

	Effective Date:	09-12-2011	
	Policy #:	H-08	
	Supersedes:		
Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of		Page:	1 of 11

PURPOSE

To establish safeguards that must be implemented by the Michigan Department of Licensing and Regulatory Affairs (LARA) workforce to protect the confidentiality of sensitive or protected health information (PHI) while stored, in use, or disclosed as permitted under all applicable confidentiality laws.

DEFINITION

Refer to HIPAA Policies and Procedures Definitions Glossary.

POLICY

LARA workforce shall use appropriate administrative, technical, and physical safeguards to protect the confidentiality, privacy, and security of sensitive or PHI. LARA workforce will only use or disclose sensitive or PHI as permitted under all applicable confidentiality laws. LARA workforce will follow the department's policy and procedures for use or disclosure of the minimum necessary, and verification of the recipient's authority to receive the sensitive or PHI.

A HIPAA covered component within LARA will not disclose PHI to a non-covered component within the department unless the purpose for the disclosure is permitted in the rules and other applicable confidentiality law, or a signed HIPAA compliant authorization has been obtained from the individual.

PROCEDURE

When sharing, transporting, transmitting, or otherwise preparing sensitive or PHI for transmission/transporting outside of work area, LARA workforce will consider all formats and use the most secure method under the circumstances. LARA workforce will also use or disclose only the minimum necessary for the intended purpose and will consider whether codes can be used as an alternative to direct identifiers.

	Effective Date:	09-12-2011
	Policy #:	H-08
	Supersedes:	
Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of		Page: 2 of 11

Set forth below are procedures establishing minimum administrative, technical, and physical standards that LARA workforce must follow to protect sensitive or PHI. Department components may develop additional policies and procedures that are more strict than the parameters set forth below in order to maximize the protection of sensitive or PH I in light of the unique circumstances of a particular area. LARA's Privacy Officer must approve the policies and procedures drafted in addition to those stated.

Verbal Communications	<p>Workforce members will not discuss sensitive or PHI outside of work areas or without a business need within work areas.</p> <p>Only the minimum necessary individually identifying information should be disclosed during oral conversations when necessary to further treatment, payment, or health care operations, or for other permitted purposes.</p>
Phones	<p>Workforce members will ensure that correct telephone numbers are dialed and that the minimum amount of information is used to convey any messages left via telephone or voice mail.</p>
Fax	<p>Fax machines must be located in secure areas not readily accessible by visitors.</p> <p>Fax only the minimum necessary to accomplish the permitted and intended purpose.</p> <p>Incoming faxes containing sensitive or PHI should not be left sitting on or near the machine.</p> <p>Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.</p>



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	3 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

Misdirected Communications - faxes containing sensitive or PHI must be immediately reported to LARAPrivacySecurity@michigan.gov. See Reminder for Misdirected Communications below.

Recipients of LARA faxes can be contacted to verify receipt of the fax.

When faxing, verify fax number and include cover sheet with the following confidentiality disclaimer:

"Confidentiality Notice: The information contained in this facsimile message from the Michigan Department of Licensing and Regulatory Affairs is intended solely for the use of the above named recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure, or distribution of any confidential and/or privileged information contained in this fax is expressly prohibited. If you have received this fax in error, please telephone us immediately so that we can correct the error and arrange for destruction or return of the faxed document."

E-mail	<p>E-mail of sensitive or PHI Outside of the State of Michigan (SOM) firewall requires workforce member to comply with one of the following options: <i>(E-mail addresses that end in "Michigan.gov" are inside the SOM firewall. Any others are going OUTSIDE the SOM firewall.)</i></p> <p><u>Option 1:</u> Since e-mailing inherently is not a secure method of transmitting sensitive or PHI, it should be used only as a last measure. If appropriate, first consider faxing or phoning PHI; or use an alternative electronic communication transmission such as</p>
---------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	4 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

the Single Sign On File Transfer system. Contact LARA Data Security Officer for other possible electronic communication alternatives.

Option 2: E-mail information without identifiers in combination with a fax or phone call with the identifiers. Also, see *Guidelines* below.

Example:

E-mail: "Beneficiary has called the Beneficiary Help Line and claims that coverage for Ultram has been denied, however, the beneficiary cannot tolerate other pain medications. Please see Fax for identifying information."

Fax (or phone call):

"E-mail sent at 1:50 pm with KK in the subject line is for Jane Doe, Medicaid 10# 99999999."

Option 3: Encrypt and password protect a document that contains the sensitive or PHI and attach to outbound e-mail. The subject line and body of the outbound e-mail must not contain sensitive or PHI. Phone or fax the password separately.

E-mail of Sensitive or PHI *Within* the SOM firewall:

E-mail exchanges that remain within the SOM firewall are more secure; however, care should be taken to follow the guidelines below.

Guidelines for all e-mails *Within or Outside* the SOM firewall containing sensitive or PHI:

When e-mailing authorized communications that reference sensitive or PHI always:

- Disclose the minimum amount of sensitive or PHI necessary to accomplish the intended purpose of the use, disclosure, or



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	5 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

- request.
- Ensure that all persons receiving the e-mail have a right to receive the information. The "To" line must be checked to make sure you have the correct e-mail address of the intended recipient before sending the email.
 - Do not include sensitive or PHI or identifiers in the subject line (identifiers may only be used minimally within the SOM firewall.)
 - Include the following disclaimer:

"Confidentiality Notice: This message, including any attachments, is intended solely for the use of the named recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure, or distribution of any confidential and/or privileged information contained in this e-mail is expressly prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy any and all copies of the original message."

Misdirected e-mails containing sensitive or PHI must be immediately reported to the Director's Office. See Reminder for Misdirected Communications Section below.

Receiving unencrypted e-mail with sensitive or PHI from outside the SOM firewall.

Advise the sender that sending information through an unencrypted electronic mail is not secure. When replying, send a separate e-mail following the stated guidelines or remove all identifying information from the original e-mail. If needed, contact the Security Officer for other electronic options to exchange sensitive and PHI.

Other Electronic	Authorized communications transmitted by other electronic
-------------------------	-----------------------------------------------------------



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	6 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

Communications	systems such as Single Sign On File Transfer will be transmitted to persons or systems with a right to receive the information, and contain only the minimum necessary information for the intended purpose of the disclosure.
Paper	<p>All paper with sensitive or PHI must be protected from the view of others who do not have a need to know the information to perform their job. Only those individuals that have the authority to access the sensitive or PHI are permitted to view the letter, report, form, document, etc.</p> <p>Paper with sensitive or PHI that is not presently in use must be turned upside down, placed in a drawer, locked in a file cabinet, or secured in another manner - based on the authorized user's reasonable judgment and present need.</p>
Mail (USPS, certified USPS, or other mail delivery service such as Fed Ex)	<p>LARA workforce must ensure that:</p> <ul style="list-style-type: none"> • The last known correct address is used for the intended recipient • The complete address information, to include apartment numbers when applicable, is used for the intended recipient • The address is typed or written in a legible manner • The return address appears on the envelope or package <ul style="list-style-type: none"> • The return address does not readily identify a specific LARA program • The mail envelope or package is appropriate in size, shape and strength for the items being mailed • The mail envelope or package is securely sealed • Materials placed into the envelope or mail package is only



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	7 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

- information that is intended for the addressee
- Do not send sensitive or PHI to an individual who is not authorized to view the sensitive or PHI

Misdirected mail containing sensitive or PHI must be immediately reported to the Director’s Office. See Reminder for Misdirected Communications Section below.

Interoffice Mail

- LARA workforce must ensure that:
- The correct address is used for the intended recipient,
 - The complete location information for the intended recipient is used to include:
 - full name,
 - department,
 - division,
 - building, and
 - floor (if applicable and available).
 - The address is typed or written in a legible manner.
 - The interoffice mail envelope is securely sealed.
 - Materials placed in an interoffice envelope or mail package is only information that is intended for the addressee.
 - Do not send sensitive or PHI to an individual who is not authorized to view the sensitive or PHI.

Misdirected interoffice mail containing sensitive or PHI must be immediately reported to the Director’s Office. See Reminder for Misdirected Communications Section below.



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	8 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	---------

Physical Collection or Transport of Sensitive or PHI Outside of Work Area

Before sensitive or protected health information can be collected, removed, or transported outside of work area, LARA workforce member must document by memo the business need to collect, remove, or transport the sensitive or PHI and obtain management approval as outlined below. The memo must also include the planned actions to ensure the privacy and security of the sensitive or protected health information.

Paper:

Workforce member must document by memo the business need for collection, removal, or transport of the paper with sensitive or protected health information and obtain supervisor, bureau director, and administrator's authorization.

In lieu of drafting a memo, any area that routinely collects, removes, or transports paper with sensitive or PHI must implement policy and procedures to ensure the paper is secured in a reasonable manner in light of the business need, purpose, and other variables such as general location, distance transported, destination, and storage locations.

Reasonable options based on the above factors may include any combination of: sealed envelopes, secure folders, locked briefcases, secured boxes, locked automobile trunks, locked and secured offsite storage rooms, etc.

Portable Electronic Devices:

Portable electronic devices can include a laptop computer, compact disc, thumb or flash drive, BlackBerry, or any other portable device that is capable of receiving and storing data from an apparatus that maintains electronic information.



Effective Date:

09-12-2011

Policy #:

H-08

Supersedes:

Subject:

Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of

Page:

9 of 11

Before downloading sensitive or protected health information to a portable electronic device, LARA workforce must:

- Draft a memo that describes:
 - o The purpose for the download,
 - o The type of device that will be used,
 - o The type of data to be downloaded
 - o Whether the data will be taken out of the agency
- Obtain the workforce member's supervisor and bureau director's signatures of approval on the memo, and
- Provide the memo to the Department's Security Officer who will work with the workforce member to ensure that the sensitive or protected health information is appropriately encrypted and password protected.

If your program area routinely collects, removes, or transports sensitive or PHI using a portable electronic device, you may obtain one memo described above. Alternatively, if you only collect or transport sensitive or PHI on a portable device from time-to-time, you may have to obtain a memo described above each time you collect or transport sensitive or PHI on a portable device.

BlackBerry or similar devices can be synced with a personal computer and *receive* e-mails. Be aware that e-mails you *receive* on your BlackBerry may contain sensitive or PHI. The e-mail procedures *above* must be followed for BlackBerry or similar

devices when sending e-mail from those devices when that e-mail contains sensitive or PHI.

Any loss, theft, or breach of paper or electronic devices must be immediately reported to the Director's Office. See Reminder for



Effective Date:	09-12-2011
Policy #:	H-08
Supersedes:	

Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of	Page:	10 of 11
---------------------------------------------------------------------------------------------------------------------	--------------	----------

	Misdirected Communications Section below.
<i>Destruction: Paper, CDs, Floppies, and other portable media</i>	Paper with sensitive or PHI must be shredded or pulverized before recycling. CDs and floppies are to be destroyed prior to disposal by shredding or pulverizing.
<i>Computer Visibility and Access</i>	<p>Sensitive or PHI on computer screens will not be viewable by a casual <i>observer</i>.</p> <p>Workforce members will use a screen <i>saver</i> or position the computer to minimize others' <i>view</i> of the screen.</p> <p>Computer log-ins will be changed routinely and not shared with others. (See related Security Policy and Procedure.)</p> <p>Workforce members will log-off if away from computer for an extended length of time.</p>

Reminder:

Misdirected Communications/Transmissions, Unpermitted or Unauthorized Communications/Transmissions or Breaches that Contain Sensitive or PHI :
 All instances of misdirected, unpermitted or unauthorized communications or breaches that contain sensitive or PHI must be immediately reported to the Director's Office to

	Effective Date:	09-12-2011	
	Policy #:	H-08	
	Supersedes:		
Subject: Protected Health Information - Physical Safeguards for the Storage, Use, or Disclosure of		Page:	11 of 11

be investigated, mitigated, and documented in the incident log.

A breach includes but is not limited to the loss or theft of any paper or electronic devices that contain sensitive or protected health information.

REFERENCES/FORMS

[45 CFR §164.304](#), [45 CFR §164.30B](#), [45 CFR §164.310](#), [45 CFR §164.312](#), [45 CFR 164.502\(a\)\(1\)\(iii\)](#), [45 CFR §164.502\(b\)](#), [45 CFR §164.514\(d\)\(1\)](#), [45 CFR §164.530\(c\)](#), [DTMB 1315.00](#).