GLOSSARY for terms used in Standards

**Abuse:** Practices that are inconsistent with sound fiscal, business or health care practices and result in unnecessary cost to state and federally funded programs. Occurs when an individual or entity unintentionally provides information to Medicare or Medicaid which results in higher payments than the individual or entity is entitled to receive. For example: providing medically unnecessary services or providing services that fail to meet professional recognized standards of care.

**Access:** The ability to use, modify or manipulate an information resource.

**Account Access Form (AAF):** The approved template used by all Data Security Administrators to provision access to Information Systems.

**Account Provisioning:** The practice of creating and managing (granting and removing) access to CWM Information Systems involving PII or financial information administered at the business unit level through a combination of a unique username and password or other authentication method.

**Aggregate Data:** Data collected from individual-level records that are combined for statistical or analytical purposes, and that are maintained in a form that should not permit the identification of individuals (note that aggregate data may include PII).

**Archive:** The Massachusetts Archives maintain valuable records of the state permanently.

**Authentication:** The process of verifying the identity of a person or system.

**Authorization:** A document signed and dated by the individual or authorized representative that permits release of specified PII to a specific entity or person for a specified purpose. A valid authorization includes all core elements required under HIPAA, 45 CFR 164.508.

**Authorization Level:** All Authorization Levels are cumulative and relate to what privilege is associated with each level, e.g. view, run reports, create and edit, delete, configure features.

**Authorized Signatory:** means a representative of the University given official permission or delegated authority from an individual with official permission under University policy to legally bind the University by signing instruments, contracts, receipts or other documents on behalf of the University.

**Best Value:** Bidder selection based not only on best price, but also on best overall benefit to the University (i.e., Bidder most qualified and capable of performing required services balanced with best economic value).

**Bidder:** The entity that submits a Response to a Solicitation.

**Breach:** The acquisition, access, use or disclosure of PII in a manner not permitted under Subpart E of 45 CFR Part 164, or Personal Information not permitted under M.G.L. c. 93 H and other applicable states’ security breach statutes, respectively, which compromises the security or privacy of such information.
Business Associate (or BA): A person or entity that is NOT a member of a Covered Entity’s workforce and that either:

1) Provides certain functions, activities, or services for or on behalf of a Covered Entity, or a Business Associate of a Covered Entity, which involves the use and/or disclosure of an individual's PII.

Examples of such activities and functions may include, but are not limited to: (a) claims processing, (b) data analysis, (c) utilization review, (d) quality assurance, (e) billing, (f) benefits management, (g) practice management, (h) re-pricing, and (i) information technology; or

2) Receives, creates or maintains PII in the course of providing the following types of services to a Covered Entity:

Examples may include: (a) legal, (b) actuarial, (c) accounting, (d) consulting, (e) data aggregation and/or storage, (f) management, (g) administrative, (h) accreditation, or (i) financial.

BAs include: (a) Health Information Organizations, E-prescribing Gateways, or other persons providing data transmission services with respect to PHI and having routine access to that PHI; (b) persons who provide personal health records to one or more individuals on behalf of a Covered Entity; and (c) subcontractors who create, receive, maintain, or transmit PHI on behalf of the BA.

Business Associate Agreement (or BAA): An agreement between a Business Associate and a HIPAA Covered Entity, or a BA and a subcontractor who creates, receives, maintains, or transmits PHI on behalf of the BA.

Business Owner: A CWM/UMMS Senior Manager responsible for the confidentiality, availability and integrity of the impacted data.

Business Unit: A center or department within Commonwealth Medicine.

Client Owner: The external party with whom UMMS maintains a contract and who provided the data to or on whose behalf UMMS collects the data.

Code of Conduct (or the Code): Outlines what we do at CWM to ensure ethical and legal compliance.

Communications Bridge (CommBridge): This is a service offered by the Massachusetts Information Technology Division that provides a standard method of messaging, provides an infrastructure that is hosted and supported by the CommBridge team at ITD, and encrypts the data over the network.

Com-PASS: Commonwealth Procurement Access and Solicitation Site.

Compliance Hotline (aka OCR Hotline): A regularly monitored phone line to confidentially or anonymously report compliance violations, legal and/or ethical issues of concern. The Compliance Hotline is 508-856-6432.
**Compliance Liaison:** A representative from a business unit who interfaces with OCR to: monitor unit compliance; serve as a single point of contact for OCR to disseminate information to the business unit; raise compliance issues with OCR; identify compliance issues; and collaborate with OCR and other liaisons on their resolution.

**Computing Device:** An electronic device such as a server, desktop or laptop, computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

**Contract:** The agreement resulting from a Solicitation executed between the selected Bidder and the University to accomplish the purposes specified in the Solicitation. The Contract shall include: the University’s Contract for Services, the Insurance Schedule, the Business Associate Agreement or the Data Management Agreement, and all other attachments and amendments to the University’s Contract for Services, including, the scope of services. If subsequent to the issuance of the Solicitation, the University amends any of the documents referenced above, the Contract may substitute the most recent version of the referenced document.

**Contractor:** The entity that enters into a Contract with the University, and includes all individuals that have a contract with the University, regardless of the site at which they work.

**Covered Entity (or CE):** Defined by HIPAA as a health plan (e.g., MassHealth); health care provider (e.g., doctor, hospital, pharmacy) that transmits health information in electronic form relating to any covered transaction under HIPAA; or health care clearinghouse (e.g., translates paper claims into electronic transactions).

**Custodian of PII:** Any department or person(s) responsible for maintaining, controlling access to, and managing release of PII that is recorded in any form or medium, paper or electronic (such as databases, spreadsheets, and/or paper files) maintained in any CWM location.

**CWM:** Commonwealth Medicine.

**CWM contracts:** means for the purpose of this standard CWM Contracts for Services Purchased using the CWM standard terms and conditions; all CWM Contracts for Services Sold; any other CWM contract or agreement requiring an Authorized Signatory including, but not limited to, Teaming Agreements, Non-Disclosure Agreements, or stand-alone Business Associate or Data Use Agreements.

**Data Management Agreement (or DMA):** Satisfactory assurances in writing between CWM and another entity, that the entity has in place adequate safeguards to protect the PII received, created or disclosed in accordance with a contract.

**Data Security Administrator (DSA):** A designated representative(s) of each CWM business unit, who is responsible for the development and monitoring of Role Based Access Controls for CWM Information Systems involving PII or financial information and provision of access to information systems administered at the business unit level.

**Data Security Manager (DSM):** The information security liaison for CWM responsible for providing direction and oversight to the DSAs to ensure appropriate development, application, and review of Role Based Access Controls.
**Data Use Agreement (or DUA):** An agreement between a CE and another entity (usually a researcher or BA) under which the CE discloses a limited data set (LDS) to the other entity. The LDS is PII from which many, but not all, of the data elements for de-identifying data have been removed. Under a DUA, the recipient of the data set agrees to limit the use of the data for the purposes for which it was given to ensure the security of the data and not to identify the information or use it to contact any individual. In addition, some agencies that are not CEs refer to agreements by which they share identifiable data as a “Data Use Agreement.” Such agreements are not always limited to identifiers permitted under HIPAA as LDS.

**De-identified PII:** PII that cannot be used to identify an individual because all of the 18 HIPAA identifiers referenced in 45 CFR 164.514(b)(2) have been removed, and there is no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

**Designated Data Access Administrator:** The data access administrator is the individual designated by a business unit to authorize and document role-based access for its workforce members. The data access administrator is the liaison to UMMS IS for the approval and coordination of access to the business unit’s data, systems and files.

**Disclosure:** The release or transfer of, provision of access to, dissemination of, or communication of PII to anyone outside of CWM.

**Discovers:** Shall mean the first day on which a Breach or Security Incident is known to Contractor (including any person, other than the individual committing the Breach, that is an employee, officer, or other agent of Contractor), or should reasonably have been known to Contractor, to have occurred.

**Disposal:** Destruction or disposal of documents with permission of University or Massachusetts Records Conservation Board. If the data are PII, destruction is in accordance with the secure destruction methods required by the University or data owner.

**Electronic Media:** Electronic storage material including memory devices in computers (hard drives) and any removable/transportable digital member medium, such as magnetic tape or disk, optical disk, or digital memory card. Electronic Media also includes transmission media used to exchange information already in electronic storage media, such as the internet.

**Electronic signature:** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature. For purposes of this standard, electronic signature is a certificate-based electronic signature.

**Encryption:** The use of a technical (algorithmic) process to transform electronic data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Valid encryption standards must comply with the defined NIST (National Institute of Standards and Technology) standards for data in motion and data in rest required to meet the HIPAA safe harbor protections under the breach notification rule. [http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html)

**ePII:** Electronic Personally-Identifiable Information.
**False Claims:** Intentionally submitting false information to the government or a government contractor in order to get money or a benefit.

**Federal Health Care Program:** is defined as any plan or program that provides health benefits, whether directly, through insurance, or otherwise, which is funded directly, in whole or in part, by the United States Government or a State health care program (with the exception of the Federal Employees Health Benefits Program). The most significant Federal Health Care Programs are Medicare, Medicaid, Tricare and the Veterans program.

**Fraud:** An intentional deception or misrepresentation that the individual knows to be false or does not believe to be true and that the individual makes knowing that the deception could result in some unauthorized benefit to himself/herself or to some other person. For example: billing for services not furnished.

**GSA System For Award Management** (also referred to as SAM): The United States General Services Administration maintains a list of parties that are debarred from Federal Procurement and Non-procurement Programs. This list includes parties that are debarred from receiving federal contracts, certain subcontracts and certain types of federal financial and non-financial assistance and benefits. These are commonly known as “Suspensions” and “Debarments”. They can be found on the GSA website at [http://www.sam.gov](http://www.sam.gov).

**Health care operations:** Certain administrative, financial, legal, and quality improvement activities of a CE, which are necessary to run its business and to support the core functions of treatment and payment (for example, quality assessment and improvement activities, training, credentialing, auditing, certification activities).

**HIPAA:** *Health Insurance Portability and Accountability Act of 1996* -- HIPAA is the federal law that establishes standards for the privacy and security of health information, as well as standards for electronic data interchange (EDI) of health information. HIPAA, as implemented, has four health information standards, and four associated sets of regulations or "rules": (1) Privacy; (2) Security; (3) Identifiers; and, (4) Transactions and Code Sets.

**HIPAA Rules:** The Omnibus HIPAA/HITECH Regulations that are the final modification to the HIPAA Privacy, Security, Breach and Enforcement Rules mandated under the HITECH Act, effective March 26, 2013.

**HITECH:** *Health Information Technology for Economic and Clinical Health Act* -- HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). HITECH imposes the HIPAA Security Rule and most of the Privacy Rule directly upon Business Associates of Covered Entities. Prior to HITECH, Business Associate obligations were imposed by contract with the Covered Entity. HITECH extends increased civil and criminal penalties to Business Associates. HITECH imposes consumer notification requirements on CEs and Business Associates if a breach of unsecured protected health information occurs. The data owner is responsible for determining when consumer notification is required.

**Human Resources (or HR):** UMMS and CWM HR department, as applicable.

**Individual:** The person who is the subject of the PII.
Individual Exercising Budgetary Control (referenced as Budgetary Control): means a representative of the business unit exercising managerial and budgetary control for the contract, who signs the contract in this capacity but who is not authorized to legally bind the University.

Individually Identifiable Health Information (IIHI): Information relating to an individual, including demographic information, that relates to past, present, or future physical or mental health of an individual; the provision of health care to an individual; or the past, present, or future payment for such health care services and which identifies the individual or there is a reasonable basis to believe the information can identify the individual.

Information Systems: All CWM applications, information assets, databases, financial systems and IT resources involving PII or financial information, which are administered at the business unit level.

ISA: Interdepartmental Services Agreement.


IT: Information Technology.

Least Privilege: The practice of limiting access to CWM Information Systems to the lowest level of user rights absolutely essential for the completion of assigned duties or functions.

Legal Hold: A directive issued typically by the University Office of General Counsel or the Massachusetts Attorney General to retain certain records for which an investigation, litigation, or other legal action has been, or may be, filed against the University or a client of the University on whose behalf CWM is the custodian of the records.

Legal Process: The formal notice, subpoena, court order or similar administrative document used by a court to exercise jurisdiction over a person or property.

Limited Data Set (or LDS): A data set that excludes specific direct identifiers related to the individual, his or her relatives, employers or household members, which may be disclosed for public health, operations, or research purposes, at the discretion of a CE, without an authorization from the individual, provided that a Data Use Agreement is executed. A LDS may include: dates (birth, death, service) and geographic designations (town or city, state, zip code), but may not include any other of the HIPAA identifiers. (see, 45 CFR §164.514(e)(2))

Massachusetts General Law 93 H (or M.G.L. 93 H): The Massachusetts security breach and notification law, which applies when UMMS CWM holds data identifying a resident of the Commonwealth by first and last name, or first initial and last name, in combination with one or more of the following: Social Security Number; driver’s license number; state-identification card number; financial account number or credit or debit card number. https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section1

MassIT: Massachusetts Office of Information Technology (previously known as ITD).

MHEC: Massachusetts Higher Learning Consortium.
Minimum Necessary Standard:  Policy governing the least amount of PII needed for an authorized Workforce member to accomplish the business objective (i.e., to complete her/his job). A BA must apply the standard when using or disclosing PII or when requesting PI from a CE or another BA.

Minimum Necessary:  The amount of PII that is the minimum necessary to accomplish the intended business purpose specified in the applicable contract or agreement.

OCR:  Office of Compliance and Review.


OIG List of Excluded Individuals/Entities (also referred to as LEIE):  The Office of Inspector General of the US Department of Health and Human Service is authorized under §1128 of the Social Security Act to exclude individuals and entities from federally-funded health care programs and maintains a list of all currently excluded individuals and entities on a list called the List of Excluded Individuals and Entities (LEIE). No payment from any federal health care program may be made for services provided by an individual or entity that was excluded. The data base can be found on the OIG’s website at http://oig.hhs.gov/exclusions/index.asp Individuals or Entities verified as included on the OIG list are known as “Excluded Individuals” or “Excluded Entities”.

OSD:  Massachusetts Operational Services Division.

Personal Representative:  A person authorized under state law to act on behalf of an individual. Certain information may be collected from, or disclosures may be made to, Personal Representatives if they are so authorized under Massachusetts law.

- Personally-Identifiable Information (or PII):  Any information that can be used to uniquely identify an individual, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical (PHI), educational, financial (PI), and employment information. CWM must not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

- CWM programs should assume all client information relates to an individual’s health care when carrying out business operations and that it is PII, unless stated otherwise.

Privacy Rule:  The Privacy Rule, 45 CFR 164.000, was promulgated by HHS, as required by HIPAA, and became effective on April 14, 2003. The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI) held by Covered Entities and pursuant to HITECH, many provisions are applicable to their business associates.

Protected Health Information (or PHI):  Individually identifiable health information as defined by HIPAA, maintained or transmitted by a CE, its BAs acting for the CE, or by a Subcontractor of a BA, which is maintained or transmitted in any form or medium. This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual
that is created or received by a health care provider, health plan, employer, or health care clearinghouse.

- Identifiers include:
  (A) Names;
  (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
     1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
     2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
  (C) 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;
  (D) Telephone numbers;
  (E) Fax numbers;
  (F) Electronic mail addresses;
  (G) Social security numbers;
  (H) Medical record numbers;
  (I) Health plan beneficiary numbers;
  (J) Account numbers;
  (K) Certificate/license numbers;
  (L) Vehicle identifiers and serial numbers, including license plate numbers;
  (M) Device identifiers and serial numbers;
  (N) Web Universal Resource Locators (URLs);
  (O) Internet Protocol (IP) address numbers;
  (P) Biometric identifiers, including finger and voice prints;
  (Q) Full face photographic images and any comparable images; and
  (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section;

This term is defined under HIPAA; however, since CWM also works for entities that are not CEs under HIPAA, the CWM standards shall refer to PHI as “PII” throughout to avoid multiple terms.

**Provision/De-Provision:** The creation, maintenance and deactivation of user accounts to permit authorized access to Information Systems.

**PSI:** Permission to Share Information is the authorization form used by MassHealth.

**Qualified Vendor List:** A list of Bidders that have submitted an application to the University in response to a Request for Applications, and that meet the standards outlined in the RFA.

**Recertification:** The twice annual review by each DSA of user accounts, roles and Authorization Levels to ensure that Access controls are accurate and up to date.

**Record:** Information recorded or captured on paper, audio or video tape, photographic media, computer or other digital media, including e-mail.
**Records Custodian:** The individual in each business unit who is responsible for implementing the Records Management Standard.

**Records Conservation Board (or RCB):** The Massachusetts state board charged with the approval of the Statewide Retention Schedule, and permission to destroy or transfer state agency records, but not University records.

**Report:** A written or verbal statement or account made to a CWM supervisor, the Compliance Hotline, the Office of Compliance and Review, any appropriate CWM Business Unit manager, or any appropriate governmental agency involving known or suspected violations or breaches of the Rules.

**Request for Applications (also RFA):** A document used to solicit competitive applications from qualified Bidders for participation in a particular University project and/or to be added to a Qualified Vendor List.

**Request for Information (also RFI):** A document used to seek information and/or input from interested parties on a particular subject matter or University project.

**Request for Proposals (also RFP):** See “Request for Responses (also RFR)”.

**Request for Responses (also RFR):** A document used to solicit competitive Responses from qualified Bidders interested in providing services or goods to the University.

**Response (or Proposal):** A Bidder’s response to a Solicitation issued by the University.

**Retention Schedule:** A Business Unit’s requirement for document retention and destruction.

**Role Based Access Control (RBAC):** The process of granting, restricting, or denying requests based on job function for system Access to prevent unauthorized Access to IT systems.

**Rules:** All applicable laws, regulations, and University and CWM policies, procedures and standards.

**Security Incident:** A verified external or internal attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**Separation of Duties (SOD):** The practice of ensuring that no one person is responsible for completing or controlling a task or set of tasks from beginning to end when it involves the potential for fraud, abuse, system compromise or other harm and disseminating such tasks among multiple individuals to prevent such fraud, abuse or harm.

**SIRT:** SIRT shall mean the Security Incident Response Team authorized under the Information Security Incident Response Team Policy.

**Sole Source (or Sole Acceptable Source/Brand):** Means that the product/service is unique and that the vendor is the only known source (worldwide) from whom the product/service can be purchased. In addition, similar types of products/services may exist, but the vendor/brand, for reasons of expertise, and/or standardization, quality, compatibility with existing equipment,
specifications, or availability, is the only source/brand that is acceptable to the requester or the University. In order to use a Sole Source, the purchaser must provide sufficient justification.

**Solicitation:** Any document used for soliciting competitive Responses from qualified Bidders interested in providing services or goods to the University (such as a “Request for Responses”).

**SSN:** Social Security Number.

**Statewide Retention Schedule:** The schedule that establishes applicable retention periods for all types of records of Massachusetts state agencies, wherever those records are found, and in whatever format. The retention period reflects a minimum retention period, after which a request for destruction of documents must be submitted to and approved by the RCB. The University references this schedule for guidance to develop University retention schedules, but is not bound by the schedule’s retention periods or the RCB requirements to seek approval for destruction.

**Subcontractor:** A person or entity to whom a BA has delegated a function, activity, or service the BA has agreed to perform for a Covered Entity in which the Subcontractor creates, receives, maintains, or transmits PHI. Subcontractors of a BA are also classified as Bas, and subject to applicable HIPAA requirements.

**Training Plan:** A plan implemented by OCR to disseminate Privacy and Security Training to the CWM Workforce.

**UMMS:** The University of Massachusetts Medical School.

**University:** The University of Massachusetts, which includes the University of Massachusetts Medical School.

**Unsecured PHI or PII:** PHI or PII that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human Services] (e.g., encryption).

**Use:** With respect to PII, any activity or function within CWM that involves the sharing, employment, application, utilization, examination, or analysis of PII necessary to provide services under any contract with a Covered Entity client.

**Waste:** The over or under utilization of services and/or inefficient use of resources that directly or indirectly result in unnecessary costs. Generally waste is not considered to be caused by criminally negligent actions but rather a misuse of resources.

**Workforce:** All CWM employees (including full time, part time, long-term temporary, and probationary employees), interns, volunteers, students, and other persons whose conduct, in the performance of work for CWM, is under the direct control of CWM, whether or not the individual is paid by CWM.