ePHI and Sensitive Regulated Data

The university engages in research, teaching, clinical, and business activities that encompass a variety of sensitive regulated data, including Protected Health Information (PHI) and electronic Protected Health Information (ePHI). The U-M Office of the Chief Information Officer defines sensitive regulated data as data that requires the university to implement specific privacy and security safeguards as mandated by federal, state, and/or local law, or university policy or agreement.

See the links in the Policy References section for more information on the permitted status of various university services with regard to sensitive regulated data.

Currently, UMHS Exchange Email & Calendar is the only service permitted for use with ePHI. U-M Google Email and Calendar are not authorized for ePHI usage. Email should not be used unless all recipients are also in UMHS Exchange.

Contents

- Protected Health Information (PHI)
- Transfer of ePHI and Sensitive Regulated Data
- UMHS Policy for De-identification
- Policy References
  - UMHS Policies
  - U-M Policies

ITS Sensitive Data Guide

For a list of services that can be used for specific data types, consult the Sensitive Data Guide to IT Services at the following link:
http://safecomputing.umich.edu/dataguide/

Protected Health Information (PHI)

PHI is information (including demographic information) about a patient that:

- Is created or received by a health care provider,
- 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
- 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 certain health information, including information in education records covered by the Family Educational Rights and Privacy Act (FERPA) and in employment records held by the University of Michigan in its role as an employer. These exclusions, however, may be considered Personally identifiable information (PII) that should be secured.

Examples of where PHI might be found include, but are not limited to the following:

- Medical records, including data recorded on paper, microfilm, or computer database
- Multimedia representations
- Administrative data
- Business or financial records

PHI may be delivered in many types of media: verbal, hardcopy (including printed, handwritten, or fax), and electronic. All of these media types are covered by the HIPAA Privacy Rule, which requires safeguards to protect the information. The HIPAA Security Rule, however, only covers electronic PHI (ePHI).

Transfer of ePHI and Sensitive Regulated Data
While HITS has implemented secure (or encrypted) outbound email on the UMHS Exchange server (see the Exchange - Outgoing Email Encryption page for more information), consider the following other options prior to sending or transferring sensitive data (or potentially identifiable patient information) outside the Health System:

- The MiChart Patient Portal (MyUofMHealth.org) should be used for communication between providers and patients. The portal has a limit of 5 MB per message.
- MiShare is best for file exchange, including the transfer of image files (screen shots, pictures, or scanned images/PDFs). MiShare can accommodate over 25 MB of data. Documents sent via MiShare stay on the server 5 days and then are deleted.
- U-M Box is for file storage, not transfer. M+Box can also accommodate a transfer of over 25 MB of data. Students, staff and faculty at the U-M are all entitled to have a 50 GB M+Box account.

Visit the Encryption - UMHS Policy 1-04-502 Guide page for more information regarding the transfer and encryption of sensitive information.

### UMHS Policy for De-identification

De-identified information is no longer considered to be PHI. The UMHS policy is designed to encourage the creation and use of de-identified or aggregate data sets in order to minimize the use of identifiable information for purposes where de-identified information will suffice, and to set requirements for the creation of these data sets in compliance with Title II of the Health Insurance Portability and Accountability Act (HIPAA), which defines policies, procedures, and guidelines for maintaining the privacy and security of individually identifiable health information, including PHI and ePHI.

The removal of specific information from a data set will reduce the limitations imposed by HIPAA.

- Appropriately de-identified data sets are not regulated by HIPAA.
- Limited data sets may be used or disclosed for research, public health, and other limited purposes, but only by those who sign a "data use agreement" (available from the Privacy Director, IRBMED, or DRDA).

The following chart describes the information that must be eliminated from a database, registry, or any other data set for the data set to be considered either a "de-identified data set" or a "limited data set". Note that for each data element listed, the information must be eliminated with respect to the patient and to any of the patient's relatives, employers, or household members.

**Important:** Even if HIPAA does not regulate the use of a dataset or permits its use or disclosure for research, federal regulations and University policies governing human subjects research may still apply. Contact IRBMED for more information at irbmed@umich.edu.

<table>
<thead>
<tr>
<th>Data Element</th>
<th>De-Identified Data Set</th>
<th>Limited Data Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Address, city and other geographic information smaller than state, 3-digit zip code may be included in a de-identified data set for an area where more than 20,000 people live; use &quot;000&quot; for areas where fewer than 20,000 people live.</td>
<td>Remove</td>
<td>Remove postal address information other than city, town, state or zip code.</td>
</tr>
<tr>
<td>All elements of dates (except year); plus age and any date (including year) if age is over 89. Examples: date of birth, date of death, date of admission, date of discharge, date of service.</td>
<td>Remove</td>
<td>May be included.</td>
</tr>
<tr>
<td>Telephone, fax numbers; e-mail addresses, web URL addresses, IP addresses.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Social security number, medical record number, health plan beneficiary number, any account number, certificate or license number.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Vehicle identifiers and serial numbers, including license plate numbers.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
<tr>
<td>Device identifiers and serial numbers.</td>
<td>Remove</td>
<td>Remove</td>
</tr>
</tbody>
</table>
Biometric identifiers (e.g., fingerprints; voice prints). DNA is not considered a biometric identifier for purposes of HIPAA.  Remove

Full-face photographs and any comparable images. Remove

Any other unique identifying number, characteristic or code. *Examples: a patient’s initials or scrambled social security or medical record numbers, except as permitted to re-identify information* Remove May be included.

Policy References

**UMHS Policies**

- UMHS Policy 01-04-340 - De-identification and Re-identification of Protected Health Information (PHI)
- UMHS HR Privacy Violation Policy
  - UMHS Disciplinary Policy Update

**U-M Policies**

U-M Office of the Chief Information Officer

- Sensitive Regulated Data: Permitted and Restricted Uses