UMHS Policy 01-04-300
Introduction to Privacy and Security Concepts and Definitions

Effective Date: 04/14/2003 Last Reviewed: 10/2017 Last Revised: 10/2017

I. POLICY STATEMENT, PURPOSE AND SCOPE

It is the policy of the University of Michigan Health System that the privacy and information security of health information in our care is protected in accordance with applicable federal and state law. These privacy and information security policies use a variety of specialized terminology. This policy provides standardized definitions of those terms.

The purpose of this policy is to provide standardized definitions of the terminology used in the other UMHS privacy and information security-related policies. This policy includes some words and phrases used often, and is not a Privacy and Security glossary of terms.

This policy applies to all workforce members of UMHS except MHC and those subsidiaries and joint ventures of MHC that are not affiliated covered entities of the University or included in the University's organized health care arrangement. The policy refers to all information resources, whether verbal, printed, or electronic, and whether individually controlled, shared, stand alone or networked.

II. DEFINITIONS

Below are definitions of some words and phrases used often in this manual and in the HIPAA Privacy and HIPAA Security Rules. These words appear in italics when used throughout this manual.

**Administrative Safeguards** - Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

**Authorization** - The written permission we need before using or disclosing a patient's protected health information (“PHI”) for a purpose other than for treatment, payment, or health care operations, or other purposes specifically exempted from authorization. It has certain required elements. The current standard UMHS authorization is available at [http://www.med.umich.edu/him/ROI.pdf](http://www.med.umich.edu/him/ROI.pdf) or by contacting the Health Information Management Department.

**Breach** - The acquisition, access, use or disclosure of PHI that compromises the security or privacy of the PHI. However, breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Covered Entity or its Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under 45 CFR Part 160, Subpart E.

2. Any inadvertent disclosure by a person who is authorized to access PHI at the Covered Entity or its Business Associate to another person authorized to access PHI at the same Covered Entity or the same
Business Associate, or Organized Health Care Arrangement ("OCHA") in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under 45 CFR Part 160, Subpart E.

iii. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Unless specifically excluded above, an acquisition, access, use or disclosure of PHI in a manner not permitted under 45 CFR Part 160, Subpart E is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

Business Associate - A person or organization who (1) performs a function or activity on behalf of UMHS or other units of the UM Organized Health Care Arrangement ("OHCA") or (2) performs a specified service, where disclosure of individually identifiable health information is considered routine, such as legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services or (3) is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.

Compound Authorization - The combination of an authorization for use or disclosure of PHI with any other document.

Confidentiality - The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity - A health care provider, health plan, or health care clearinghouse regulated by HIPAA. The University of Michigan is a "hybrid" covered entity because some units, including UMHS, are regulated by HIPAA. A unit is considered included in the U-M Hybrid Covered Entity if it is a health care provider, a health plan, and/or serving as an "internal" business associate to another unit within the U-M Hybrid Covered Entity or serving as a business associate to an external covered entity or external business associate.

De-identified - Information is "de-identified" (and not subject to the Privacy Rule or these policies and procedures) if it does not identify a patient and if there is no reasonable basis to believe that it could be used to identify a patient. See UMHS Policy 01-04-340 De-identification and Re-identification of Protected Health Information (PHI) regarding removal of specific identifiers to de-identify information.

Designated Record Set - See Policy 01-04-306, UMHS Designated Record Set.

Disclosure - The release, transfer, provision of access to, or divulging in any other way of PHI outside the UM OHCA. See also Use (defined below).

Electronic Media - PHI that is transmitted by electronic media or maintained in electronic media.
**Electronic Protected Health Information (ePHI)** - PHI that is transmitted by electronic media or maintained in electronic media.

**Encryption** - The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

**Family Member** - (1) A person who is a dependent of an individual as the result of marriage, birth, adoption or placement for adoption, or (2) A first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as marriage or adoption) are treated the same as relatives by consanguinity (relatives who share a common biological ancestor). In determining the degree of relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

- First-degree relatives include an individual's parents, siblings and children
- Second-degree relatives include an individual's grandparents, grandchildren, uncles, aunts, nephews, nieces and half-siblings
- Third-degree relatives include an individual's great-grandparents, great-grandchildren, great-uncles/aunts, and first cousins
- Fourth-degree relatives include an individual's great-great grandparents, great-great grandchildren, and first cousins once removed (i.e. the children of the individual’s first cousins)

**Genetic Information** - Information about

1. An individual's genetic tests;
2. The genetic tests of that individual's family members;
3. The manifestation of disease or disorder in family members of the individual (family medical history);
4. An individual's request for, or receipt of, genetic services, or the participation in clinical research that includes genetic services by the individual or family member of the individual or;
5. The genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual and the genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology

Genetic information does not include information about the sex or age of the individual, the sex or age of family members, or information about the race or ethnicity of the individual or family members that is not derived from a genetic test.

**Genetic Services** - A genetic test, genetic counseling (including obtaining, interpreting or assessing genetic information) or genetic education.

**Genetic Test** - An analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder or pathological condition.

**Health Care Component** - A component or combination of components of a hybrid covered entity designated by the hybrid covered entity, which performs the functions of a health plan, health care provider, or health care clearinghouse. If a hybrid covered entity designates a health care component or components, it must include any component that would meet the definition of a covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

**Health Care Operations** - These include any of the following activities of the covered entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that “generalizable knowledge” is not the primary
purpose of any studies resulting from the activities; patient safety 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 patients with information about treatment alternatives; and related functions that do not include treatment;

2. Reviewing 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 skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that applicable legal requirements are met;

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating UMHS, including formulary development and administration, development or improvement methods of payment or coverage policies; and

6. Business management and general administrative activities of UMHS, including, but not limited to:

a) Management activities relating to implementation of and compliance with HIPAA;

b) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI 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 UMHS 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) Consistent with the applicable requirements of the HIPAA Privacy Standards, creating de-identified health information or a limited data set, and fundraising for the benefit of UMHS.

Most research activities are not included in Health Care Operations.

**Health Care Provider** - A person or organization - such as a doctor, dentist, nurse, pharmacy, dialysis center, DME provider, hospital, clinic, nursing home or ambulatory care facility - who provides clinical care, coordination, and treatment to individuals.

**Health Oversight Agency** - An agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. Health Oversight Agencies include some subcontractors and agents of public agencies. Examples of health oversight agencies include the federal Department of Health and Human Services (including CMS, OCR, FDA, and OHRP), the Michigan Department of Community Health, and the Family Independence Agency.

**Health Plan** - An HMO, insurer, or other payer that is issued, administered or serviced by the University of
Michigan.


**Individually Identifiable Health Information** - Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. See UMHS Policy 01-04-340 De-identification and Re-identification of Protected Health Information (PHI).

**Information System** - An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

**IRBMED** - The University of Michigan Medical School Institutional Review Board.

**IT Service Providers** - See UMHS Policy 01-04-500, Exhibit C: UMHS IT Service Providers.

**Limited Data Set** - Protected health information from which all of the following direct identifiers of individuals and their relatives, household members, and employers have been removed:

- Names
- All geographic subdivisions smaller than a state, except for the initial three digits of a zip code if:
  - the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and
  - the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone and fax numbers; electronic mail addresses; web addresses (URLs); Internet Protocol (IP) 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; biometric identifiers, including finger and voice prints; full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (such as a patient's initials or scrambled social security or medical record numbers)

**Manifestation (Manifested)** - With respect to a disease, disorder or pathological condition, an individual has been or could be reasonably diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. A disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.
**Marketing** - To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. See UMHS Policy 01-04-370: Marketing and Outreach Using Protected Health Information (PHI) to Target Communications.

**Minimum Necessary Standard** - A limitation placed on *uses, disclosures*, and requests for *PHI*.

**Mitigation** - The reasonable action that we would take to reduce the damage of any known wrongful use or disclosure of *PHI*.

**Notice of Privacy Practices** or NPP - The document used by the University of Michigan Health System to inform patients how UMHS uses their PHI and to inform them of their privacy rights and responsibilities under HIPAA. A current version of the University's NPP is posted on the UMHS Website at http://www.umich.edu/hipaa/npp.htm. See UMHS Policy 01-04-320 - The Notice of Privacy Practices (NPP).

**Organized Health Care Arrangement** ("OHCA") - one or more of the following:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
   
   (a) Hold themselves out to the public as participating in a clinically integrated joint arrangement; and

   (b) Participate in joint activities that include at least one of the following:

   (i) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

   (ii) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

   (iii) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

**Payment** - The activities undertaken by (1) a *health plan* to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (2) a *health care provider* or health plan to obtain or provide reimbursement for the provision of health care. These activities relate to the individual to whom health care is provided and include but are not limited to: determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographic characteristics; 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; review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and
address, date of birth, social security number, payment history, account number, and name and address of the health care provider and/or health plan.

**Payment Activities** - The activities undertaken by a *health plan* to obtain premiums or to determine or fulfill its responsibility for coverage and provision of plan benefits, as well as those activities undertaken by a *health care provider* to obtain or to provide reimbursement for the provision of health care. These include, but are not limited to, determinations of eligibility or coverage, risk adjusting amounts due based on enrollee health status and demographic characteristics, billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing, review of health care services, utilization review activities, and disclosure to consumer reporting agencies of any of the following *PHI*: name and address; date of birth; social security number; payment history; account number; and name and address of the *health care provider* and/or *health plan*.

**Physical Safeguards** - physical measures, policies, and procedures to protect a covered entity or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

**Privacy Board** - The *Privacy Board* is a committee established by the UMHS to grant waivers of authorization under HIPAA for certain research projects and to facilitate other privacy compliance activities as specified in its Standard Operating Procedures and by the Privacy Director. The Institutional Review Board may function as the Privacy Board, so long as the following are satisfied: A Privacy Board is constituted solely to review research protocols, review proposals for, and either approve or deny the waiver of HIPAA authorization, when appropriate. An IRB may also grant waivers of HIPAA authorization, but only an IRB may review research protocols as required by other laws and policies and waive or alter informed consent requirements for a research study. Privacy board members focus almost exclusively on subjects' privacy under HIPAA, whereas IRB members will focus more broadly on subjects' welfare, as the Common Rule requires. If the IRB is asked to grant a waiver under HIPAA, IRB members must separately consider privacy under HIPAA and overall welfare of the research subjects under other laws and IRB policies.

**Privacy Director** - The *Privacy Director* is the individual who is responsible for UMHS's compliance with the Privacy Rule.

**Privacy Officials** - *Privacy Officials* are individuals who coordinate the privacy compliance activities of individual departments, divisions or other units and serve as liaisons to the Privacy Director.

**Privacy Standards or Privacy Rule** - The final rule "Standards for Privacy of Individually Identifiable Health Information," published by the Department of Health and Human Services and any subsequent amendments to it. See [http://www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa).

**Protected Health Information** ("PHI") - *PHI* is individually identifiable information about a patient that:

1. is created or received by a *health care provider*;

2. relates to the past, present, or future physical or mental health of the patient; the provision of health care to the patient; or payment for the provision of health care to the patient; and

3. identifies the patient or with respect to which there is a reasonable basis to believe it could be used to identify the patient.

*PHI* excludes:

1. Individually identifiable health information of a person who has been deceased for more than 50 years.
2. Certain health information, including information in education records covered by the Family Educational Rights and Privacy Act as amended ("FERPA"); and in employment records held by the University of Michigan in its role as an employer.

**Public Health Authority** - An agency or other subdivision of a federal, state, or local government authority, or a contractor or agent of the agency that is responsible for public health matters as part of its official mandate. A public health authority can create health information as well as receive it. Examples of public health authorities include many agencies of the federal Department of Health and Human Services, such as the Centers for Disease Control and Prevention and the National Institutes of Health; the Michigan Department of Community Health; and the Washtenaw County Public Health Department.

**Research** - A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

**Safeguard Requirements of a Hybrid Covered Entity** - A hybrid covered entity must ensure that:

A. A health care component does not disclose PHI to another (non-covered) component where such disclosure would be prohibited by HIPAA if the health care component were a separate and distinct legal entity;

B. Its health care components protect electronic PHI with respect to another component of the covered entity to the same extent that it would be required by HIPAA if the health care component and the other component were separate and distinct legal entities;

C. If a person performs duties for both a health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of or incident to the member's work for the health care component in a way that would be otherwise prohibited by HIPAA.

**Sale of Protected Health Information** - A disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI. Sale of PHI does not include a disclosure of PHI for public health purposes, for research purposes where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes, for treatment and payment purposes, for the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence, to or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, to an individual, when requested under section 164.512(a) and for any other permitted purposes where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by other law.

**Sanctions** - Administrative actions taken by the University of Michigan against members of its workforce who fail to comply with our policies and procedures or with the requirements of the *Privacy Rule*.

**Security Incident** - The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

**Security Officer** - The individual who is responsible for UMHS's compliance with the *Security Rule*.

**Security Standards or Security Rule** - The final rule "Standards for Security of Individually Identifiable Health Information", published by the Department of Health and Human Services, and any subsequent amendments to it, which establishes national standards to protect individuals' electronic personal health
information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. See http://www.hhs.gov/ocr/hipaa.

**Sensitive Data** - See definition in UM SPG 601.12.

**Subcontractor** - A person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

**Treatment** - The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.

**Unsecured Protected Health Information (or Unsecured PHI)** - Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the (HHS) Secretary under section 13402(h)(2) of Public Law 111-5.

**Use** - The sharing, employment, application, utilization, examination, or analysis of PHI within the UM OHCA. See also UMHS Policy 01-04-312, "Disclosure to Family and Friends of Patients" for additional information.

**Workforce** - Our workforce includes faculty, staff, students, volunteers, trainees and other persons whose conduct is under our direct control or under the direct control of our Business Associate(s), whether or not we pay them or they are paid by the Business Associate.

**Workstation** - An electronic computing device; for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

**III. POLICY STANDARDS**

None

**IV. PROCEDURE/ACTIONS**

None

**V. EXHIBITS**

None

**VI. REFERENCES**

None

**Author:** HIPAA Implementation Team (Contact: UMHS Compliance Office, 615-4400)

**Approved by:** The Health System Executive Group, April 10, 2003; and the Associate Vice President, UMHS, February 9, 2004; October 12, 2004

**Revised by:** UMHS Compliance Office - October 11, 2004; February 25, 2010; April 29, 2011; August 15, 2014