and that we are required to retain records of the Plan relating to claims, coordination of benefits, payments by the Plan and related matters.

POLICY #8: ACKNOWLEDGMENT OF NOTICE OF PRIVACY PRACTICES POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to make a good faith effort to obtain each individual's written acknowledgment that the individual has received CASE's Notice of Privacy Practices ("Notice") upon the individual's first receipt of health care items or services through CASE.

PURPOSE: The purpose of this policy is to explain: (1) when CASE is required to obtain an acknowledgment; (2) the relevant procedures CASE must follow when obtaining the acknowledgment from individuals; and (3) the requirements for documentation of the acknowledgment process.

I. OBTAINING AN ACKNOWLEDGMENT

A. Acknowledgment requirement. Except in an emergency, CASE must make a good faith effort to obtain an individual's written acknowledgment of receipt of the Notice no later than the date of the first delivery of health care services to the individual, including services delivered electronically. If the Notice that is delivered electronically as part of first service or item delivery, CASE must be capable of capturing the individual's acknowledgment of receipt electronically. It is anticipated that CASE will be obligated to deliver Notices and obtain acknowledgements of such deliveries only in connection with services rendered by the Dental Clinic and "faculty practice plan" of the CASE Dental School.

B. Patient's failure to provide acknowledgment. If an individual refuses or otherwise fails to provide an acknowledgment, CASE must document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained (*e.g.*, the individual refused to sign the acknowledgment after being requested to do so). CASE is not prohibited from providing treatment or otherwise using or disclosing PHI as permitted by law if the individual does not sign an acknowledgment after having been asked to do so.

C. Single acknowledgment. Only one signed acknowledgment is required per individual. CASE is not required to collect a signed acknowledgment every time an individual receives services. Even if CASE's Notice is revised, CASE is not required to ask individuals to sign a new acknowledgment.

D. Log book. CASE may utilize any practical means of recording the receipt of acknowledgements.

II. RECORD RETENTION REQUIREMENTS

CASE will retain copies of any written acknowledgments of receipt of the Notice, or, if not obtained, documentation of its good faith efforts to obtain such written acknowledgment. CASE will retain this documentation from the date of its creation until six years after the date when it was last in effect.

ACKNOWLEDGMENT OF NOTICE OF PRIVACY PRACTICES: FREQUENTLY ASKED QUESTIONS

A. *May CASE use a logbook that individuals sign after receipt of a Notice of Privacy Practices to comply with the acknowledgment requirements?*

Yes. CASE may have the individual sign or initial an acknowledgment within a log book that individuals sign when they receive a Notice of Privacy Practices, so long as the individual is clearly informed on the log book of what they are acknowledging. However, the acknowledgment must be separate and distinct from any other acknowledgment or any grant of waiver or permission.

B. *How can CASE comply with the acknowledgment requirement if an individual has a personal representative?*

If an individual has a personal representative, such as the parent of a minor, the personal representative may sign the acknowledgment on behalf of the individual. But if the individual is unable to sign an acknowledgement and is not accompanied by her or his personal representative, CASE may choose to send the Notice of Privacy Practices and acknowledgment to the personal representative and provide instructions for the personal representative to send the acknowledgment back via mail or drop it off during the next visit to CASE.

ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES
SAMPLE FORM

The undersigned acknowledges receipt of this Notice of Privacy Practices.

Date: _____

_____
Signature of Patient
Or Legal Representative

_____
Printed Name

_____
Relationship of
Legal Representative to Patient

The individual or the individual's legal representative did not provide a written acknowledgment of receipt of this Notice of Privacy Practices. The following explains the good faith efforts to obtain the written acknowledgment and the reasons why the acknowledgment was not obtained: _____
_____
_____
_____.

POLICY #9: USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR FUNDRAISING POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will use PHI for fundraising purposes only as permitted under the Privacy Rules.

PURPOSE: The purpose of this policy is to explain when and under what circumstances CASE might use PHI for fundraising purposes.

I. GENERAL RULES

A. CASE may use or disclose to a business associate or to an institutionally related foundation, as defined below, the following PHI for the purpose of raising funds for its own benefit:

1. Demographic information relating to an individual; and
2. Dates of services provided to an individual.

For these purposes, demographic information includes an individual's name, address and other contact information, age, gender and insurance status. The term does not include any information about illnesses or treatment.

B. CASE will comply with the procedural requirements of these policies and procedures for fundraising related uses and/or disclosures of PHI whenever using or disclosing PHI in connection with its fundraising activities.

II. PROCEDURAL REQUIRMENTS

A. Notice of Privacy Practices. CASE will include in its notice of privacy practices a disclosure that CASE might use or disclose PHI for fundraising purposes and might contact an individual as part of its fundraising efforts. The notice of privacy practices shall also provide information on how an individual can opt out of receiving fundraising materials.

B. Opt Out Information. Any fundraising materials disseminated on behalf of CASE in connection with which there has been a disclosure of PHI will

include a description of how the recipient can opt-out of receiving future fundraising materials.

C. Implementation of Opt Out Elections. If CASE receives notice from an individual that he or she desires to opt out of receiving additional fundraising communications, CASE will use its best efforts to insure that such individuals do not receive any further fundraising communications.

FUNDRAISING: FREQUENTLY ASKED QUESTIONS

A. *May CASE disclose PHI for fundraising purposes?*

Yes. However, CASE may disclose only a limited amount of PHI for these purposes and may make such disclosure only to a business associate or to a tax-exempt, charitable foundation which has as its mission the support of CASE.

B. *What if an individual does not want to receive fundraising materials?*

CASE must disclose in any fundraising materials in connection with which PHI was used or disclosed information on how an individual can elect to not receive any additional similar materials. CASE must use its best efforts to honor all such requests.

CASE WESTERN RESERVE UNIVERSITY

HIPAA POLICIES

POLICY #10: MARKETING POLICIES AND PROCEDURES

POLICY: Any marketing communications by Case Western Reserve University ("CASE') which involve PHI must comply with the Privacy Rules' specific requirements for such communications as well as any applicable state law or regulations.

PURPOSE: The purpose of this policy is to assist CASE in complying with requirements of the Privacy Rules governing marketing practices that involve PHI.

I. DEFINITION OF MARKETING

A. Marketing defined. Marketing is a communication about a product or service that encourages recipients of the communication to buy or use the product or service. Marketing specifically includes an arrangement between CASE and a third party whereby CASE discloses PHI, in exchange for direct or indirect remuneration, to assist the third party or its affiliate to make a communication about its own product(s) or service(s) that encourages recipients of the communication to purchase or use such product(s) or service(s).

B. Exceptions to the definition of marketing. Marketing does not include communications made by CASE:

1. for the individual's treatment;

2. for case management or care coordination for the individual, or to recommend alternative treatments, therapies, health care providers, or settings of care; or

3. to describe a health-related product or service (or payment for such product or service) that is provided by CASE, or included in a plan of benefits of CASE, including communications about the entities participating in a health care provider or health plan network, replacement of, or enhancements to, a health plan, 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.

C. Examples of exceptions. Examples of communications that should not be considered marketing include, but are not limited to, communications regarding the following:

1. certain therapeutic substitution recommendations;

2. information regarding insurance coverage and formularies;

3. counseling and drug utilization review (DUR);

4. certain disease management activities; and

5. general health information, such as communications that explain how to lower cholesterol or enroll in wellness programs.

II. USE AND DISCLOSURE OF PHI FOR MARKETING PURPOSES

A. General rule. CASE may use or disclose an individual's PHI for marketing purposes only if CASE has obtained a valid, written authorization from the individual.

B. Exceptions to the general rule. CASE may use and disclose PHI without an authorization to make a marketing communication to an individual, if the communication:

1. occurs in a face-to-face encounter with the individual (not telephone consultations); or

2. concerns promotional gifts of nominal value provided by CASE (*e.g.*, calendars, pens, and other general, inexpensive promotional merchandise).

CASE personnel shall not use or disclose PHI for marketing purposes, except as set forth above in this Section II.B, without the written approval of CASE's privacy officer, who will be responsible for confirming that an appropriate individual authorization has been obtained.

D. Format requirements. A marketing authorization must conform in all respects with the requirements set forth in CASE's Authorization Policy. In addition, if the marketing involves direct or indirect remuneration to CASE from a third party, the authorization must state that such remuneration is involved.

MARKETING
FREQUENTLY ASKED QUESTIONS

A. *Is a communication with a patient that is intended exclusively to further the treatment of the patient considered marketing for purposes of the Privacy Rules?*

No. The definition of "marketing" in the Privacy Rules excludes a communication made for treatment of the individual. For example, a dentist may refer an individual to an oral surgeon for a follow-up or provide free samples of a prescription drug to a patient.

B. *Is an authorization required if a marketing communication is made face-to-face with a patient?*

No. The Privacy Rules except from the marketing authorization requirements communications that are made face-to-face or communications that are in the form of a promotional gift of nominal value provided by CASE. Thus, dentists may give patients free toothbrushes, floss and toothpaste.

POLICY #11: REQUESTS FOR ADDITIONAL PRIVACY POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to evaluate all individual requests for additional restrictions on the use and disclosure of PHI on a case-by-case basis in compliance with the procedures set forth below. At its option, CASE will accommodate an individual's reasonable request to receive communications from CASE by alternative means or at alternative locations, if the individual specifies the alternative means or location.

PURPOSE: The purpose of this policy is to explain: (1) when an individual has a right to request that CASE restrict the use or disclosure of his or her PHI; (2) when an individual has a right to request that CASE send communications of PHI by alternative means or to alternative locations; and (3) the procedures that CASE must follow to handle these requests.

I. RIGHT TO REQUEST RESTRICTION OF USES AND DISCLOSURES

A. Individual's right to request restrictions. An individual may request additional restrictions on CASE's use and disclosure of his or her PHI when the PHI is used or disclosed for the following purposes:

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

2. to persons assisting in the individual's care; or

3. to friends, caregivers, or family members for notification purposes.

An individual does not have a right to request restrictions on other uses or disclosures of PHI.

B. Agreeing to a restriction. CASE is not required to agree to a request for a restriction.

1. If CASE agrees to a restriction it must document the agreement, and may not use or disclose PHI in violation of the restriction except in the following circumstances:

a. emergency treatment situations;

b. disclosures that CASE is permitted to make without an individual's permission, such as those required by law; and

c. disclosures made to the federal government during an investigation of CASE's compliance with the HIPAA Privacy and Security Rules.

2. If the restricted PHI is disclosed in an emergency treatment situation, CASE must ask the health care provider to whom it is disclosed not to use or disclose the PHI for other purposes.

3. All requests for additional restrictions must be referred to CASE's Privacy and/or Security Officer, who will determine whether the requests will be granted. The privacy officer will maintain documentation of all requests, decisions regarding such requests, and termination of restrictions. CASE's Privacy and/or Security Officer will determine how the restriction will be disseminated to CASE's locations and other personnel, based upon the type of restriction.

C. Terminating a restriction. CASE may terminate its agreement to a restriction if:

1. the individual agrees to or requests the termination in writing;

2. the individual orally agrees to the termination and CASE documents the oral agreement by a notation in the individual's record or similar documentation; or

3. CASE informs the individual that it is terminating its agreement to the restriction. In this situation, the termination is effective only for the PHI created or received after CASE has informed the individual of the termination.

II. RIGHT TO REQUEST ALTERNATIVE COMMUNICATIONS

A. Individual's right to request alternative communications. Unlike requests for additional restrictions on uses and disclosures, which CASE is free to grant or deny, CASE must accommodate reasonable requests by individuals to receive communications of PHI from CASE by alternative means or at alternative locations. For example, an individual may request that CASE communicate with him or her at the individual's place of employment, by mail to a designated address, or by telephone to a certain phone number.

B. Writing requirement. CASE requires the individual to make a request for alternative communication in writing. All requests must be directed to CASE's Privacy Officer. CASE's Privacy Officer will maintain documentation of the request and handle the dissemination of the request to CASE personnel who need to be aware of the request. Privacy Officer will notify Security Officer of requests as necessary.

C. Refusing requests. CASE may refuse to accommodate a request if the individual has not provided information as to how payment, if applicable, will be handled, or has not specified an alternative address or other method of contact. CASE's Privacy Officer will make all determinations as to whether to accommodate a request.

D. Reasons for requests. CASE may not require the individual to give a reason for the request as a condition of accommodating the request.

III. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

CASE's Privacy Officer will document any restriction that CASE accepts, and will retain the documentation until six years after the date the restriction was last in effect.

REQUESTS FOR ADDITIONAL PRIVACY: FREQUENTLY ASKED QUESTIONS

A. *Why types of requests <u>may</u> be considered reasonable requests for alternative communications?*

- An individual lives with an abusive man and is concerned that his knowledge of her health care treatment may lead to additional abuse, so she requests that any mail from CASE be sent to a friend's home or that telephone calls be made to her at work.

- An individual does not want his family to know that he is taking a prescription medication, so he requests that CASE send all written communications to a designated post office box instead of his home address, or he requests that CASE mail information using closed envelopes instead of post cards.

- An individual who is not a minor does not want her parents to know that she is receiving medical treatment, so she requests that CASE contact her by e-mail.

B. *Are restrictions effective to prevent uses and disclosures for which the individual's permission is not required?*

No. If the use or disclosure does not require the individual's permission (***e.g.***, disclosures required by law, for law enforcement purposes, legal or administrative proceedings, and other disclosures for "national priority purposes"), the restriction is not binding on CASE. CASE can agree to this type of restriction, but the restriction is not enforceable. For example, if CASE makes a disclosure relating to serious and imminent threats (a situation where the individual's permission to make the disclosure is not required), the disclosure will not be in violation of the regulation even if the disclosure is contrary to an additional restriction previously accepted by CASE.

C. *If CASE terminates a restriction without the individual's permission, does this apply to all of the individual's PHI that CASE holds?*

No. If CASE wants to terminate the restriction without the individual's permission, it may only terminate the restriction with respect to PHI it creates or receives after it informs the individual of the termination. The restriction continues to apply to PHI created or received prior to informing the individual of the termination. Thus, any PHI that has been collected before the termination may not be used or disclosed in a way that is inconsistent with the restriction, but any PHI that is collected after informing the individual of the termination of the restriction may be used or disclosed as otherwise permitted.

D. *If CASE agrees to a restriction, is CASE bound by that restriction?*

Yes. When the individual requests a restriction and CASE agrees to the individual's request, CASE is ordinarily bound by that restriction, with a few specified exceptions.

E. *If CASE agrees to a restriction, are other parties bound by that restriction?*

Yes. If CASE agrees to the restriction, CASE's business associates must also be bound by the restriction. However, any downstream entities to whom PHI is subsequently disclosed would not be bound by the restriction. Although the rules encourage CASE to disclose the existence of a restriction when appropriate to do so, CASE is not required to disclose this information.

[OPTIONAL – INDIVIDUAL IS NOT REQUIRED TO USE THIS FORM]

REQUEST FOR ADDITIONAL PRIVACY AND SECURITY
SAMPLE FORM

Individual Name:_____

Date of Birth:_____ SSN _____ - _____ - _____

Individual Address: _____ _____ _____
Street Apartment number

_____ _____
City, State Zip Telephone number

Type of protected health information affected by this request: (Please check all that apply)

☐ Home phone #
☐ Home address
☐ Occupation
☐ Name of employer
☐ Visit notes
☐ Health care records
☐ Prescription information

☐ Individual history
☐ Office address
☐ Office phone #
☐ Spouse's name
☐ Spouse's office phone #
☐ Other _____

I. REQUEST FOR LIMITATIONS AND RESTRICTIONS ON USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

How would you like the use and/or disclosure of your protected health information restricted?

_____

_____

_____ _____

Signature of Individual or Legal Guardian Date

INDIVIDUAL PLEASE NOTE: CASE WESTERN RESERVE UNIVERSITY IS NOT REQUIRED TO AGREE TO YOUR REQUEST. YOUR REQUEST WILL BE FORWARDED TO CASE WESTERN RESERVE UNIVERSITY'S PRIVACY OFFICER FOR REVIEW. PLEASE SEE CASE WESTERN RESERVE UNIVERSITY'S NOTICE OF PRIVACY PRACTICES FOR MORE INFORMATION REGARDING SUCH REQUESTS.

II. CONFIDENTIAL COMMUNICATIONS

Do you wish to receive communications of the above indicated protected health information at an address other than that specified above or in some alternative manner? ☐ **YES** ☐ **NO**

If yes, please specify either a different address or means of communication as to the protected health information indicated above:

_____

_____

_____

_____

_____

_____

_____

_____

CASE WESTERN RESERVE UNIVERSITY WILL ACCOMMODATE THIS REQUEST IF REASONABLE. YOUR REQUEST WILL BE FORWARDED TO CASE WESTERN RESERVE UNIVERSITY'S PRIVACY OFFICER FOR REVIEW. PLEASE SEE CASE WESTERN RESERVE UNIVERSITY'S NOTICE OF PRIVACY PRACTICES FOR MORE INFORMATION REGARDING SUCH REQUESTS.

POLICY #12: RIGHT TO ACCESS RECORDS POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will process, in accordance with the procedures outlined below, a request to access, inspect, and/or obtain a copy of certain PHI maintained by CASE, if the request is made by an individual or his or her authorized representative.

PURPOSE: The purpose of this policy is (1) to establish a process for individuals to access, inspect and obtain a copy of certain PHI maintained by CASE; and (2) provide guidance to CASE employees in complying with such requests.

I. RIGHT OF ACCESS TO PHI

A. Basic right to access. In general, an individual has a right to inspect and obtain a copy of his or her PHI held by CASE, for as long as the PHI is maintained by CASE. Exceptions to the right of access are set forth below.

B. Written Requests. CASE may require the individual to make requests for access in writing, provided that it informs individuals of this requirement in advance and applies the policy uniformly. CASE will inform individuals of this requirement in CASE's Notice of Privacy Practices.

C. Denials without an opportunity for review. CASE may deny the individual's request for access to PHI without providing the individual an opportunity for review of the decision in any of the following circumstances:

1. the PHI was compiled by CASE in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

2. the PHI was obtained by CASE in the course of research that includes treatment of the research participants, while such research is in progress, and the individual previously agreed to this temporary suspension of access; or

3. the PHI 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.

D. Denials with an opportunity for review. In the following circumstances, CASE may deny an individual access to his or her PHI, so long as the individual is given

a right to have the denial reviewed: (1) 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 individual or another person, (2) the PHI makes reference to another person (other than a health care provider) 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 of such other person; or (3) the request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

E. Right to review of denial. If CASE denies the individual access to his or her PHI for a reason described in Section I.D. above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by CASE's privacy officer to act as a reviewing official and who did not participate in the original decision to deny access. CASE must provide or deny access in accordance with the determination of that health care professional.

F. Verification. Prior to disclosing PHI to a person unknown to CASE, CASE must verify the identity of the person requesting the PHI and the authority of the person to have access to the PHI requested. In addition, CASE must obtain any documentation, statements, or representations, whether oral or written, from the requestor when such information is a condition of the disclosure.

II. RESPONDING TO A REQUEST FOR ACCESS

A. Acting on the request. If the PHI to which an individual requests access is maintained or is accessible on-site, CASE must act on a request for access within 30 days of the date CASE received the request. If the PHI is not maintained or accessible on-site, CASE must act on a request for access within 60 days of receiving the request. All requests for access to PHI shall be directed to CASE's privacy officer, who will coordinate the handling of the request.

1. If CASE grants an individual's request for access, it must inform the individual that the request has been granted and provide access to the PHI.

2. If CASE denies the individual's request for access, it must provide the individual with a written denial. (See Section II.C below.)

3. If CASE cannot act on a request within the applicable deadline, it may extend the deadline by no more than 30 days by providing the individual

with a written statement of the reasons for the delay and the date by which CASE will complete its action on the request. CASE must provide the written statement within the original time period and may only extend the time period once.

B. Provision of access. If CASE grants a request for access, it must comply with the following requirements.

1. CASE must notify the individual and provide the access as requested, including allowing the individual to inspect or obtain a copy, or both, of the PHI.

2. CASE must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or if not, in a readable hard copy form or other form that is agreed upon by CASE and the individual. For example, if CASE maintains PHI electronically and the individual requests an electronic copy, CASE must accommodate this request if the PHI is readily producible in this format.

3. If acceptable to the individual and CASE, CASE may provide the individual with a summary or explanation of the PHI instead of providing access to the actual PHI.

4. CASE will provide access in a timely manner, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request. CASE may discuss the scope, format, and other aspects of the request for access with the individual as necessary to provide timely access.

5. If the individual requests a copy of the PHI or agrees to a summary or explanation, CASE may charge a reasonable, cost-based fee, provided that the fee includes only the cost of copying, postage, and preparing an explanation or summary of the PHI (if a summary is requested by the individual).

C. Denial of access. If CASE's privacy officer determines to deny access to PHI, CASE will take the following actions, and maintain complete documentation of such actions:

1. Give the individual access to any other PHI requested, to the extent possible, after excluding PHI for which CASE has grounds to deny access.

2. Provide a timely, written denial to the individual. The denial must be in plain language and must include (i) the basis for the denial; (ii) if applicable, a statement of the individual's right to review of the decision, including a description of how the individual can exercise these review rights; and (iii) a description of how the individual may complain to CASE or the Secretary of Health and Human Services, including the name or title and telephone number of the CASE contact person or designated office.

3. Inform the individual where to direct the request for access, if CASE does not maintain the PHI that is the subject of the individual's request for access, and CASE knows where the requested information is maintained.

4. If the individual has requested a review of a denial, CASE's privacy officer will designate a licensed health care professional who was not directly involved in the denial to review the decision to deny access. The privacy officer will refer the request for review to the reviewing official. The reviewing official must determine, within a reasonable period of time, whether or not to deny access. CASE's privacy officer will provide written notice to the individual of the reviewing official's decision and carry out the decision.

III. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

It is CASE's policy to document the records that are subject to access by individuals and the titles of the persons or offices responsible for receiving and processing requests for access. CASE will retain this documentation from the date of its creation until six years after the date when it was last in effect.

RIGHT TO ACCESS RECORDS: FREQUENTLY ASKED QUESTIONS

A. *Is CASE required to deny the individual access in the situations described in Sections I C and D of its policy on rights of access to PHI?*

Even in situations where CASE is permitted to deny the individual's request, CASE may choose to provide the requested PHI to the individual. For each request by an individual, CASE may provide all of the information requested or evaluate the requested information, consider the circumstances surrounding the individual's request, and make a determination as to whether the request should be granted or denied, in whole or in part, in accordance with one of the permitted bases for denial.

B. *If the individual requests a summary or agrees to a summary at CASE's suggestion, does he or she still have the right to access the actual PHI?*

Yes. Individuals have the right to obtain access both to summaries and the underlying information. An individual retains the right of access to the underlying information even if he or she requests access to, or production of, a summary.

C. *May CASE charge any fees related to individuals' requests for access?*

CASE may not charge any fees solely for retrieving or handling the information or for processing the individual's request. However, CASE may charge a fee for copying, including supplies (paper or computer disk), labor and postage. CASE may also charge a fee for preparing a summary or explanation of the information that an individual may request or accept.

D. *Is CASE required to provide individuals access to information that was obtained or created prior to the compliance date of the rules?*

Yes. Information created prior to the compliance date of the rules must be accessible by the individual. However, since CASE is not required to maintain PHI in accordance with the rules until the compliance date of April 14, 2003, CASE is not required to recreate any PHI that is destroyed prior to that date. Thus, if an individual requests access to PHI created prior to the compliance date, CASE must provide access if it still maintains the information. But if CASE no longer maintains the information, it is not required to recreate it to comply with the individual's request.

REQUEST TO INSPECT AND COPY PROTECTED HEALTH INFORMATION
SAMPLE FORM

Name: _____ Date of Birth: _____

Address: _____ SS# _____
Street

_____
Apartment #

_____
City, State Zip

I request access to:

____ inspect

____ copy

____ inspect and copy

the following protected health information:
_____.

I understand and agree that I am financially responsible for the following fees associated with my request: copying charges, including the cost of supplies and labor, and postage related to the production of my information. I understand that the charge for this service is $_____ per page, with a minimum charge of $_____.

_____ _____
Signature of Individual, Personal Representative or Legal Guardian — Date

_____
Print Name of Individual, Personal Representative or Legal Guardian

DENIAL LETTER

SAMPLE FORM

Date

Name
Address
City, State, Zip

Dear _____:

In accordance with the Final Rule for the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") and HIPAA Administrative Simplification – Security; Final Rule ("Security Rule") issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), CASE is unable to honor your request to inspect and obtain a copy of your protected health information ("PHI") for the following reason(s):

[ ] CASE does not possess the information requested. [Insert location of PHI, if known]

[ ] You have requested psychotherapy notes, as defined in the Privacy Rule, and CASE is not required to allow you to inspect and obtain a copy of your psychotherapy notes.

[ ] The Privacy and Security Rules does not require CASE to permit you to inspect and obtain a copy of the requested information because it has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding.

[ ] The Privacy and Security Rules do not require CASE to permit you to inspect and obtain a copy of the requested information because it is subject to or exempted by the Clinical Laboratory Improvements Amendments of 1988.

[ ] The Privacy and Security Rules do not require CASE to permit you to inspect and obtain a copy of the requested information because the information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

[ ] The Privacy and Security Rules do not require CASE to permit you to inspect and obtain a copy of the requested information because the information was/is being created or obtained in the course of on-going research that includes treatment and you agreed to the denial of access when you consented to participate in the research. Your right of access will be reinstated upon the completion of the research.

[ ] The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, and this denial meets the requirements of that law. (The Privacy Act of 1974 protects personal information about individuals held by the federal government.)

[ ] A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.

[ ] The requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

[ ] You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to you.

If access to requested information has been denied for any of the last three reasons listed above, you have the right to have the denial reviewed by another licensed healthcare professional who did not participate in this denial. If you choose to have this denial reviewed, please submit a written request to CASE's Privacy Officer at CASE, 10900 Euclid Avenue, Cleveland, Ohio 44106.

CASE's Privacy Officer will respond with a written decision within a reasonable period of time whether or not to ultimately grant or deny access to your PHI as originally requested. You may file a complaint regarding this denial with the privacy officer of CASE or with the Secretary of the U.S. Department of Health and Human Services. Complaints to the Secretary must be in

writing, name CASE, describe the acts/omissions believed to violate the Privacy and Security Rules, and be filed within 180 days of the alleged violation.

Very truly yours,

_____
Privacy Officer of CASE

POLICY #13: REQUESTING AMENDMENTS POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to respond to an individual's request for an amendment to his or her PHI held by CASE (and/or CASE's business associates) in a manner which complies with the Privacy and Security Rules.

PURPOSE: The purpose of this policy is to establish a process for responding to individual requests to amend PHI maintained by CASE.

I. RIGHT TO AMENDMENT OF PROTECTED HEALTH INFORMATION

A. Right to request an amendment. An individual has the right to request that CASE amend PHI about the individual that is contained in CASE's records for as long as the PHI is maintained by CASE. All such requests shall be forwarded immediately to CASE's privacy officer.

B. Accepting an individual's request for amendment. If CASE has no grounds to deny the individual's request for amendment (as determined by CASE's privacy officer. s*ee* Section I.C. below), CASE will do all of the following:

1. Make the appropriate amendment to the individual's PHI or record. CASE should, at a minimum, identify the records that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

2. Inform the individual on a timely basis that the amendment is accepted and obtain the individual's identification of and agreement to have CASE notify the relevant persons with whom the amendment needs to be shared.

3. Make reasonable efforts to inform and provide the amendment within reasonable time to:

   a. persons identified by the individual as having received PHI and needing the amendment; and

   b. persons, including business associates, that CASE knows have the unamended information and may have relied, or might rely in the future, on the information to the detriment of the individual.

C. Denying an individual's request for amendment. Under certain circumstances, CASE may deny the individual's request for amendment to his or her PHI held by CASE.

1. Permissible reasons for denial. CASE may deny a request for an amendment only for any of the following reasons:

a. the PHI was not created by CASE, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.

b. the PHI is not part of the individual's designated record set.

c. the PHI would not be available for inspection under CASE's policy regarding the individual's right to access to PHI.

d. the PHI is accurate and complete.

2. Denial procedures. If CASE's privacy officer determines that CASE should deny the requested amendment, in whole or in part, CASE will take the following steps.

a. CASE's privacy officer will provide the individual with a valid, written denial that explains:

(i) the basis for the denial;

(ii) how the individual may file a written statement disagreeing with the denial;

(iii)the individual's options with respect to future disclosures of the disputed information; and

(iv)how the individual may make a complaint to CASE or to the Department of Health and Human Services about the denial.

b. CASE will permit the individual to submit to CASE a written statement disagreeing with the denial and the basis for the disagreement.

(i) CASE's privacy officer may prepare a written rebuttal to the individual's statement of disagreement.

(ii) If CASE prepares a rebuttal, CASE must provide a copy to the individual.

c. CASE must identify, as appropriate, the information in the individual's record that is the subject of the disputed amendment and append or otherwise link to this information the individual's request for an amendment, CASE's denial of the request, the individual's statement of disagreement, and CASE's rebuttal to the individual's statement, if any.

d. CASE will adhere to the following guidelines if it makes future disclosures of the individual's disputed PHI:

(i) If the individual has submitted a statement of disagreement, CASE will include either the statement, as an appendix to the PHI, or an accurate summary of such statement, with any subsequent disclosure of the PHI to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, CASE will include the appended information with any subsequent disclosure only if the individual has requested that CASE do so.

D. Receiving a notice of amendment from other health care providers or health plans. Health care providers or health plans may contact CASE to advise CASE that they have made amendments to an individual's PHI. When CASE is informed by a health care provider or health plan of an amendment to an individual's PHI, CASE must make necessary amendments to the PHI in its records.

E. Time period for acting on requests. CASE's privacy officer should act on an individual's request for an amendment within 60 days of receipt of the request. If CASE is unable to act on the amendment request within 60 days, CASE may extend the time period once for 30 days, if within the original 60 day time limit CASE provides the individual with a written statement of the reasons for the delay and the date by which CASE will complete its action on the request. The Privacy Rule permit CASE only one 30 day extension.

II. DOCUMENTATION AND RECORD RETENTION REQUIREMENTS

CASE's privacy officer will be responsible for receiving and processing requests for amendments by individuals. CASE's privacy officer will also document requests for

amendments and the resolution of those requests. CASE will retain this documentation from the date of its creation until six years after the date when it was last in effect.

REQUESTING AMENDMENTS: FREQUENTLY ASKED QUESTIONS

A. *If an individual's request for an amendment of PHI does not meet the requirements established by CASE, is CASE required to grant the request?*

No. For example, if CASE requires that a request for amendment be in writing and state a reason for the amendment and CASE has informed individuals of these requirements, then CASE is not required to act on an individual's request that does not meet these requirements. However, CASE's privacy officer should inform the individual why no action is being taken and document why CASE did not take action. The individual has the right to resubmit his or her request in compliance with CASE's policy.

B. *Is CASE required to <u>delete</u> information from the individual's records?*

No, CASE is never required to delete information from an individual's records. The Privacy and Security Rules do not attempt to alter record retention laws or CASE's current practices. CASE is only required to append information as requested to ensure that the individual's records are complete. If CASE agrees that the information is erroneous and wants to delete it, and such a deletion is consistent with other law and CASE's practices, then CASE may do so. However, CASE's privacy officer may wish to seek legal review before information is deleted.

C. *Does the request for amendment requirement apply only to information held by CASE?*

No, the requirement for amendment applies to records maintained by or for CASE. Relevant information in the possession of CASE's business associates will also be covered by this requirement, and CASE's business associates will be required to make any necessary amendments.

REQUEST FOR CORRECTION/AMENDMENT OF PROTECTED HEALTH INFORMATION SAMPLE FORM

Name: _____

Date of Birth: _____

Patient Address: _____
Street

_____
Apartment #

_____
City, State Zip

Type of Entry to be Amended: _____

- ☐ *Visit note*
- ☐ *Nurse note*
- ☐ *Prescription*
- ☐ *Patient history*
- ☐ *Other* _____ *(description)*

Please explain how the entry is inaccurate or incomplete.

_____

_____

Please specify what the entry should say to be more accurate or complete.

_____

_____

_____ _____
Signature of Individual Representative or Legal Guardian — Date

Amendment has been:

- ☐ Accepted
- ☐ Denied
- ☐ Denied in part, Accepted in part

If denied (in whole or in part)*, check reason for denial:

☐ PHI was not created by CASE
☐ PHI is not available to the individual for inspection in accordance with the law.
☐ PHI is not a part of individual's designated record set.
☐ PHI is accurate and complete.

Comments from CASE workforce member who created or received the PHI:

_____

_____

_____

_____

Was a statement of disagreement filed as to the denial of amendment? ☐ Yes ☐ No

If yes, was a rebuttal filed by CASE and sent to the individual requesting the amendment? ☐ Yes ☐ No

CASE must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, CASE's denial of the request, the individual's statement of disagreement, if any, and CASE's rebuttal, if any, to the designated record set.

Name of CASE Workforce Member Completing Form: _____

Title: _____

_____ _____
Signature of CASE Workforce Member Date

*If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to CASE's Privacy Officer, 10900 Euclid Avenue, Cleveland, Ohio 44106. If you do not provide us with a statement of disagreement, you may request that we provide to you copies of your original request for amendment, our denial, and any disclosures of the protected health information that is the subject of the requested amendment. Additionally, you may file a complaint with CASE's privacy officer or the Secretary of the U.S. Department of Health & Human Services.

*CASE MUST INFORM AN INDIVIDUAL THAT A REQUEST FOR AMENDMENT OF PHI MUST BE MADE IN WRITING TO BE CONSIDERED BY CASE AND THAT THE INDIVIDUAL IS REQUIRED TO PROVIDE A REASON TO SUPPORT THE REQUESTED CHANGE.

POLICY #14: ACCOUNTING OF DISCLOSURES POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to provide individuals, upon request, a timely accounting of certain disclosures of their PHI as required by law.

PURPOSE: The purpose of this policy is to establish a process by which CASE will respond to individuals' requests for an accounting of disclosures of their PHI.

I. RIGHT TO AN ACCOUNTING OF DISCLOSURES

A. Basic right to an accounting. An individual has a right to receive an accounting of several types of disclosures of his or her PHI made by CASE and its business associates for the six-year period prior to the date of the request. However, as listed below, several types of disclosures of PHI are exempt from this accounting requirement. All requests for an accounting of disclosures shall be forwarded to CASE's privacy officer or his or her designated representative.

B. Exceptions to the accounting requirement. CASE is not required to provide an accounting of disclosures that were made by CASE:

1. prior to April 14, 2003, the compliance date of the Privacy Rules;

2. for purposes of treatment of the individual, such as disclosures made to a health care provider involved in the individual's treatment;

3. for payment activities, including billing, claims management, eligibility determinations, coordination of benefits, determination of cost-sharing amounts, and adjudication of health benefit claims;

4. for health care operations, including management and administrative activities, quality assessment and improvement, training programs, auditing, compliance, business planning and development, and certain due diligence activities conducted in connection with the sale or transfer of assets;

5. to the individual requesting the accounting;

6. to individuals involved in the individual's care where the individual verbally agreed to the disclosure;

7. to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and certain other national security activities;

8. to a correctional institution or law enforcement official, upon a request by, and during such time as, the correctional institution or law enforcement official had lawful custody of the individual;

9. incidental to a use or disclosure that is otherwise permitted by the Privacy Rules;

10. pursuant to a valid individual authorization; or

11. as part of a limited data set that was disclosed pursuant to a data use agreement for purposes of research, public health or health care operations.

C. Suspension of accounting. A health oversight agency or law enforcement official may request that CASE temporarily suspend an individual's right to receive an accounting of disclosures made to the health oversight agency or law enforcement official. Upon appropriate request, CASE must temporarily suspend an individual's right to receive an accounting of these disclosures for the time specified by such agency or official, if such agency or official provides CASE with a written statement that (i) an accounting to the individual would be reasonably likely to impede the agency's activities; and (ii) specifies the time period for which a suspension is required. But if that agency or official statement is made orally to CASE, CASE must:

1. document the statement, including the identity of the agency or official making the statement;

2. temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

3. limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement from the agency or official is submitted during that time.

CASE personnel shall refer instructions for any such suspension to CASE's privacy officer.

D. Time period for action. All requests for an accounting of disclosures of PHI shall be referred to CASE's privacy officer. CASE will act on an individual's request for an accounting no later than 60 days after receipt of such a request, in one of the following ways:

1. CASE will provide the individual with the accounting requested; or

2. if CASE is unable to provide the accounting within 60 days of receipt of the request, CASE may extend the time to provide the accounting once, by no more than 30 days, if CASE, within 60 days of receipt of the request, provides the individual with a written statement of the reasons for the delay and the date by which CASE will provide the accounting.

E. Fees for providing an accounting. CASE must provide the first accounting to an individual in any 12-month period without charge. CASE may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the same 12-month period. If a fee will be charged, CASE will inform the individual in advance of the fee and provide the individual an opportunity to withdraw or modify the request for an accounting to avoid or reduce the fee.

II. REQUIRED CONTENTS OF AN ACCOUNTING OF DISCLOSURES

A. Core elements. An accounting of disclosures must be in writing and must contain the following elements for each disclosure:

1. the date of the disclosure;

2. the name of the entity or person who received the PHI;

3. the address of the entity or person who received the PHI, if known;

4. a brief description of the PHI disclosed; and

5. either (a) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or (b) a copy of a written request for a disclosure made pursuant to CASE's policy for disclosures to government entities.

B. Multiple disclosures. For certain disclosures that occur on a regular basis, other than disclosures listed in section I.B. above, CASE may provide a summary accounting addressing the series of disclosures rather than a detailed accounting of each disclosure.

1. When a summary accounting is permissible. A summary accounting for multiple disclosures is permissible if, during the period covered by the accounting, CASE has made multiple disclosures of PHI:

   a. for a single purpose to HHS so it may investigate or determine CASE's compliance with the rules; or

   b. to the same person or entity for a single national priority purpose (as set forth in CASE's policy regarding priority disclosures).

2. Required information for a summary accounting. Rather than include all of the core elements listed in section II.A. above for every disclosure in a series of disclosures, CASE may limit the accounting to the following information:

   a. the core elements (set forth in Section II.A. above) for the first disclosure during the accounting period;

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

   c. the date of the most recent disclosure in the series during the accounting period.

3. Research disclosures. In cases where PHI has been disclosed, pursuant to a waiver of authorization, the Privacy Rules permit CASE to use an abbreviated method of accounting for such disclosures. CASE may choose to follow this method of accounting for disclosures of PHI for research purposes. These procedures apply where disclosures have been made involving fifty (50) or more individuals and the PHI of the individual requesting disclosure may have been included in such a disclosure. The abbreviated accounting for disclosure must include:

   a. the name of the protocol or other research activity in connection with which the disclosure was made;

   b. a description, in plain language, of the research protocol or other research activity in connection with which the disclosure was made, including the purpose of the research and the criteria for selecting particular records;

   c. a brief description of the type of PHI that was disclosed;

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

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

f. a statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If CASE provides an accounting for research disclosures in accordance with the above procedures, and if it is reasonably likely that the PHI of the individual requesting an accounting was disclosed for the described research protocol or activity, CASE will, at the request of the individual, assist the individual in contacting the entity that sponsored the research and/or the researcher.

III. RECORD RETENTION REQUIREMENTS

A. Required documentation. CASE's privacy officer must create and maintain the following documentation, which can be kept in an electronic format:

1. the core elements of each disclosure as set forth in Section II.A. above;

2. the written accounting that is provided to the individual; and

3. the titles of the persons or offices within CASE responsible for receiving and processing an individual's request for an accounting.

B. Retention period. CASE must retain the required documentation for a period of six years from the date of its creation or the date when it was last in effect, whichever is later.

ACCOUNTING OF DISCLOSURES: FREQUENTLY ASKED QUESTIONS

A. *Do individuals have the right to receive an accounting of disclosures made by CASE to its business associates?*

Yes. Individuals have the right to request and receive an accounting of disclosures made by or to a business associate of CASE, to the same extent they have a right to an accounting of disclosures made by CASE.

B. *Can an individual request an accounting of disclosures for a period of less than six years?*

Yes. An individual may request, and CASE may then provide, an accounting of disclosures for a period of time less than six years from the date of the request. For example, an individual may request an accounting of disclosures that occurred during the two years prior to the request.

C. *Does CASE have to make copies of requests for disclosures available with the accounting?*

No. CASE is, however, required to give a brief statement of the purpose of the disclosure with the accounting. The statement must reasonably inform the individual of the basis for the disclosure. In lieu of this statement of purpose, CASE may include a copy of the relevant written request for disclosure.

REQUEST FOR AN ACCOUNTING OF CERTAIN DISCLOSURES OF
Protected Health Information for Non-TPO Purposes
SAMPLE FORM

As an individual, you have the right to receive an accounting of certain non-routine disclosures of your identifiable health information made by Case Western Reserve University for purposes other than treatment, payment, or healthcare operations. Your request must state a time period that may not be longer than six (6) years and may not include dates before April 14, 2003. The first list you request within a 12-month period will be provided free of charge. For additional lists during the same 12-month period, you may be charged for the costs of providing the list; however the, CASE will notify you of the cost involved and you may choose to withdraw or modify your request.

To request an accounting of disclosures made by Case Western Reserve University for purposes other than treatment, payment, or health care operations, you must submit your request in writing to Case Western Reserve University's privacy officer, 10900 Euclid Avenue, Cleveland, Ohio 44106.

I request as accounting of all disclosures of protected health information about me made by Case Western Reserve University ف from _____ _____, _____ through _____ _____, _____, or ف during the six (6) years prior to this request. I understand that CASE is not obligated to account for any disclosures of PHI prior to April 14, 2003. I also understand that CASE is obligated to account only for such disclosures as required under the Privacy Rules and that this means that certain disclosures of my PHI might not be included in an accounting of disclosures provided by CASE.

Name:_____ Date of Birth:_____

Address: _____
Street

_____
Apartment #

_____
City, State Zip

_____ _____
Signature of Patient or Legal Guardian Date

LOG TO TRACK DISCLOSURES OF PHI

PATIENT NAME_____

For each individual, Case Western Reserve University is required to keep a log of all disclosures of PHI for non-TPO reasons for which Case Western Reserve University did not receive a signed authorization from the individual. For each disclosure, fill in the date it occurred along with a description of the type of disclosure. In addition, provide a description of the PHI disclosed along with the names and titles to whom it was disclosed.

DATE	DESCRIPTION OF DISCLOSURE	DESCRIPTION OF PHI	Who Requested	To Whom PHI Was Disclosed	Approve/Deny (+ initials)

Note: Case Western Reserve University must retain related documentation and tracking log for each individual for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

POLICY #15: PERSONNEL DESIGNATIONS
POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") that at all times an individual will be designated as the CASE Privacy Officer (the CASE contact person for purposes of the Privacy Rules.)

PURPOSE: The purpose of this policy is to: (1) identify those individuals, by name or job title, who shall serve as CASE's privacy officer and contact person; (2) specify the responsibilities of the privacy officer and contact person; (3) identify those individuals, by name or job title, who shall serve as CASE's information security officer and contact person; and (4) specify the responsibilities of the information security officer and contact person.

I. DESIGNATION OF THE PRIVACY OFFICER

A. In General

1. CASE shall designate a privacy officer and a contact person. One person may serve as both the privacy officer and the contact person.

2. Whenever possible, CASE shall make such designations by means of job title.

B. Designation of Privacy Officer and Contact Person. CASE's privacy officer and contact person shall be the [*insert title*], who reports to [*insert reporting path and or organization chart*].

II. DUTIES OF THE PRIVACY OFFICER

A. Privacy Officer. CASE's privacy officer shall be responsible for development and implementation of CASE's Privacy Policies and Procedures. The privacy officer shall also be available to CASE's designated health care components and employees to assist with application, interpretation and implementation of and compliance with CASE's Privacy Policies and Procedures and the Privacy Rules. CASE's designated

health care components and employees should direct inquiries concerning CASE's Privacy Policies and Procedures and/or the Privacy Rules to the CASE privacy officer. A list of Privacy Officer duties and responsibilities is attached and incorporated in these Policies and Procedures.

B. Contact Person. CASE's contact person shall be responsible for receiving complaints from individuals concerning CASE's privacy practices and shall be able to provide information about matters addressed in CASE's Notice of Privacy Practices.

III. DESIGNATION OF THE INFORMATION SECURITY OFFICER

A. In General

1. CASE shall designate an information security officer and a contact person. One person may serve as both the Privacy Officer and the contact person.

2. Whenever possible, CASE shall make such designations by means of job title.

B. Designation of Information Security Officer and Contact Person. CASE's information security officer and contact person shall be Rey LeClerc, who is CASE's Chief Information Security Officer.

IV. DUTIES OF THE INFORMATION SECURITY OFFICER

A. Information Security Officer. CASE's information security officer shall be responsible for development and implementation of CASE's Policies and Procedures concerning the Security Rules. The privacy officer shall also be available to CASE's designated health care components and employees to assist with application, interpretation and implementation of and compliance with CASE's Information Security Policies and Procedures and the Security Rules. CASE's designated health care components and employees should direct inquiries concerning CASE's Information Security Policies and Procedures and/or the Privacy Rule to the CASE information security officer. A list of Information Security Officer duties and responsibilities is attached and incorporated in these Policies and Procedures.

B. Contact Person. CASE's contact person shall be responsible for receiving complaints from individuals concerning CASE's security practices.

V. RECORD RETENTION REQUIREMENTS

CASE shall at all times maintain a written or electronic record of its designations of a Privacy and/or Security Officer and a contact person and shall retain such designations for a period of six years after an initial or any subsequent designation.

PERSONNEL DESIGNATIONS: FREQUENTLY ASKED QUESTIONS

A. *Can one person serve as both the privacy officer, information security officer and the contact person?*

Yes. The contact person can be, but is not required to be, the privacy officer and/or the information security officer.

B. *How are the jobs of the privacy officer, information security officer and the contact person different?*

The privacy officer is responsible for promulgating and overseeing compliance with CASE's Privacy Policies and Procedures. The privacy officer also serves as a resource to the CASE designated health care components and CASE employees for matters related to application, implementation and interpretation of and compliance with the Privacy Rule.

The information security officer is responsible for promulgating and overseeing compliance with CASE's Information Security Policies and Procedures. The information security officer also serves as a resource to the CASE designated health care components and CASE employees for matters related to application, implementation and interpretation of and compliance with the Security Rule.

The contact person interacts with persons whose PHI is maintained, used and/or disclosed by CASE. The contact person will handle inquiries from recipients of CASE's notice of privacy and information security practices and receive complaints about CASE's Policies and Procedures and/or compliance with the Privacy and Security Rules.

POLICY #16: TRAINING POLICIES AND PROCEDURES

POLICY: All members of the Case Western Reserve University ("CASE") designated health care components will receive training regarding CASE's privacy and security policies and procedures as necessary and appropriate for each member of the workforce to carry out his or her functions within a designated health care component in compliance with such policies and procedures.

PURPOSE: The purpose of this policy is to ensure that CASE's workforce receives effective and timely education regarding CASE's Policies and Procedures, and that a training curriculum is created and maintained to meet the needs of CASE's employees.

I. PRIVACY AND SECURITY TRAINING

A. Initial training. Current members of the workforce CASE's designated health care components should complete privacy and security training program. Completion of privacy and security training is mandatory and will be considered when workforce members are evaluated during performance reviews. Failure to complete privacy and security training will result in disciplinary action.

B. New members. As part of their initial orientation, new members will receive privacy and security training.

C. Additional training. When material changes are made to one of CASE's Policies or Procedures, all members of the workforce whose functions are affected by the change must receive training on the new Policies and Procedures within a reasonable time after the material change has been made. Additional training sessions may be conducted for specific employees who have responsibilities involving specific compliance issues. In addition, the CASE privacy and security officers may direct specific employees to attend privacy and security training if he or she believes that such training is warranted.

D. Content of training. In privacy and security training, workforce members will review CASE's Policies and Procedures and will discuss any changes in these

Policies and Procedures. The training program will focus on federal laws and regulations governing the privacy and security, confidentiality, and security of PHI, as well as any more stringent state laws.

E. Documentation requirements. CASE's privacy and security officers will document that the required training has been provided.

TRAINING: FREQUENTLY ASKED QUESTIONS

A. *Is CASE required to impose privacy and security training requirements on its business associates?*

No. CASE is not responsible for monitoring whether or not its business associates have established privacy and security training programs for members of their workforce.

B. *Does privacy and security training need to be conducted annually?*

No. However, CASE recognizes that for a privacy and security program to be effective, members of the workforce must receive education and training on a regular basis. CASE will establish appropriate periodic training for workforce members.

HIPAA POLICIES

POLICY #17: PRIVACY AND SECURITY SAFEGUARDS POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to maintain appropriate administrative, technical and physical safeguards to protect the privacy and security of PHI.

PURPOSE: The purpose of this policy is to establish a process by which CASE will maintain appropriate administrative, technical and physical safeguards to protect the privacy and security of PHI.

I. OBLIGATIONS

A. CASE shall reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy and Security Rules and CASE's Policies and Procedures.

B. CASE shall reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure in accordance with the Privacy and Security Rules and CASE's Policies and Procedures.

II. IMPLEMENTATION

A. Each CASE designated health care component will take reasonable steps to protect PHI in any form (paper, electronic, etc.) from unauthorized use, access or disclosure.

B. Each CASE designated health care component will take reasonable precautions to protect paper records that contain PHI from inadvertent disclosure. The following are examples of steps that designated health care components could implement as appropriate to the specific circumstances of the designated health care component:

1. files and documents should be stored in secure areas or in reasonably protective containers such as locked cabinets, locked drawers or locked files;

2. files and documents that are to be discarded should be placed in designated containers for shredding or shredded;

3. files and documents should be promptly removed from printers and fax machines and should not be left on countertops and desktops in insecure area;

4. printers and facsimile machines should be located in areas that minimize exposure of PHI to unauthorized persons;

5. such other steps as may be appropriate in light of the particular circumstances.

C. The members of the workforce of CASE's designated health care components shall take reasonable steps to protect the privacy of all verbal exchanges and conversations that contain PHI. For example, members of the workforce of CASE's designated health care components shall make a reasonable effort to ensure that verbal exchanges that contain PHI occur in private areas.

D. Uses or disclosures of PHI that are incidental to an otherwise permitted use or disclosure of PHI may occur. Such incidental uses or disclosures are not considered a violation of the Privacy and Security Rules or the Policies and Procedures, provided that CASE designated health care components have implemented reasonable safeguards and minimum necessary requirements.

E. Each CASE designated health care component shall make reasonable efforts to ensure that PHI that is visible is protected from unauthorized disclosure. This should include reasonable positioning of computer screens, whiteboards and other devices which display PHI to limit unauthorized viewing.

F. Each CASE designated health care component shall take reasonable precautions to safeguard PHI in electronic form.

1. The designated health care component shall take reasonable measures to protect the confidentiality, integrity and availability of PHI in electronic form.

2. When the designated health care component transmits PHI over public or open networks it will take reasonable precautions, such as data encryption, to ensure the confidentiality and integrity of the transmitted information.

III. ENFORCEMENT

A violation of any provision of this policy may result in disciplinary action, up to and including the termination of employment, suspension of privileges or imposition of academic sanctions consistent with applicable CASE policies and procedures. A

violation of this policy can result in civil and/or criminal penalties. See CASE Policies and Procedures, "Internal Enforcement."

SAFEGUARDS: FREQUENTLY ASKED QUESTIONS

A. *What are reasonable precautions to safeguard PHI in patient files?*

Patient files should be stored in secure areas if at all possible, otherwise in protective containers such as locked cabinets, locked drawers or locked files.

B. *What types of precautions should be taken to safeguard PHI in verbal exchanges and conversations?*

If possible, verbal exchanges regarding PHI should be conducted in reasonably private areas, and voices should be modulated to avoid unintended transmission to others. Minimum necessary requirements should be observed with respect to incidental uses or disclosures.

C. *What types of precautions should be utilized to safeguard PHI on computer screens?*

Computer screens should be positioned to limit unauthorized viewing of PHI. Some computer screens may need to be relocated to more private areas.

POLICY #18: PATIENT COMPLAINTS POLICIES AND PROCEDURES

POLICY: Because confidentiality of PHI and compliance with applicable laws and regulations are of utmost importance to Case Western Reserve University ("CASE"), it is CASE's policy to promptly receive, respond, and resolve complaints regarding allegations of improper use or disclosure of PHI by CASE or its business associates.

PURPOSE: The purpose of this policy is to establish a process for the receipt and resolution of privacy-related complaints.

I. GENERAL RULE

An individual may lodge a formal complaint about CASE's information practices, including, but not limited to, complaints regarding:

1. the privacy and security of PHI;
2. use and disclosure of PHI;
3. individuals' access to, or amendment of, their PHI;
4. practices or actions of CASE's business associates;
5. CASE's marketing practices; or
6. any other complaint relating to CASE's privacy policies and procedures.

II. HANDLING AND DOCUMENTATION OF COMPLAINTS

A. Handling of Complaints. All complaints shall be forwarded to CASE's contact person, who will determine the appropriate responses to the complaints. If the CASE contact person and CASE privacy officer are not the same person, the CASE contact person shall provide copies to or otherwise make the CASE privacy officer aware of all privacy complaints.

B. Documentation. CASE's privacy officer must maintain complete documentation of any privacy complaint and CASE's review and disposition of the matter, including a

record of any changes to Policies and Procedures or the imposition of sanctions against members of its workforce, if any. CASE must retain all documents relating to the complaint and the investigation for a period of at least six years after the date of their creation.

PATIENT COMPLAINTS: FREQUENTLY ASKED QUESTIONS

A. *Can an individual make an anonymous complaint about privacy issues to CASE?*

Yes. If an individual desires to make an anonymous complaint, CASE should treat that complaint in the same manner as other complaints. Individuals may complete anonymous Complaint Forms or provide anonymous complaints over the telephone or by mail. To facilitate this option CASE has implemented an Integrity Hotline, through which complaints or concerns may be submitted on an anonymous basis by phone at (866)483-9367 or online at https://www.caseintegrityhotline.com. The Integrity Hotline allows filers of reports to monitor the university's response, as well as the status and resolution of the complaint, which is reviewed, documented, and resolved, and the resolution documented, in accordance with this policy.

B. *Can a CASE employee make a privacy complaint to CASE?*

Yes. The Privacy Rules allow any person to make a privacy complaint to CASE regarding its privacy practices. Employees and other individuals who are not employers of CASE have the right to file a complaint about CASE's compliance with its Policies and Procedures and the Privacy Rules.

C. *If an individual requests feedback about his or her complaint, is there a time period in which CASE must respond?*

No. Because the rules do not require CASE to provide the individual with feedback about the resolution of his or her complaint, there is no specified time period for providing that information. If CASE's privacy officer chooses to provide feedback to the individual, the privacy officer should decide on a time period for informing individuals about the resolution of their complaints, document this time period in a policy, and consistently apply the policy to all complaints.

PRIVACY COMPLAINT FORM
SAMPLE FORM

CASE WESTERN RESERVE UNIVERSITY values the privacy and confidentiality of the protected health information, and is committed to operating in a manner that promotes the protection of PHI.

If the staff at Case Western Reserve University have fallen short of this goal, we want you to notify us. Please be assured that your complaint will be handled with discretion. Please use the space provided below to describe your complaint. It is our intent to use this feedback to better protect your rights to confidentiality.

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____
Name (Printed) Date

_____ _____
Signature Phone Number

POLICY #19: INTERNAL ENFORCEMENT – SANCTION POLICY POLICIES AND PROCEDURES

POLICY: This policy addresses violations of federal and state privacy laws and/or the HIPAA Policies and Procedures of Case Western Reserve University ("CASE") ("Privacy and/or Security Violations") by workforce members of designated covered components at CASE. It is the policy of CASE to apply appropriate sanctions against faculty members, staff, other members of the CASE workforce, or students of designated covered components at CASE who fail to comply with CASE's Policies and Procedures.

PURPOSE: The purpose of this policy is to establish written guidelines for undertaking disciplinary action against workforce members of designated covered components at CASE or students who commit Privacy and/or Security Violations.

I. GENERAL RULES

A. Workforce members or students of designated covered components at CASE are encouraged to report possible Privacy and/or Security Violations to the CASE's Privacy and/or Security Officers.

B. Whenever possible Privacy and/or Security Violations arise, CASE's Privacy Officer, the School's HIPAA Representative, the Vice President of Human Resources, the Provost, or appropriate Vice President or Dean will conduct an investigation and determine whether a Privacy Violation has occurred.

C. If the Privacy and/or Security officer(s), the School's HIPAA Representative, the Provost, the Vice President for Human Resources, or appropriate Vice President or Dean (referred to as the "Appropriate Administrative Officer") determines that a workforce member of a designated covered component at CASEt has committed a Privacy and/or Security Violation, such member shall be subject to appropriate sanctions as determined by the Appropriate Administrative Officer, and/or Legal Counsel for CASE. Even if no actual Privacy and/or Security Violation has occurred, disciplinary measures may be imposed if otherwise warranted by the circumstances.

D. Appropriate sanctions may be based on factors such as the severity, frequency, degree of deviation from expectations, and length of time involved in any Privacy and/or Security Violations. Privacy and/or Security Violations may result in

disciplinary action consistent with the terms and conditions of CASE's Human Resources Policies and Procedures, Faculty Handbook, Student Services Guide, or any other CASE policy and procedure manual. Where otherwise permitted, CASE reserves the right to terminate employment at any time, for any reason, with or without undertaking any other disciplinary actions outlined in this policy. In light of the variety of possible situations that may arise, CASE may need to make decisions related to employment in a manner other than as provided in this policy.

E. The sanctions that may be imposed because of a Privacy and/or Security Violation may include, but are not limited to, informal counseling, verbal warning, written warning, suspension or termination. An employee may also be placed on probation or demoted. Restitution will be required if appropriate in the circumstances. In all cases, whether to impose sanctions, and the appropriate sanctions to impose, are within the discretion of CASE. In most cases the sanction will depend on the seriousness of the offense, among other factors. *See* Section II, below.

F. A manager or supervisor, even if he or she did not actually commit a Privacy and/or Security Violation, may also be sanctioned in connection with a Privacy and/or Security Violation to the extent that inadequate supervision or a lack of due diligence contributed to the violation, or if the manager or supervisor's conduct was culpable or sanctionable in other ways. Managers and supervisors may be sanctioned for failing to detect noncompliance with applicable policies (including CASE's Policies and Procedures) and legal requirements, where reasonable diligence would have led to the discovery of any problems or violations.

G. A record of any Privacy and/or Security Violation and any discipline imposed in connection with such Privacy and/or Security Violation shall be maintained in the employee's personnel file with a copy to be filed in a master file maintained by the CASE Privacy and/or Security officer(s) or the Appropriate Administrative Officer in accordance with applicable policies of CASE.

II. ENFORCEMENT OF SANCTIONS

The following section discusses the imposition of sanctions in the event of a Privacy and/or Security Violation. The type of sanction(s) imposed will generally reflect the seriousness of the Privacy and/or Security Violation. Factors which may be considered in determining an appropriate sanction may include the severity, frequency, degree of deviation from expectations, and length of time involved in a Privacy and/or security Violation. Some offenses, such as intentional violations, are so serious that they will justify termination or suspension on the first offense. For offenses that may not justify serious discipline on the first offense, lesser sanctions may be applied in the discretion of CASE. Progressive discipline is not a right, and CASE reserves the right to impose discipline or to terminate employment at any time, for any reason, with or without undertaking any of the other sanctions outlined in this policy.

A. Informal Counseling. The Appropriate Administrative Officer or Privacy and/or Security Officer(s) may engage in informal counseling with respect to privacy and/or security issues and/or Privacy and/or Security Violations that do not warrant more severe sanctions. Documentation of informal counseling may be maintained in personnel and departmental files.

B. Verbal Warning. The Appropriate Administrative Officer or Privacy and/or Security Officer(s) may issue a verbal warning to an employee. Documentation of the verbal warning will be maintained in personnel and departmental files.

C. Written Warning. The Appropriate Administrative Officer, in consultation with the Privacy and/or Security Officer(s), may issue a written warning to an employee. Such a warning may be appropriate, for example, when the behavior of the employee is a repeated violation and verbal counseling has been administered, or the violation is more serious in nature and/or subjects CASE to potential legal liability. Written warnings will be documented in personnel and departmental files.

D. Probation. In appropriate circumstances an employee may be placed on probation for a specified period of time. When probation is imposed, the employee will generally be provided with a written description of the behavior that resulted in the probation and the required behavioral or performance objectives that must be met in order to remove the employee from probation. Copies of documents relating to probations will be kept in personnel and departmental files.

E. Suspension. Suspension, or temporary release from duty, is a more severe action that may be imposed in the discretion of CASE. Suspension may also be used during investigations in order to more easily conduct such investigations.

1. Suspensions may be issued when, in the discretion of CASE, it is determined that a second warning would not suffice or that an initial incident is too severe for a warning yet not sufficiently severe for termination. Suspensions may vary in length, according to the severity of the Privacy and/or Security Violation. Suspensions may be paid or unpaid, in the discretion of CASE and consistent with applicable laws.

2. Suspensions will be documented in personnel and departmental files.

F. Demotion. In appropriate circumstances, an employee may be demoted (transferred to a lower-level position) as a sanction for Privacy and/or Security Violations. Demotions will be documented in personnel and departmental files.

G. Termination of Employment. Termination of employment is generally the most serious disciplinary sanction for Privacy and/or Security Violations.

1. In situations where employment with CASE is at-will, and may be terminated at any time and for any reason, the decision to terminate an employee for a Privacy and/or Security Violation is in the discretion of CASE. Termination as a disciplinary sanction may, for example, be imposed after other disciplinary measures have failed or when a Privacy and/or Security Violation merits such sanction as determined in the sole discretion of CASE.

2. Copies of relevant documentation pertaining to terminations will be maintained in personnel and departmental files.

H. Restitution. Where an employee's Privacy and/or Security Violations have caused harm or damage to CASE, sanctions may include restitution to CASE.

III. ACTIONS THAT MAY RESULT IN SANCTIONS

Without limiting CASE's right to discharge an employee at any time, with or without cause, the following acts of misconduct are provided as nonexclusive examples of Privacy and/or Security Violations that may result in sanctions up to and including termination.

- Misuse or theft of PHI, with or without the intent to unlawfully sell the information to an outside party.

- Failure to properly maintain an up-to-date accounting of instances in which CASE has released an individual's PHI to a third party.

- Discussion of an individual's PHI in the presence of unrelated third parties.

- Disclosure of PHI for research purposes without a proper authorization or waiver of authorization, where such disclosure is not otherwise permitted under the Privacy and Security Rules.

Below are examples of privacy and security violations:

Examples
LESS SEVERE:
▪ Failing to log-off/close or secure a computer with protected health information displayed. ▪ Leaving a copy of protected health information (PHI) in a non-secure area. ▪ Dictating or discussing protected health information (PHI) in a non-secure area (lobby, hallway, cafeteria, elevator)
▪ Sharing ID/password with another coworker or encouraging a coworker to share ID/password. ▪ Repeated violation of previous levels
MORE SEVERE:
▪ Accessing or allowing access to protected health information (PHI) without having a legitimate reason. ▪ Giving an individual access to your electronic signature. ▪ Repeated violation of previous levels.
▪ Accessing or allowing access to protected health information (PHI) without having a legitimate reason and disclosure or abuse of the protected health information (PHI). ▪ Using protected health information (PHI) for personal gain. ▪ Tampering with or unauthorized destruction of information. ▪ Repeated violations of previous levels

INTERNAL ENFORCEMENT: FREQUENTLY ASKED QUESTIONS

A. *Do the Privacy and Security require the CASE Privacy and/or Security Officer(s) to be involved in the employee sanctions process?*

No. The Privacy and Security require only that CASE have and apply appropriate sanctions against employees who fail to comply with the Privacy and Security or CASE's Policies and Procedures, and that CASE document any sanctions that are applied. In practice, the Privacy and/or Security Officer(s) should consult with the Appropriate Administrative Officer in determining whether and how to sanction an employee for a Privacy and/or Security Violation.

B. *Do the Privacy and Security provide specific penalties for any particular violations?*

No. Employee sanctions may be based on factors such as the severity, frequency, degree of deviation from expectations, and length of time involved in any Privacy and/or Security Violations. However, the appropriate sanctions to impose are within the discretion of CASE. Privacy and/or Security Violations may result in disciplinary action including, but not limited to: informal counseling, verbal warning, written warning, probation, suspension, demotion, dismissal or restitution.

C. *Will an employee be subject to sanctions for reporting a suspected violation of CASE's Policies and Procedures?*

No. In fact, all employees are strongly encouraged to report actual or suspected Privacy and/or security Violations to their supervisor or the CASE Privacy and/or Security Officer(s). CASE will not impose sanctions on any employee who in good faith reports a suspected Privacy and/or Security Violation simply because of such reporting.

I

PRIVACY AND/OR SECURITY OFFICER(S)'S INCIDENT EVENT LOG
SAMPLE FORM

Date Received	Date Investigation Complete	Nature of Complaint	Results of Investigation	Sanctions

POLICY #20: MITIGATION OF HARMFUL EFFECTS ON PRIVACY AND SECURITY RULE VIOLATIONS

POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to mitigate, to the extent practicable, any harmful effect known to CASE of a use or disclosure of protected health information made in violation of its Policies and Procedures or the requirements of the Privacy and Security Rules, to the extent that such use or disclosure is made by CASE and/or one of its business associates.

PURPOSE: The purpose of this policy is to state CASE's commitment to mitigation of any harmful effects known to CASE of a use or disclosure of PHI made in violation of the Privacy and Security Rules.

I. MITIGATION

A. Importance of Confidentiality. CASE has adopted its Policies and Procedures in part to ensure the confidentiality and protection of PHI maintained by CASE and/or its business associates. CASE respects the confidentiality and privacy of PHI. To the extent that PHI is used or disclosed by CASE and/or one of its business associates in a manner not permitted by the Privacy and Security Rules, CASE will take action to mitigate any harmful effect of such use or disclosure to the extent such harmful effect is known to CASE.

B. Mitigating Steps. CASE may take any one or more of the following actions to mitigate any harmful effects of a use or disclosure of PHI made in violation of the Privacy Security Rules:

1. recover the PHI which was used or disclosed from the party who participated in the use of or received a disclosure of PHI not permitted under the Privacy and Security Rules (a "recipient");

2. request assurances from a recipient that all PHI that was used or disclosed other than as permitted by the Privacy and Security Rules has been returned to CASE and that no copies of such PHI were retained by the recipient or any of its employees or agents;

3. obtain from the recipient an itemization of any uses or disclosures of the PHI made by the recipient;

4. notify such persons or entities as it deems appropriate and in a manner determined in its discretion that PHI may have been used or disclosed other than as permitted by the Privacy and Security Rules and request such other persons or entities to cooperate in mitigating any harmful effects of such use or disclosure that are known to CASE; and

5. other appropriate actions as determined in the discretion of CASE.

II. REPORTING

Any member of CASE's workforce who becomes aware of any use or disclosure of PHI in a manner not permitted by the Privacy and Security Rules and/or CASE's Policies and Procedures should report relevant information concerning the use or disclosure to the CASE privacy officer.

III. IMPLEMENATION OF MITIGATION

Upon receipt of a report of a possible use or disclosure of PHI other than as permitted by the Privacy and Security Rules and or the Policies and Procedures, the CASE privacy officer shall investigate such report, and, if appropriate, shall apply the procedures specified in this policy to mitigate any harmful effects of such use or disclosure as are known to CASE.

IV. SANCTIONS

Any member of CASE's workforce who participates in or facilitates a use or disclosure of PHI not permitted by the Privacy and Security Rules or CASE's Policies and Procedures is subject to sanctions in a manner consistent with the "Internal Enforcement" policy of CASE's Policies and Procedures.

MITIGATION: FREQUENTLY ASKED QUESTIONS

A. *Must CASE always take action in the event of an improper use or disclosure of protected health information?*

No. CASE must only take steps in mitigation of harmful effects of an improper use or disclosure that are known to CASE.

B. *Must CASE fully mitigate any harmful effects that are known to it on account of an improper use or disclosure of PHI?*

CASE is required to mitigate harmful effects to the extent practicable. CASE is not required to eliminate harm unless it is practicable to do so.

C. *Does the duty to mitigate harmful effects apply to a violation of CASE's Policies and Procedures as well as to a violation of the Privacy and Security Rules?*

Yes. Harmful effects that are known to CASE that arise from either a violation of the Privacy and Security Rules or CASE's Policies and Procedures must be mitigated to the extent practicable.

POLICY #21: REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will not intimidate, threaten, coerce, discriminate against or take any other retaliatory action against any person for exercising rights with respect to their PHI.

PURPOSE: The purpose of this policy is to express CASE's opposition to any retaliation against an individual with respect to the individual's exercise of rights related to the privacy of PHI.

I. INTRODUCTION

The Privacy Rules provide that a covered entity may not intimidate, threaten, coerce, discriminate against or take other retaliatory action (a "Retaliatory Act") against certain persons or entities for actions taken in connection with PHI and/or the Privacy Rules.

II. PROHIBITIONS

CASE will not perform any Retaliatory Act with respect to any individual because of the:

A. exercise by the individual of any rights under the Privacy Rules;

B. participation by the individual in any processes established under the Privacy Rules, including the filing of a complaint with respect to CASE's compliance with the Privacy Rules and/or its Policies and Procedures;

C. filing of a complaint by the individual with the Secretary of the United States Department of Health and Human Services concerning CASE's compliance with the Privacy Rules;

D. the actions of such individual in testifying, assisting or participating in an investigation, compliance review proceeding or hearing under Part C of Title 11 of the Social Security Act;

E. the opposition of such individual to any act or practice of CASE made unlawful under the Privacy Rules provided that such individual has a good faith belief that the practice opposed is unlawful and the manner of such individual's opposition is reasonable and does not involve a disclosure of protected health information in violation of the Privacy Rules.

III. REPORTING

Any member of CASE's workforce who becomes aware of any Retaliatory Act should report relevant information concerning such act to the CASE privacy officer.

IV. CORRECTIVE MEASURES

Upon receipt of a report of a possible Retaliatory Act, the CASE privacy officer shall investigate such report, and, if appropriate, apply the procedures specified in this policy to prevent any future occurrences of Retaliatory Acts.

IV. SANCTIONS

Any member of CASE's workforce who participates in or facilitates a Retaliatory Act is subject to sanctions in a manner consistent with the "Internal Enforcement" policy of CASE's Policies and Procedures.

INTIMIDATING AND RETALIATORY ACTS:

FREQUENTLY ASKED QUESTIONS

A. *What is an example of conduct that might be considered to be in violation of this policy?*

An example of conduct that would violate this policy is threatening to not provide treatment to an individual because the individual made a complaint to CASE's privacy officer about a failure to comply with the Privacy Rules.

B. *Is refusing to provide an item or services to an individual because of a refusal by the individual to pay for such item or services wrongful?*

No, so long as the refusal has nothing do with any exercise of privacy rights by the individual. A refusal to provide services because an individual refuses to pay is not considered a retaliatory, threatening or intimidating act for purposes of the Privacy Rules.

POLICY #22: WAIVER OF RIGHTS
POLICIES AND PROCEDURES

POLICY: Case Western Reserve University ("CASE") will not require any individual to waive her or his rights to file a complaint with respect to privacy or any other rights under the Privacy Rules as a condition of treatment, payment, enrollment in a CASE-sponsored health plan or eligibility for benefits.

PURPOSE: The purpose of this policy is to state CASE's position to not require waivers of privacy rights as a condition of treatment, payment, enrollment in a CASE-sponsored health plan or eligibility for benefits.

I. WAIVERS NOT REQUIRED

CASE will not require any individual to waive either (a) her or his right to file a complaint with the Secretary of the Department of Health and Human Services concerning CASE's compliance with the HIPAA privacy rules, or (b) any of her or his other rights under the Privacy Rules as a condition of treatment, payment, enrollment in a CASE-sponsored health plan or eligibility for benefits.

II. EXCEPTIONS

This policy does not prohibit CASE from requiring an authorization for use or disclosure of PHI:

(a) before an individual may receive research-related treatment;

(b) prior to enrollment in any CASE-sponsored health plan or permitting such individual to be eligible to receive benefits from the plan if the authorization is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk-rating determinations; or

(c) as a condition to the provision of health care that is solely for the purpose of creating PHI for disclosure to a third-party, so long as such authorization concerns disclosure to such third-party.

WAIVER: FREQUENTLY ASKED QUESTIONS

A. *To what types of individual rights under the Privacy Rules does the prohibition against waivers of rights apply?*

Individuals have a number of specific rights under the Privacy Rules. These include the right to request additional privacy protections, confidential communications and amendments of PHI, the right to access their PHI and the right to an accounting of disclosures of their PHI. It is impermissible to require a patient to waive her or his right to exercise any of these rights or to file a complaint about CASE's compliance with the Privacy Rules.

POLICY #23: DOCUMENTATION OBLIGATIONS POLICIES AND PROCEDURES

POLICY: It is the policy of Case Western Reserve University ("CASE") to comply with all requirements of the Privacy and Security Rules concerning documentation.

PURPOSE: The purpose of this policy is to establish a process by which CASE will comply with obligations under the Privacy and Security Rules to maintain certain documentation related to PHI and the performance of certain of CASE's obligations under the Privacy and Security Rules.

I. OBLIGATIONS

A. CASE shall maintain its HIPAA policies and procedures in written or electronic form.

B. If a communication is required by the Privacy and Security Rules or the CASE's Policies and Procedures to be in writing, CASE shall maintain such writing, or an electronic copy, as documentation.

C. If CASE is required by the Privacy and Security Rules or the Policies and Procedures to document an action, activity or designation, CASE shall maintain a written or electronic record of such action, activity or designation.

II. IMPLEMENTATION

A. The CASE Privacy and Security Officers shall maintain all CASE Policies and Procedures, as they may be amended from time to time, in written or electronic form.

B. The CASE Privacy and Security Officers shall maintain in writing, or in electronic form, every communication required by the Policies and Procedures to be in writing.

C. The CASE Privacy and Security Officers shall maintain a written or electronic record of each action, activity or designation required by the Privacy and Security Rules or the Policies and Procedures to be documented.

III. RECORD RETENTION REQUIREMENTS

A. CASE shall retain all documentation required by the Privacy and Security Rules or the Policies and Procedures for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

B. All documentation required by this policy shall be retained by the CASE Privacy and Security Officers.

DOCUMENTATION: FREQUENTLY ASKED QUESTIONS

A. *What types of records are subject to the documentation requirements of the Privacy and Security Rules and CASE's Policies and Procedures?*

Two examples of records that must be retained under the documentation requirements of the Privacy and Security Rules and the Policies and Procedures are: (1) the designation of the HIPAA Privacy and Security Officers and contact person for CASE, and (2) the designated health care components of CASE.

B. *Who is responsible for maintaining the documentation required by the Privacy and Security Rules and the Policies and Procedures?*

CASE's Policies and Procedures require the CASE Privacy and Security Officers to maintain the required documentation.

C. *How long must the required documentation be retained under the Privacy and Security Rules and the Policies and Procedures ?*

The required documentation must be retained for six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

POLICY #24: BUSINESS ASSOCIATES POLICIES AND PROCEDURES

POLICY: All agreements with business associates of Case Western Reserve University ("CASE") must be in writing and must contain certain mandatory provisions designed to protect the privacy and security of individuals' PHI. CASE personnel shall not disclose PHI to a business associate without a signed business associate agreement.

PURPOSE: The purpose of this policy is to protect, through the execution and enforcement of written agreements, the privacy and confidentiality of PHI that CASE discloses to individuals and entities that are business associates of CASE.

I. INTRODUCTION

A. Need for business associate agreements. From time to time, CASE may contract with an individual or company to provide services to CASE or on behalf of CASE. If such a relationship involves sharing PHI that CASE maintains, then CASE is required to enter into a written contract, known as a "business associate agreement," with the individual or company. The primary purpose of the agreement is to ensure that the business associate will use or disclose the PHI for lawful purposes only.

B. General rules regarding business associates. The Privacy Rules define a business associate as a person or entity that provides certain functions, activities, or services to or for CASE, involving the use or disclosure of PHI. CASE may disclose PHI to a business associate, or allow the business associate to create or receive PHI on its behalf, so long as CASE and the business associate enter into a valid business associate agreement.

C. Limitations on the use of PHI. The business associate may only use the PHI that it receives in its capacity as CASE's business associate as permitted by law and its contract with CASE.

D. Additional compliance obligations. Disclosures of PHI to business associates must comply with all of CASE's other Policies and Procedures.

II. IDENTIFICATION OF A BUSINESS ASSOCIATE

A. Definition. A business associate is a person or entity who, other than as a member of CASE's workforce:

1. on behalf of CASE performs or assists in the performance of functions or activities involving the use or disclosure of individually identifiable health information, including, without limitation, PHI; examples of such functions include but are not limited to:
   - claims processing or administration
   - data analysis, processing or administration
   - utilization review
   - quality assurance
   - billing
   - benefit management
   - practice management, or
2. provides one of the following services to CASE where the provision of services involves the disclosure of individually identifiable health information:
   - legal
   - actuarial
   - accounting
   - consulting
   - data aggregation
   - management
   - administrative
   - accreditation
   - financial.

B. Workforce. Members of CASE's workforce are not considered business associates.

C. Treatment exception. When CASE discloses PHI to a health care provider for the purpose of providing treatment to the individual, the health care provider is not considered a business associate.

III. PROPOSED AGREEMENTS WITH BUSINESS ASSOCIATES

A. Proposed business associate agreements. CASE's employees must forward to CASE's privacy officer all proposed agreements between CASE and an entity or individual pursuant to which CASE may provide access to PHI. It is CASE's preference to utilize the attached form Business Associate Agreement for use with CASE's business associates.

B. Review of proposed agreements. To determine whether a business associate agreement is required, the privacy officer and legal counsel will review each proposed agreement between CASE and an outside contractor if the contractor will use and disclose PHI pursuant to the agreement.

IV. REQUIRED ELEMENTS OF A BUSINESS ASSOCIATE AGREEMENT

A. A business associate agreement must be in writing and must include provisions that:

1. establish the permitted and required uses and disclosures of PHI by the business associate, which may include the use and disclosure of PHI for the proper management and administration of its business and to provide data aggregation services for CASE;

2. provide that the business associate will:

a. not use or further disclose the PHI, other than as required by the contract or applicable law;

b. use appropriate safeguards to be implemented by the business associate to prevent inappropriate use or disclosure;

c. report to CASE any inappropriate use or disclosure of PHI of which it becomes aware;

d. ensure that agents and subcontractors of the business associate who receive PHI from CASE also agree to the same restrictions and requirements with regard to use and disclosure of PHI;

e. make available PHI as necessary for compliance with the Privacy Rules' requirement to allow individuals to review and copy their PHI;

f. make available PHI as necessary to address an individual's request to amend his or her PHI;

g. make available PHI as necessary to provide an accounting of disclosures;

h. make its internal practices, books, and records concerning PHI received from or created or received on behalf of CASE available to the Department of Health and Human Services; and

i. upon termination of the contract, return or destroy (or if not feasible, continue to protect) all PHI received from or created or received on behalf of CASE; and

3. authorize CASE to terminate the contract if the business associate violates a material term of the contract.

B. Optional provisions in the business associate contract. In addition to the required elements listed above, the business associate contract may also contain additional elements.

1. The business associate contract may permit the business associate to use the PHI it receives from CASE for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate if:

a. the disclosure is required by law; or

b. the business associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law for the purpose for which it was disclosed to that person, and the person notifies the business associate of any instances of which the person is aware in which the confidentiality of the PHI has been breached.

2. The business associate contract may permit the business associate to provide data aggregation services to CASE.

V. PRIVACY AND SECURITY VIOLATIONS COMMITTED BY A BUSINESS ASSOCIATE

A. Duty to notify. If a CASE employee or other staff personnel knows or has reason to believe that a business associate of CASE is inappropriately using or disclosing PHI, whether the PHI was received by CASE or not, the employee or other staff personnel is required to notify CASE's Privacy Officer immediately regarding the suspected violation.

B. Review of alleged violations. Upon receiving notice of an alleged or actual violation of a business associate agreement from any source, including notice obtained through individual complaints and reports from CASE personnel, CASE's Privacy Officer will initiate a review of the conduct or activities at issue.

C. Investigation and resolution of violations. If the CASE Privacy Officer determines that the complaint, report or other form of notice contains substantial and credible evidence of violations by a business associate, the Privacy Officer will commence a formal investigation into the conduct or activities of the business associate.

1. If the investigation reveals that a business associate has violated its agreement with CASE, the Privacy Officer shall notify the Vice President and General Counsel immediately.

2. If the Privacy Officer, in consultation with the Vice President and General Counsel, determine that the business associate has committed a material breach or violation of its obligations under the business associate agreement, the Privacy Officer, with the assistance of the Vice President and General Counsel, must take reasonable steps to remedy the breach or terminate the contract of a business associate when feasible. If termination of the contract is not feasible, CASE must report the problem to the Department of Health and Human Services ("HHS").

BUSINESS ASSOCIATES: FREQUENTLY ASKED QUESTIONS

A. *Are all companies or entities with which CASE does business considered business associates?*

No. The business associate relationship does not describe all relationships between CASE and other persons or organizations. Business associate contracts are only required for those cases in which CASE is disclosing PHI to a person or organization that will use the PHI on behalf of CASE (as if it were standing in the shoes of CASE), when the other person or organization will be creating or obtaining PHI on behalf of CASE, or when the business associate is providing specified services to or for CASE and the provision of those services involves the disclosure of PHI by CASE to the business associate (*e.g.*, legal advice and accounting services).

B. *Is CASE required to enter into business associate agreements with entities such as couriers, janitorial services or financial institutions?*

No. CASE is not required to enter into a business associate contract with a person or organization that acts merely as a conduit for PHI (*e.g.*, the US Postal Service or private couriers). A conduit transports information but does not access it other than on a random or infrequent basis as may be necessary for the performance of the transportation service or as required by law. Because CASE does not intend for any disclosure of PHI to occur and the probability of exposure of any particular PHI to a conduit is very small, conduits are not considered business associates of CASE.

CASE need not enter into a business associate contract with a person or entity who has only incidental or minimal contact with PHI. For example, a business associate contract is not required between CASE and a janitorial service, despite the fact that the service's janitor may accidentally see PHI while cleaning CASE's facilities.

Banks and other financial institutions are not considered to be acting on behalf of CASE. Therefore, no business associate contract is required when CASE processes consumer financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or transfers funds for payment to CASE.

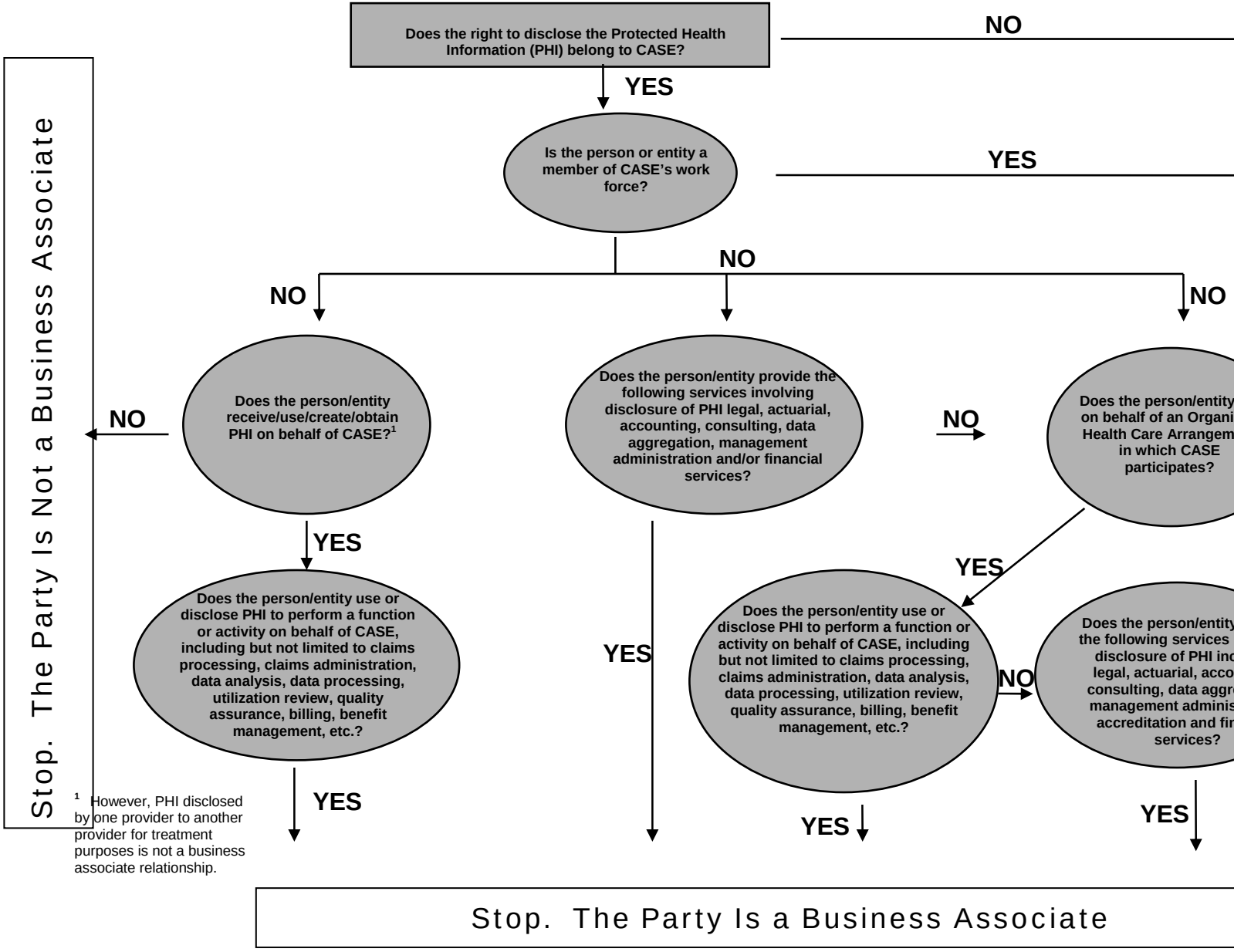
C. *Is CASE required to enter into business associate agreements with individuals' insurance companies or health plans?*

No. CASE is not required to enter into a business associate contract with an insurance company or health plan. Although it is possible for CASE to be both a covered entity and a business associate to another covered entity under certain circumstances, this is not

one of those situations. When the insurance company discloses PHI to CASE to allow

CASE to determine the individual's insurance coverage and submit a payment claim, CASE is not providing a service to, or on behalf of, the insurance company. CASE is simply following the procedures necessary to obtain payment for services provided to the individual. Similarly, the insurance company is not considered a business associate of CASE when CASE discloses PHI to the insurance company for payment purposes.

A GUIDE FOR THE PRIVACY OFFICER TO IDENTIFY BUSINESS ASSOCIATES



[1] However, PHI disclosed by one provider to another provider for treatment purposes is not a business associate relationship.

BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT is made by and between **CASE WESTERN RESERVE UNIVERSITY** ("CASE") and ________ ("Business Associate"). The purpose of this Agreement is to comply with the privacy standards of the Health Insurance Portability and Accountability Act of 1996 and the applicable regulations promulgated thereunder (collectively referred to as "HIPAA") as those standards and regulations pertain to business associate relationships.

I. OBLIGATIONS OF BUSINESS ASSOCIATE

Section 1.1 **Use and Disclosure of Protected Health Information**. For the purposes of compliance with HIPAA, Business Associate's relationship with CASE shall be considered that of "Business Associate." As used hereunder, the terms "Business Associate", "Protected Health Information", "use" and "disclosure" shall have the meanings ascribed to them in 45 CFR Sections 160.103, 164.501 and 164.504.

Business Associate agrees to conduct its business with CASE in accordance with all applicable laws and regulations, including HIPAA. Business Associate further agrees to comply with all policies and procedures adopted by CASE related to use and disclosure of Protected Health Information.

Disclosure by CASE to Business Associate of any Protected Health Information will be made for the sole purpose of helping CASE carry out its healthcare functions and to allow Business Associate to complete its contractual obligations to CASE. Protected Health Information will not be used or disclosed by Business Associate other than as permitted by this Agreement or applicable law. Business Associate may not use any Protected Health Information for any of its purposes or activities not related to this Agreement. Business Associate represents and warrants that it will use Protected Health Information only to complete its obligations pursuant to this Agreement, and as may otherwise be required by law.

Section 1.2 **Safeguards Against Misuse of Information**. Business Associate covenants, represents and warrants that it will safeguard and protect all Protected Health Information from use and/or disclosure other than as provided by this Agreement, and that upon Business Associate's learning of any misuse or improper disclosure of Protected Health Information, Business Associate will take immediate steps to stop such impermissible use or disclosure and to prevent further dissemination or misuse of such Protected Health Information.

Section 1.3 **Reporting of Disclosures of Protected Health Information.** Business Associate further represents and warrants that it will immediately report to CASE and/or its Privacy Officer any use or disclosure of Protected Health Information not provided for by this Agreement of which Business Associate becomes aware.

Section 1.4 **Agreements by Third Parties**. Business Associate covenants, represents and warrants that it will cause its agents, including any subcontractor(s) to whom it may provide Protected Health Information received from, or received or created by Business Associate on behalf of CASE, to agree to the same restrictions and conditions that apply to Business Associate with respect to such Protected Health Information. Business Associate further agrees it will incorporate in any and all agreement(s) with subcontractor(s) to whom it discloses PHI subject to and/or protected by this Agreement a provision naming CASE as an intended third party beneficiary with respect to the enforcement of, and right to benefit from, the subcontractor's covenants regarding the use and disclosure of Protected Health Information.

Section 1.5 **Access to Information.** Business Associate agrees to make available Protected Health Information within ten (10) days of a request by CASE. If any individual requests access to Protected Health Information directly from Business Associate, Business Associate shall provide information concerning such request to CASE. Any denials of access to the Protected Health Information shall be decided solely by CASE.

Section 1.6 **Availability of Books and Records**. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the Department of Health and Human Services for purposes of determining CASE's compliance with HIPAA.

Section 1.7 **Availability of Protected Health Information for Amendment.** Business Associate agrees to provide to CASE an individual's Protected Health Information for amendment within ten (10) days of a receipt of a request from CASE. Business Associate further agrees to incorporate any approved amendments into the Protected Health Information in accordance with the requirements of 45 C.F.R. §164.526.

Section 1.8 **Accounting of Disclosures**. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for CASE to respond to a request by an individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528 (an "Accounting"). Within ten (10) days of receipt of notice by Business Associate from CASE that CASE has received a request for an Accounting, Business Associate agrees to make available to CASE any information in Business Associate's possession that is required for CASE to make the Accounting in accordance with the requirements of 45 C.F.R. §164.528, provided that Business Associate need not provide information about disclosures of Protected Health Information: related to treatment, payment, or health care operations: made to the individual who is the subject of the relevant PHI or pursuant to an authorization from such individual; or made earlier than six (6) years prior to the date on which the Accounting was requested. If any individual requests an Accounting directly from Business Associate, Business Associate shall, within three (3) days of receipt of such request, forward the request to CASE.

Section 1.9 **Mitigation**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

Section 1.10 **Security**. Business Associate shall:

(a) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on behalf of CASE as required by 45 C.F.R. Part 164, Subpart C;

(b) ensure that any agent, including a subcontractor, to whom Business Associate provides electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on behalf of CASE, agrees to implement reasonable and appropriate safeguards to protect it; and

(c) report to CASE any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in any way connected with electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on behalf of CASE, of which Business Associate becomes aware.

II. TERMINATION OF AGREEMENT

Section 2.1. **Term**. The Term of this Agreement shall be effective as of _____ _____, _____ and shall terminate when all of the Protected Health Information provided by CASE to Business Associate, or created or received by Business Associate on behalf of CASE, is destroyed or returned to CASE, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

Section 2.2 **Termination for Cause**. Upon CASE acquiring knowledge of a material breach of this Agreement by Business Associate, CASE shall either:

(a) give notice to Business Associate and provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement [and any other related agreement(s) with Business Associate (which such other agreement(s) shall hereby be amended to be consistent with this termination provision of this Agreement)] if Business Associate does not cure the breach or end the violation within the time specified by CASE;

(b) immediately terminate this Agreement [and any other related agreement(s) with Business Associate (which such other agreement(s) shall hereby be amended to be consistent with this termination provision of this Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible or CASE deems, in its total discretion, that such termination is necessary; or

(c) if neither termination nor cure are feasible, CASE shall report the violation to the Secretary.

Section 2.3 **Return/Destruction of Protected Health Information**. Business Associate agrees that upon termination of this Agreement, Business Associate shall return or destroy all Protected Health Information received from, or received or created by Business Associate on behalf of CASE, and Business Associate agrees that it will not maintain copies of such Protected Health Information in any form, except as might otherwise be required and/or permitted by applicable law, in which event, Business Associate shall continue to protect the confidentiality of any such Protected Health Information in a manner consistent with this Agreement. The provisions of this Agreement regarding uses and disclosures of Protected Health Information shall continue beyond termination of this Agreement.

Section 2.4 **Right to Cure**. At the expense of Business Associate, CASE shall have the right to cure any breach of Business Associate's obligations under this Agreement. Business Associate agrees to cooperate and comply with the efforts by CASE to cure any such breach.

III. MISCELLANEOUS

Section 3.1 **Effect**. This Agreement, including all exhibits or other attachments thereto, constitutes the final, complete and exclusive understanding between the parties with respect to the subject matter of this Agreement and supersedes any prior or contemporaneous agreement.

Section 3.2 **Amendment**. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by the party to be charged. Business Associate and CASE agree to amend this Agreement to the extent necessary to permit either party to comply with the Privacy

Standards (the "Standards"). Business Associate agrees to comply with all such Standards and amend this Agreement to incorporate any material required by the Standards.

Section 3.3 **Indemnification**. Business Associate hereby agrees to indemnify and hold CASE harmless from and against all liability and costs, including attorneys' fees, created by a breach of this Agreement by Business Associate, its agents and subcontractors.

IN WITNESS WHEREOF, CASE and Business Associate have executed this Agreement as of _____ _____, 200___.

Case Western Reserve University

By: _____

Title: _____

_____
[Name of Business Associate]

By: _____

Title: _____

POLICY #25: PASSWORD MANAGEMENT POLICIES AND PROCEDURES FOR WORKFORCE OF COVERED COMPONENTS

POLICY: Users who are workforce members of covered components are responsible for Network-ID accounts and any activities that are made using it. The password associated with the Network-ID is what protects an account from unauthorized access. Passwords must meet the minimum requirements as outlined in this policy.

PURPOSE: Passwords are the means by which the identity of system users is validated and information is protected from unauthorized access. If someone else obtains the password, they can use a user's account to peruse private data, including PHI, electronic mail and ERP personal records; alter or destroy files; and perform illegal activities in user's name. As a result, the proper selection and protection of a password are very important.

I. OBLIGATIONS

Computer system users who are workforce members of a covered component should choose passwords that cannot be easily guessed using the following standards:

- Passwords must be a minimum of eight characters and must contain more than one character types such as letters (a-z, A-Z), numbers (0-9), or symbols (!@#$ etc.).
- Passwords must be cryptic and not easily guessed.
- Passwords will automatically expire at least every 180 days.
- Passwords cannot be reused.
- Passwords must be maintained in a confidential manner:
    - User accounts and passwords cannot be shared.
    - Passwords should not be posted or kept in hard copy in an insecure location.
    - Passwords should never be sent via electronic messages (e.g., e-mail) without encryption.
    - Passwords to access any of Case's systems should not be used on any external (non-Case) systems (e.g., Internet accounts).
    - Passwords should be immediately changed if they are suspected or are known to have been disclosed to unauthorized parties.
- [*R. LeClerc will revise:*] Unattended computers should be locked. This will be enforced by having Case's computers automatically lock after 20 minutes of

inactivity. A locked computer session will require the user to provide their password to regain use of their system.

II. GUIDELINES

The ideal password is easy to remember but difficult for someone else to guess. This will allow users not write it down, where it can be discovered, while being sufficiently strong to prevent security breaches.

When constructing and using a password, users should abide by the following guidelines:

Do not use personal information – Such as names (including self, family members, friends, coworkers, pets), permutations of the user-ID, hobbies, phone numbers, birth dates, social security numbers, home town or street, automobile brand, computer systems being used, business functions, or other information about one's self that is readily discovered.

Do not use commonly used words – For example 'Case', 'password', department names, sports teams, celebrity names, seasons, days of the week, months or years.

Do not use consecutive keys, repeated keys, or simple keyboard patterns – Such as 'aaaa…', '1111…', 'abcd…', '1234…', 'qwerty', or 'ghjkl.'

Do not use a systematic, or a well-adhered to algorithm – For example, appending consecutive numbers to a word for each password change (e.g., '01', then '02', etc.).

Use as many different character types as possible – When forming your password, use numbers, punctuation characters, and mixed upper and lower-case letters. Choosing characters from the largest possible alphabet will make your password more secure.

Use a password that you can type quickly, without having to look at the keyboard – This makes it harder for someone to steal your password by watching over your shoulder.

Lock your computer when left unattended – Unattended computer sessions should be locked to prevent potential misuse. Use lock screen password protection (by typing 'Ctrl-Alt-Delete', then selecting 'Lock Workstation').

Change your password when in doubt – If you have any uncertainty about whether anyone else knows your password, change it immediately.

Examples

There are several methods that are available to assist you in choosing a secure, easy-to-remember password that conforms to the above guidelines. These include the following:

- Use the first letter of each word in a phrase, poem, or song that you can easily remember. Choose a line or two from a song or poem, and use the first letter of each

- word. For example, "<In Xanadu did Kubla Kahn a stately pleasure dome decree>" becomes "<IxdKKaspdd>."
- Intentionally use misspelled words, or words with a number or punctuation mark, preferably somewhere in the middle. Examples include: “kite276s”, and “w3aTH!er”.
- Choose two short words and concatenate them together with numbers or symbols between them. For example:

  dog + rain becomes "Dog:4rain"

  my + ninety-nine + books becomes "My9-9books"

- Use a pronounceable phrase that uses numbers or symbols to substitute for words. For example:

  “the number one winner” becomes "the#1Winner"

  “meet me at eight” becomes “meetME@8”

  “dollars to doughnuts” becomes “$2doughNuts”

NOTE: Please do not use any of the above examples verbatim! [? ? ? ? ?]

III. ENFORCEMENT

A violation of any provision of this policy may result in disciplinary action, up to and including the termination of employment, suspension of privileges or imposition of academic sanctions consistent with applicable CASE policies and procedures and see CASE HIPAA Policies and Procedures, “Internal Enforcement – Sanction Policy.”

POLICY #26: SECURITY OF ELECTRONIC INFORMATION AND SYSTEMS

POLICY: Case Western Reserve University (Case) will protect and secure electronic information and systems of covered components, prevent access to electronic information and systems by unauthorized individuals, and control and monitor access by authorized system users to individual records that the user has no legitimate need to view or use. Information Technology Services (ITS) will recommend specific institutional technology practices to achieve desired levels of information security cost-effectively and will monitor implementation of approved practices. Case-wide standards for the security of electronic information and systems will be developed by the Information Technology Services Policy Advisory Committee (ITSPAC) based on recommendations from ITS and other groups. These standards will become policy upon approval by the Provost and CFAO.

PURPOSE: The purpose of this policy is to protect electronic information and systems involving covered components from unauthorized disclosure, alteration, or destruction, while supporting timely access by authorized users.

I. OBLIGATIONS

C. CASE shall reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Security Rules and CASE's Policies and Procedures.

D. CASE shall reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure in accordance with the Security Rules and CASE's Policies and Procedures.

II. IMPLEMENTATION OF SECURITY OF ELECTRONIC INFORMATION & SYSTEMS AS TO COVERED COMPONENTS

- **Institutional Responsibilities**

ITSPAC develops CASE-wide standards that include, but are not limited to, standards for individual user authentication; encryption; access control and monitoring; transmission of confidential information; physical security of hardware; backup, retention, and archival or electronic information; and disaster recovery. These standards will become policy upon approval by the Provost and CFAO.

ITS implements and enforces security requirements for the electronic data and systems it manages. Through the Chief Information Security Officer (CISO), ITS also provides

support for CASE-wide adoption and adherence to approved security standards for electronic information and systems.

- **Organizational Unit Responsibilities**

  Management of each covered component, through its Chief Technology Officer (CTO), supports adherence to approved security standards for electronic information and systems.

- **Individual Responsibilities**

  Each workforce member of a covered component using electronic data and systems is responsible for knowing and adhering to established security standards.

  Each individual within CASE is also responsible for reporting immediately any known or suspected breach of the security or integrity of a system; the confidentiality of records/data obtained from a system; or any failure to adhere to approved security standards for electronic information and systems, to any of the following:

  - The manager, supervisor, or CTO of the organizational unit in which the breach or failure occurred.
  - The manager, supervisor, or CTO of the individual who witnessed the breach or failure.
  - CASE CISO
  - CASE Audit Officer
  - CASE Employee Relations Office
  - CASE Integrity Hotline

III. ENFORCEMENT

A violation of any provision of this policy may result in disciplinary action, up to and including the termination of employment, suspension of privileges or imposition of academic sanctions consistent with applicable CASE policies and procedures or the CASE HIPAA Policies and Procedures, "Internal Enforcement."

POLICY #27: SECURITY MANAGEMENT PROCESS

POLICY: Information is integral to Case Western Reserve University (CASE) and is a critical asset for the University. Case is committed to ensuring the integrity, reliability, availability and confidentiality of its data and computer system as they relate to PHI held by covered components. To maintain this standard of excellence, Case considers information security to be of paramount importance and an essential cornerstone of its operations.

PURPOSE: The purpose of this policy is to provide policies and procedures to prevent, detect, contain, and correct Security Violations regarding ePHI of covered components.

Senior Management has empowered the Information Security Officer and the Information Security Subcommittee composed of ITS Directors, CTOs and Faculty Senate to evaluate, establish, maintain and ensure compliance of control measures to protect the University's information resources from unauthorized or accidental modification, destruction or disclosure. The Information Security Subcommittee will advise ITSPAC and the Vice President for Information Technology Services - Chief Information Officer of the University on standards, policies and practices related to the security, risk assessment and compliance of rules and regulations used in support of campus-wide and school-based information security policies and procedures.

I. OBLIGATIONS OF INFORMATION SECURITY SUBCOMMITTEE

- Foster a collaborative approach to information security efforts across academic units, administrative units, and information technology services departments to mitigate risks through various technical and/or policy initiatives.
- Conduct risk analysis and risk management tasks.
- Developing security policies, standards, guidelines and procedures and other elements of an infrastructure to support information security.
- Architecting control measures to improve information security (including evaluating and selecting products and services).
- Assist in the development of scenarios of usage, test for abnormalities or exposures of application systems.
- Developing, presenting and managing the dissemination of information security awareness and training materials.

- Investigating alleged information security breaches and if necessary, assisting with disciplinary and legal matters to support information security.

- Reviewing and modifying existing policies/procedures (information system activity review.)

- Coordinating and monitoring information security activities throughout Case, including the preparation of periodic status and progress reports.

- Providing consulting assistance on implementation of information security controls (e.g. encryption system deployment, secure telecommunications and secure application system development procedures).

- Serving as liaison between the various groups dealing with information security matters (e.g. with business units, legal, human resources and auditors).

- Representing Case on information security matters to external groups.

II. BUSINESS JUSTIFICATION

Information security ensures business continuity and minimizes business damage by presenting or reducing the impact of security-related incidents. When established and maintained within Case, information security enables information to be shared while ensuring the integrity and protection of the data and technology assets.

III. ASSUMPTIONS

Information security must be kept in perspective and must be consistent with long-term business strategies. Cooperation of all Information Technology groups and business management leaders is needed for the effectiveness of the security program.

IV. VALUES AND CODE OF PRACTICE

The primary goal of the Information Security Subcommittee is to promote management practices that will ensure the confidentiality, integrity and availability of Case's information resources. To achieve this goal, the Information Security Subcommittee will:

- Support the establishment and compliance of appropriate information security policy, standards, procedures and controls for information security.

- Promote good information security concepts and practices.

- Maintain the confidentiality of all proprietary or otherwise sensitive information encountered in the course of professional activities. The information shall not be used for the personal benefit nor released to inappropriate parties.

- Use due care to obtain and document sufficient factual material on which to base conclusions and recommendations. Not to intentionally injure or impugn the professional reputation or practice of colleagues or clients.

- Inform the appropriate parties of the results of investigation work performed.

- Support the education of management, clients and the general public to enhance their understanding of auditing and information systems.

- Perform professional responsibilities with due diligence and honesty in accordance with the law and the highest ethical principles.