Name of Standard: Use and Disclosure of PII

Responsible Department
UMMS Office of Management (OoM)
OoM Contact: PrivacyandCompliance@umassmed.edu or 508-856-TEAM

STANDARD STATEMENT

Commonwealth Medicine (CWM) is committed to protecting the privacy and security of Personally Identifiable Information (PII) that it creates, receives, uses, discloses, stores, or has access to pursuant to client contracts and to comply with federal and state laws mandating such protections. Workforce will make all reasonable efforts to safeguard the PII they receive or maintain on behalf of clients, including limiting the use and disclosure of PII to the minimum necessary to accomplish the intended purpose, and not using the PII for any purpose other than that which is authorized. CWM shall establish standards relating to use and disclosure of PII, that Workforce who use or may come into contact with PII in their job duties must follow.

REASON FOR STANDARD

CWM is committed to complying with state and federal laws applicable to its business activities including applicable provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 42 CFR Part 2, and all regulations established pursuant to these statutes. This Standard provides guidance for CWM Workforce creating, receiving, using, disclosing, requesting, storing, transmitting or disposing of PII from a HIPAA Covered Entity (CE), Business Associate (BA), or other client.

ENTITIES AFFECTED BY THIS STANDARD

- All Workforce
- All Business Units within CWM

RELATED DOCUMENTS

- CWM Access Control
- Business Associate Agreement Standard
- Data Management Agreement Standard
- Verification of Identity Standard

DEFINITIONS: (See GLOSSARY on Office of Management (OoM) website for additional definitions)

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.

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

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).

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.

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

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)).

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.

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.

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.

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 CE client.

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.

SCOPE

This Standard applies to all CWM Business Units and Workforce who handle or come into contact with PII, regardless of whether it is within the scope of their duties.

STANDARDS (Procedures)

PII received from a CE, BA, or other client, or created on its behalf, may only be used or disclosed for the purposes described in the relevant Business Associate Agreement (BAA), Data Management Agreement (DMA), Data Use Agreement (DUA), or other contract or agreement or as required by law; provided that such use and disclosure does not violate HIPAA or other privacy laws.

Workforce may use PII only for the purposes for which the information is received or created. PII which is collected or provided to CWM for one contracted purpose may not be used for a new or different purpose, unless a new or amended agreement is executed.

CWM Business units shall follow the procedures described in this standard and incorporate them into their Business Unit-specific procedures. Business Unit-specific procedures may be more restrictive, but not less restrictive, than the procedures set forth herein.

Anyone found in violation of this standard may be subject to disciplinary action up to and including termination.

PROCEDURES:

A. General Rules Regarding Use and Disclosure of PII
B. Minimum Necessary
C. De-identification
D. Limited Data Sets
E. Work Practices
- Exhibit A: Transmission of PII
  - Attachment 1: Email
  - Attachment 2: Faxing
  - Attachment 3: Electronic Data Interchange (EDI), Secure File Transfer Protocol (SFTP), or other Third-Party Secure Document Service
  - Attachment 4: Phone Messages
  - Attachment 5: Commercial Courier or the United States Postal Service
- Exhibit B: Management and Disposition of PII
  - Attachment 1: Electronic Storage of PII
  - Attachment 2: Paper Management and Storage of PII
  - Attachment 3: Disposal of PII
- Exhibit C: Out of Office Use of PII

F. Individual Rights Regarding PII
G. Disclosures in Response to a Subpoena or Court Order

A. General Rules Regarding Use and Disclosure of PII

1. Workforce shall:
   a. Use or disclose PII only if authorized by your Business Unit procedures, and:
      i. as permitted or required by Business Unit's BAA or Contract;
      ii. as required by law; or,

iii. to HHS to investigate or determine compliance.

b. Not use or disclose PII in a manner that violates the Privacy Rule if done by the CE.
c. Only disclose PII directly in response to an individual owner's request or a valid Authorization if permitted by Business Unit's procedures.

2. Each Business Unit shall be responsible for:
   a. Determining which members of its Workforce shall be authorized to access PII to carry out their job responsibilities.
   b. Implementing Business Unit procedures that document disclosures made on a routine and recurring basis and which limit the PII disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure.
   c. Implementing Business Unit procedures for the review of non-routine disclosures.
   d. Executing the appropriate agreement (e.g., BAA, DMA, DUA or other agreement) prior to disclosing PII to a non-Workforce individual or subcontracted entity working with CWM:
      i. Subcontractor must be authorized to access PII by CE or Client.
      ii. All terms required by CE under the BAA with CWM must be included in the BAA with the subcontractor.
   e. Maintaining appropriate and complete documentation of all disclosures as described in Section F.5 on accounting of disclosures.

3. Workforce who are authorized to use or disclose PII on behalf of a CE client may only share the PII with other Workforce who are authorized to access the PII under that contract. PII collected or provided for a specific contract may not otherwise be shared within CWM, unless accompanied by an authorization or written data sharing agreement with the client.

4. Refer to Business Unit procedures or contact OoM for assistance on how to handle specific requests for disclosure. These may include:
   a. Required by law requests from oversight agencies;
   b. Personal representative, attorney, or other third-party requests with an authorizations/Permission to Share Information (PSI) form;
   c. Payment or health care operations-related activities;
   d. Other non-routine requests; or
   e. Subpoenas or Court Orders as more fully described below in Section E.
   f. Requests for Substance Use Data

5. Refer all external or third-party notices of Audit, Oversight, or Inspection involving PII to the Director of Finance – CWM, UMMS Financial Services (Controller) and OoM.

B. Minimum Necessary

1. Workforce, when using, disclosing or requesting PII, must make reasonable efforts to limit PII to the minimum necessary to accomplish the intended business purpose specified in the applicable agreement. Workforce shall:
   a. Use only that PII which is reasonably necessary to accomplish the intended business purpose;
   b. Restrict access, through role-based CWM Access Controls, to only those Workforce requiring access to perform their role;
   c. Only access PII when necessary to perform the job;
   d. Not attempt to access PII unless authorized;
   e. Not print or copy PII unless necessary to perform job functions;
   f. Not remove PII from the workplace unless authorized by supervisor; and,

g. Only share PII with individuals who are also authorized to access PII to perform job duties.

2. Workforce shall not collect, use or disclose Social Security Numbers (SSN), driver's license numbers, state-issued identification card numbers, or financial account or credit or debit card numbers if not necessary to accomplish the intended purpose specified in the applicable contract or agreement. If a SSN is necessary, limit the collection to the last four digits if this will serve the intended purpose.
3. When leaving a phone message for an individual, don't include PII (see, Exhibit A-4).
4. Workforce shall use and disclose de-identified information whenever possible. There may be restrictions in the release of de-identified information depending upon the project. (see, Subsection C, De-identification below).
5. If de-identified information is insufficient to accomplish the intended purpose, Workforce shall, whenever possible, use a Limited Data Set (LDS) (see, Subsection D, Limited Data Set below) without direct identifiers.
6. Exceptions to the Minimum Necessary Standard include disclosure to a healthcare provider for treatment, to the individual or authorized representative, with a valid authorization, to the U.S. Department of Health and Human Services (HHS) for HIPAA compliance or when required by law.
7. Business Units shall establish a procedure to respond to the receipt of PII in excess of the Minimum Necessary. At a minimum, such procedure should address informing the disclosing party of the excess PII and working with the party to return or destroy the excess PII and to prevent a recurrence.

C. De-identification:

1. Health information de-identified according to HIPAA standards is not subject to the same restrictions on use and disclosure as PII. Whenever possible, de-identified information should be used.
2. PII is rendered not identifiable when all of the following identifiers are removed:
   a. Names;
   b. Geographic subdivisions smaller than a State, including street address, city, county and zip code;
   c. All elements of dates, except the year;
   d. Telephone numbers;
   e. Fax numbers;
   f. E-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 plates;
   m. Device identifiers and serial numbers;
   n. URLs;
   o. IP addresses;
   p. Biometric identifiers;
   q. Full face photographic images and other comparable images;

r. Any other unique identifying number, characteristic, or code[1]; and,
s. There is no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

3. Check the BAA, DMA, DUA or other similar contracts for restrictions that may limit the disclosure of de-identified information if it is derived from PII.

D. Limited Data Set:

CWM may be the recipient of a limited data set (LDS) from a CE or CWM may, as a BA, create an LDS on behalf of a CE for research, public health, and health care operations.

1. An LDS includes individually identifiable data in which the CE may disclose:
   a. Dates such as admission, discharge, service, date of birth and date of death,
   b. City, state, five digit or more zip codes, or
   c. Ages in years, months or days or hours.
2. When creating an LDS for a CE, Workforce may not disclose the following direct identifiers in a LDS:
   a. Names,
   b. Postal Address information, other than town, city, state, and zip codes,
   c. Telephone numbers,
   d. Fax numbers,
   e. Social Security numbers,
   f. Medical records numbers,
   g. Health plan beneficiary numbers,
   h. Account numbers,
   i. Certificate/license numbers,
   j. Vehicle identifiers and serial numbers, including license plates,
   k. Device identifiers and serial numbers,
   l. URLs,
   m. IP addresses,
   n. Biometric identifiers, or
   o. Full face photos or comparable images.
3. A DUA must accompany an LDS, since it contains PII. A DUA must:
   a. Establish the permitted uses and disclosures of the LDS,
   b. Identify who may use or receive the information,
   c. Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or by law,
   d. Require the recipient to use appropriate safeguards to prevent any use or disclosure that is not permitted by the agreement,
   e. Require the recipient to ensure that any agents, including a subcontractor, to whom it provides the information will agree to the same restrictions as provided in the DUA, and,
   f. Prohibit the recipient from identifying the information or contacting the individuals.

[1] A code may be assigned to allow information de-identified to be re-identified provided that the code or other means or record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual and the key or cross-walk is not disclosed and is securely maintained.

E. Disclosures Pursuant to a Subpoena or Court Order:

1. For routine subpoenas, Business Units shall establish a Business Unit procedure with the CWM client, that owns the requested information (for example, Medicaid Appeals):
   a. Supervisor shall establish unit-specific procedures for notifying CWM client of subpoenas received.
   b. If the document names a CWM client (e.g., MassHealth) the supervisor shall notify the client contact according to the unit-specific procedures.
   c. Disclose PII in response to a subpoena only if directed by applicable client (and document disclosure).
   d. Document a copy of the subpoena and the notification of the client contact.
2. Workforce shall:
   a. Immediately report the receipt of any subpoena, court order, or similar administrative or legal process (legal process) to supervisor that is not part of Business Unit routine process.
   b. Supervisor shall notify OoM and OoM shall forward the subpoena or other legal process to the appropriate legal division (for example, UMass Office of General Counsel; EOHHS Privacy Office).
3. For all subpoenas to which CWM responds, supervisor, in conjunction with OoM shall:
   a. Determine if the subpoena seeks PII subject to HIPAA and/or FIPA (Massachusetts' Fair Information Practices Act) or whether the information is a public record.
   b. Ensure that none of the requested information is subject to 42 CFR Part 2. No patient information subject to 42 CFR Part 2 may be released pursuant to a subpoena without a court order authorizing the disclosure issued pursuant to the regulations. (Check with OoM.)
   c. Determine if the subpoena includes an appropriate authorization from the individual. If it includes a compliant authorization, the information may be released.
   d. Determine if the subpoena seeks documents that contain PII but for which there is no authorization. If so, OoM shall review the request as necessary with the OGC for the appropriate response under HIPAA, FIPA, or other states' laws.
      i. Under HIPAA, a CE may release information pursuant to a subpoena that is not authorized or accompanied by a court order if it receives a "satisfactory assurance" in compliance with 45 CFR §164.512(e)(1)(iii) or (iv).
      ii. Documentation of a satisfactory assurance must include:
         a) A demonstration of a good faith attempt to provide written notice to the individual subject, proof of mailing including the date of mailing (certificate of mailing or certified mailing receipt) to the individual, and
         b) A sufficient time has elapsed and any objections resolved or a qualified protective order is submitted to the court.
   e. Ensure that the HIPAA standard is followed when the subpoena is issued to a HIPAA CE or to UMMS in its capacity as a BAA.
   f. Review for FIPA includes a more restrictive standard than HIPAA, requiring the data subject's authorization or a court order, with notice to the data subject before UMMS may release information pursuant to a subpoena. The FIPA standard must be followed when responding to subpoenas issued to a MA state agency or to UMMS where UMMS is a holder of the data on the agency's behalf.
4. For all court orders to which CWM responds:
   a. Refer all court orders to OoM for review as necessary with the OGC.

b. In response to a court order seeking HIPAA identifiable information, UMMS may, with the approval of the CE, disclose only the PHI expressly authorized by the order.

c. If the court order contains personal data as defined by FIPA, with the approval of the state agency client, notice of the court order and request for the personal data shall be sent to the data subject as soon as possible with an authorization form to allow for the release of the data. The letter shall provide the individual fourteen days to respond unless the return date in court is earlier. The letter shall indicate that after the date established in the letter, that UMMS will release the requested information in compliance with the court order.

F. Individual Rights Regarding PII:

HIPAA provides the individual whose data is held with certain rights. For the most part, CWM holds data as a BA, and must respond to requests from individuals through the CE. In some instances, CWM may be authorized by the CE to respond directly and provide documents to the individual. CWM shall respond to the CE or the individual, as directed, with respect to the following:

1. **Right to access PII**: This right includes both the right to inspect or obtain a copy of the PII about the individual in a designated record set (DRS).
   a. A DRS is a group of records maintained by or for the CE that is:
      i. Medical records and billing records about individuals maintained by or for a covered health care provider;
      ii. Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
      iii. Used, in whole or in part, by or for the CE to make decisions about individuals.

   b. A DRS excludes:
      i. Psychotherapy notes;
      ii. Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

   c. Reasonable steps must be taken to verify the identity of an individual making a request for access.

   d. Access must be provided, pursuant to 45 CFR §164.524, in the form and format requested, if it can be readily produced. If not, it must be produced in a readable hard copy form, or other form and format mutually agreed upon with the individual.
      i. If electronic copies are requested, the individual must be provided access in the requested electronic format if it is readily producible, even if records are in hard copy.
      ii. Response to requests for access must be provided no later than 30 days after request is made to CE, unless the CE extends the time by 30 days.
      iii. A summary of PII may be provided in lieu of, or in addition to, providing access to the information, or an explanation of the PII may be provided, if the individual agrees in advance to the summary or explanation and to any fees imposed.
      iv. A reasonable cost-based fee may be imposed to access PII provided that it includes only the cost of: (1) labor for copying the PII requested; (2) supplies for creating the paper copy or electronic media (e.g. CD or USB drive); (3) postage, if mailed; and (4) preparation of an explanation or summary of the PII as agreed to by individual. The fee may not include costs associated with verification, documentation, searching for and

retrieving the PII, maintaining systems, recouping capital for data access, storage, or infrastructure, or other costs even if such costs are authorized by state law.

v. No costs may be imposed on individuals to inspect their PII.

2. **Amendment of PII**: CEs must permit an individual to request an amendment of the PII in the DRS as provided for in 45 CFR § 164.526. If the DRS is held by CWM as a BA, the CE will forward the request to CWM, which must act as directed by the CE. If CWM receives the request directly from the individual to amend the DRS it holds, it shall act as required in the BAA.
   a. The individual may be required to make the request in writing and to provide a reason to support the requested amendment, provided the CE informs individuals in advance.
   b. The request for amendment must be acted upon within 60 days of the request.
3. **Request of Restrictions on Use and Disclosure of PII:** CEs are required by 45 CFR §164.522 to permit an individual to request that the CE restrict uses and disclosures about the individual with respect to treatment, payment, health care operations and disclosures permitted under 45 CFR § 164.510(b) (disclosures to family members and friends directly involved in the individual's care).
   a. If the CE agrees to restrictions and informs CWM of this restriction, CWM shall comply with the restriction(s) for as long as it remains in effect.
   b. If the request for a restriction is received directly from an individual, CWM shall confer with the CE unless otherwise stated in the BAA.
4. **Confidential Communications**: An individual's request for confidential communication submitted to a CE provider or plan may be forwarded to CWM as its BAA, if applicable to the contracted work.
   a. If the Business Unit receives a request for confidential communication from the CE, it must ensure that it notes the change in communication in all appropriate records.
   b. If the Business Unit receives a request for confidential communication from the individual it shall confer with the CE and take such steps as the CE directs.
5. **Accounting of Disclosures**: Individuals have a right to learn to whom the CE has disclosed their PII for up to six years prior to the date of any request. Such requests include disclosures made to or by the BA. In response to a request from a CE or as required under the BAA, the Business Unit shall provide a log of disclosures. The Business Unit shall:
   a. Maintain a log of disclosures for which HIPAA requires the CE to provide an accounting, to the extent that CWM directly discloses PII on behalf of a CE client, including all disclosures except:
      i. To the individual or his or her personal representative;
      ii. Pursuant to an authorization;
      iii. Related to treatment, payment, and operations;
      iv. Pursuant to national security or intelligence purposes;
      v. To correctional institutions or law enforcement officials as permitted under law;
      vi. Those that are "incident to a disclosure" that is otherwise not required to be included in the accounting;
      vii. As part of an LDS;

viii. To persons involved in the individual's care as provided for in 45 CFR §164.510.

b. The accounting must include for each disclosure:
   i. Date of disclosure;
   ii. Name of entity or person who received the PII and, if known, the address;
   iii. Brief description of the PII disclosed; and
   iv. Brief description of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

c. Multiple disclosures to the same entity or person for a single purpose may be summarized by including:
   i. The first and last dates of the series of disclosures;
   ii. The frequency or number of disclosures; and
   iii. Items ii-iv listed in subparagraph b, directly above.

d. Create a Business Unit procedure to ensure the required accounting is maintained and provided upon request to the CE for those Business Units that disclose PII directly.

RESPONSIBILITIES

At a minimum:

Business Unit Head/Program Director/Supervisor shall:

- Ensure the development, dissemination, and monitoring of Business Unit procedures as necessary to implement this standard.
- Ensure appropriate documentation to support unit-specific procedures is in place.
- Establish appropriate role-based access in conjunction with the Data Security Manager and Data Security Administrator and consistent with CWM Privacy and Security Standards.
- Limit removal of PII from workplace, and authorize, only as necessary, those members permitted to remove PII.
- Establish standards for protecting PII, if it is authorized to be removed from workplace.
- Compete an inventory of all PII maintained by the Business Unit and update annually.
- Ensure appropriate BA or DMAs are executed with contractors.
- Report to OoM any unauthorized use or disclosures.
- Ensure appropriate training of Workforce on Business Unit procedures.

Workforce shall:

- Attend HIPAA Privacy and Security Training, prior to accessing any PII.
- Follow Business Unit use and disclosure procedures.
- Access only the Minimum Necessary PII to complete work according to assigned security role.
- Use de-identified data to the extent possible.
- Access only PII to which the Workforce member is authorized for the specified task.
- Not share PII, unless authorized by supervisor.
- Observe all workstation security requirements.
- Report to supervisor all requests for disclosure of PII, unless otherwise directed by Business Unit procedures.
- Not remove PII from workplace unless authorized by supervisor.
- If authorized to work with PII off-site, follow all off-site standards.
- Report to manager or OoM if aware of unauthorized use or disclosure.

OoM shall:

- Respond to all inquiries regarding use and disclosure.
- Assist with the development of unit-specific procedures, as requested.
- Coordinate requests for data access from state agencies, and review DMA and BAAs.
- Serve as the point of contact with clients for subpoenas and court or administrative agency orders, where no unit-specific protocol is established.
- Evaluate reports of unauthorized use or disclosures of PII.

DOCUMENT HISTORY

Effective Date: 10/1/11
Revision Date(s) 09/23/13; 06/01/16, 5/5/17; 12/31/19
Review Date(s): 12/1/18

APPROVAL

June Sullivan

June Sullivan
Senior Director of Compliance and Privacy
Office of Management

Exhibit A

PROCEDURES FOR TRANSMISSION OF PII

- Before mailing, emailing, faxing or otherwise transmitting PII, Workforce must be certain that the disclosure of PII to the intended recipient is a permitted and authorized disclosure. If uncertain, check with your supervisor or OoM.

- Confirm the method of transmission is permitted for the particular job function and follow specific Business Unit procedures. Electronic PII in transit must be encrypted in accordance with UMMS IT policies.

- Evaluate the need to transmit PII and if necessary to transmit, follow minimum necessary rules. Use secure, restricted shared files for transferring or sharing PII within Business Units instead of email.

- Contact the UMMS IT Helpdesk for information on methods other than email for the secure transmission of PII.

- Do not transmit Social Security numbers or other high-risk identifiers that could lead to medical identity or financial fraud unless a supervisor explicitly determines it is necessary for business purposes.

For specific guidelines, see the following attachments to Exhibit A:

A-1: Email
A-2: Faxing
A-3: Electronic Data Interchange (EDI), Secure File Transfer Protocol (SFTP), or other Third-Party Secure Document Service
A-4: Phone Messages
A-5: Commercial Courier or the United States Postal Service

Exhibit A-1

EMAIL

When emailing PII, Workforce shall:

a. Confirm the email method is secure.
    i. If the email is both to and from an email address that ends in "umassmed.edu", ".state.ma.us" or "umassmemorial.org" the email is secure.
    ii. If the University has a "TLS" [Transport Layer Security] relationship with another organization's email, the email is secure. Check the IT website for a list of current TLS Domains.
    iii. Otherwise, type SECURE in the subject line of the email, and the email will be encrypted. This engages the UMMS secure email system – Office 365 Message Encryption. Office 365 Message Encryption Instructions

b. Not forward or reply to email messages that include PII or attachments with PII except in accordance with minimum necessary rules and utilizing secure processes.
c. Not auto forward email from an umassmed.edu address to any outside email address.
d. For recurring transfers of data between parties or large files contact UMMS IT to discuss other solutions including TLS or secure FTP rather than email.

e. Follow all best practices when emailing PII:
    i. Never include any PII in the subject line of the email. The subject line is not encrypted.
    ii. Before emailing, verify address by sending a test email message and requesting a response.
    iii. Double-check email address before hitting send to verify the selected recipient is correct as email programs that automatically populate the address field often select addressees other than the intended email recipient.
    iv. Use prepared contact lists whenever possible to avoid errors.
    v. Use the following or similar language as a Header or Footer "Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender immediately and destroy or permanently delete all copies of the original message."
    vi. Do not open emails containing PII in public areas.

Exhibit A-2

FAXING

When faxing PII, Workforce shall:

a. Call to let the recipient know a fax containing PII will be sent and to confirm the fax number.
b. Request that recipient attend the fax machine until fax transmission is complete unless the receiving machine is in a locked limited-access location or a desktop application.
c. Request that the recipient confirm receipt of fax.
d. Use a fax cover sheet that clearly identifies who is sending the fax with the business unit contact information including individual to contact and phone number.
   Include a confidentiality notice on the fax cover sheet. Use the following or similar language: *This communication is intended only for the person or entity to which it is addressed. It may include confidential, proprietary and privileged information. If you are not the intended recipient, any dissemination or sharing of this communication is strictly prohibited. If you received this communication in error, please contact the sender immediately and shred all copies of the original message and permanently delete it from the system, if applicable.*
e. Use pre-programmed buttons to enter the recipient's fax number, for regular faxes.
f. After entering the fax number, visually check the fax number before pressing send.
g. Make sure the fax confirmation option is activated. Verify transmission with fax activity confirmation sheet.
h. Remain at machine until transmission is complete. Do not leave faxes containing PII unattended.
i. If transmission cannot be completed, remove all documents containing PII from vicinity of machine and call recipient to inform him/her of the problem.
j. If transmission is completed, remove all documents containing PII from the fax machine, confirm receipt with recipient, and retain fax activity confirmation with original documents.
k. If recipient does not confirm within a reasonable period, contact recipient.

Exhibit A-3

SECURE FILE TRANSFER PROTOCOL (SFTP) OR OTHER THIRD-PARTY SECURE DOCUMENT DELIVERY SERVICE

a. SFTP and other secure third-party document delivery services may be used to transmit PII.

b. Workforce should consult with UMMS IT for further instructions on these methods of transmission.

Exhibit A-4

PHONE MESSAGES

Phone messages should not contain any of the following information about the individual for whom the message is left:

1. Full name
2. Address
3. Date of Birth
4. Social Security Number
5. Medical record number
6. Health Plan beneficiary number
7. Account Number; or
8. Any other identifying number, characteristic or code.

Generally, messages should request that the individual (use first name in the event that it is not the correct number) return the call or remind the person of an appointment. Be careful when leaving contact information that you do not inadvertently disclose information. Full name should only be left in the phone message if it is the minimum necessary and the message is left with a covered entity.

Exhibit A-5

COMMERCIAL COURIER OR THE UNITED STATES POSTAL SERVICE

When using commercial courier or the United States Postal Services to transmit PII, Workforce shall:

1. Include a full return address including Business Unit.
2. Double check contents to ensure that only correct PII is included.
3. Ensure envelope or package is well sealed.
4. Mark package “confidential.”
5. Follow **Business Unit rules** to verify identity of courier.
6. Retain tracking number as applicable.
7. Timely confirm receipt of PII directly with receiver, in accordance with the **Business Unit’s procedures**. Otherwise:
   i. If receipt of PII cannot be confirmed, contact the delivery service to track the package.
   ii. If the item cannot be located, immediately contact supervisor and OoM.

Exhibit B:

MANAGEMENT AND DISPOSITION OF PII

For specific guidelines, see the following attachments to this Exhibit B:

B-1: Electronic Storage of PII
B-2: Paper Management and Storage of PII
B-3: Disposal of PII

Exhibit B

B-1: ELECTRONIC STORAGE OF PII

Workforce shall:

1. Only store PII as required to perform job functions and permitted by **Business Unit procedures.**
2. Create new databases of PII only with supervisor authorization.
3. Only store PII on network drives and shall not store PII on “C” drive or any other local drive.
4. Store PII on a group drive only as authorized by data security administrator and only if access is restricted to Workforce members who require access to perform their job duties.
5. Ensure that computer is password-protected and has an automatic time-out engaged at all times.
6. Only store PII on portable devices (including, but not limited to, laptop computers, USB thumb drives, external hard drives, tablets, CDs) if authorized and only if portable device is encrypted according to standards approved by UMMS IT and CWM’s standards.

Exhibit B-2

PAPER MANAGEMENT AND STORAGE OF PII

Workforce shall:

1. Print PII only as authorized and avoid making more copies than necessary.
2. Pick up print jobs immediately after printing and use secure print whenever possible.
3. Not remove paper PII from its normal storage location (i.e., locked file cabinets) unless necessary to perform job duties and shall not remove PII from the workplace unless explicitly authorized by supervisor.
4. Store paper PII in locked filing cabinets whenever possible and not leave PII unattended in clear view.

Exhibit B-3

DISPOSAL OF PII

Business Units must implement reasonable safeguards on proper disposal procedures for PII to limit incidental and avoid prohibited disclosures of PII in connection with the disposal of information. Business Units must consider the potential risk to privacy and the form, type and amount of PII to be disposed. The PII must be rendered essentially unreadable, indecipherable, and so that it cannot be reconstructed. The methods of disposal should be reassessed periodically, based on current technology, accepted practices, security and availability of timely and cost-effective disposal technologies and services.

1. Dispose of PII in accordance with unit-specific record retention schedule(s), the CWM Records Management Standard and the University of Massachusetts Records Management, Retention and Disposition Policy.
2. Dispose of paper PII by cross-cut shredding or placing in a locked recycle bin according to unit-specific procedures.
3. Dispose of CDs containing PII by cross-cut shredding (contact UMMS IT Helpdesk for assistance).
4. Contact UMMS Facilities Management or the UMMS IT Helpdesk for assistance when retiring or recycling desktop or laptop computers, or any media including:
   a. An external hard drive
   b. USB thumb drive
   c. CD
   d. DVD
   e. Multi-function printer
   f. Fax machine, or
   g. Any other media to ensure proper destruction of any PII contained on the media.
5. Maintain documentation of disposal of PII including a list of records, date of disposal and method of disposal (e.g., certificate of destruction).
6. If destruction/disposal services are contracted, the contract must include a BAA, include instructions for proper disposal and require a certificate of destruction from the contractor.

Exhibit C-1

OUT OF OFFICE USE OF PII

Workforce shall:

1. Only access PII remotely if authorized in writing by supervisor.
2. Use a UMMS-authorized computer for remote access.
   a. Remotely access only Minimum Necessary PII.
3. Not physically remove PII from the workplace, unless explicitly authorized by supervisor.
   b. Hard copies of PII must be securely carried when removed from the workplace.
   c. Electronic PII shall not be removed from the workplace using portable devices unless devices are encrypted.
   d. Only Minimum Necessary information may be removed.
4. With respect to Hardware Requirements:
   a. Use a UMMS authorized computer configured solely for remote access.
   b. Ensure that the remote computer is password-protected.
   c. Activate password-protected screen savers, set to engage after 5 minutes of inactivity, or less.
   d. Ensure remote computer is equipped with a hardware-based firewall, approved by UMMS IS.
   e. Ensure remote computer is equipped with antivirus software, approved by UMMS IS.
   f. Use a laptop computer only if authorized by supervisor and laptop is equipped with encryption and theft recovery software, as approved by UMMS IS.
   g. Ensure that computer's operating system and software applications are updated automatically.
   h. Do not download any applications to the remote computer.
   i. Shut down the remote computer at end of each work day.
   j. Bring computer to UMMS IS Helpdesk for maintenance and assessment, upon request.
5. With respect to Internet Connection:
   a. Enable all security-related features of wireless connection when using a wireless network to work with PII remotely.
   b. Use the UMMS-approved VPN kit to establish and maintain a connection to UMMS systems, in accordance with all UMMS IS policies.
6. With respect to Work Space:
   a. Work in an area where PII cannot be seen or overheard by others.
   b. Ensure that all PII is in a locked drawer when unattended.
7. With respect to Work Practices:
   a. Use PII only as permitted by supervisor and as required by job duties.
   b. Do not share log-in information or passwords with any other individual.
   c. Do not store written log-in information or passwords in work space or on remote computer.
   d. Do not allow other individuals to use University-issued remote computers.
   e. Lock the remote computer (using CTRL-ALT-Delete) whenever leaving it unattended.
   f. Do not print any PII in the remote location.
   g. Do not make any copies of PII in the remote location.
   h. Do not save PII to the remote computer's hard drive, any mobile storage media, or any location other than an approved UMMS network drive.
   i. Do not disclose PII to any third party from the remote location, except with written permission from a supervisor.

j. Do not use personal email accounts to send work emails.
k. Conduct phone conversations in an area where such conversations cannot be overheard.
l. Secure PII, if necessary to transport hard copy PII between UMMS and the remote work location.
m. Do not leave PII unattended during transport except in an enclosed, locked trunk.
n. Use an approved cross-cut shredder, if necessary to dispose of paper PII in the remote location.