


Administrative, Technical and Physical Safeguards

	Louisiana Department of Health (LDH)	
	Policy Number	24.1
	Effective Date	April 14, 2003
	Inquiries to	Office of the Secretary Bureau of Legal Services P.O. Box 3836 Baton Rouge, Louisiana 70821-3836 (225) 342-1112 FAX (225) 342-2232

LDH is committed to fostering, cultivating and preserving a culture of equity, diversity and inclusion. Our human capital is the most valuable asset we have. The collective sum of the individual differences, life experiences, knowledge, inventiveness, innovation, self-expression, unique capabilities and talent that our employees invest in their work represents a significant part of not only our culture, but our Department's reputation and achievement as well.

If there is a discrepancy between an LDH Policy and a Program Office or facility policy, the LDH policy shall govern/overrule/supersede the conflicting section within the Program Office or facility policy.

I. PURPOSE

The intent of this policy is to establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use or disclosure.

II. APPLICABILITY

LDH's HIPAA Privacy Policies are applicable to LDH's workforce and its Business Associates.

III. IMPLEMENTATION

The implementation date of these policies is April 14, 2003.

IV. DEFINITIONS

The definitions are included in the body of these policies.

V. RESPONSIBILITIES

LDH's workforce and its Business Associates are responsible for assuring that LDH's HIPAA Privacy Policies are followed. The LDH Privacy Officer and the Program Privacy Officers are responsible for the implementation, resolution and enforcement of all aspects related to LDH HIPAA Privacy Policies.

VI. EXCEPTIONS

The exceptions are listed in the policies.

VII. POLICY: ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

- A. LDH must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of LDH privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information. This policy applies only to Protected Health Information (PHI) or Other Confidential Information about Individuals (OCII) received, created, used, disclosed or maintained by LDH.
- B. Safeguarding Confidential Information - LDH Workplace Practices
 1. Paper
 - a) Each LDH workplace will store files and documents containing confidential information in locked rooms or storage systems when available.
 - b) In workplaces where lockable storage is not available, LDH staff must take reasonable efforts to ensure the safeguarding of confidential information.
 - c) Each LDH workplace will ensure that files and documents containing confidential information that are awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
 - d) Each LDH workplace will ensure that shredding, burning or other authorized methods of disposal of files and documents containing confidential information is performed on a timely basis, documented and consistent with all applicable record retention requirements.

- e) Each LDH workplace must foster workforce awareness of the potential for inadvertent disclosure of confidential information.

2. Oral

- a) LDH workforce members must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- b) Each LDH workplace should make enclosed offices and/or interview rooms available for the verbal exchange of confidential information, when such rooms are available for that purpose.
- c) When conducting telephone conversations that involve the exchange of confidential information, every reasonable step should be taken to insure that the conversation will not be overheard by unauthorized individuals.

Exception: In work environments structured with few offices or closed rooms, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that LDH has met the reasonable safeguards and minimum necessary requirements.

- d) Each LDH workplace must foster workforce awareness of the potential for inadvertent verbal disclosure of confidential information.

3. Visual

- a) LDH workforce members must reasonably ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
- b) Computer screens: Each LDH workplace must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
- c) Paper documents: LDH staff must be aware of the risks regarding how paper documents are used and handled, and must take all reasonable and necessary precautions to safeguard confidential information.
- d) Fax machines, copiers, scanners and other similar devices: These types of devices should not be located in areas accessible to the public. All reasonable and necessary precautions should be taken to safeguard confidential

information passing through such devices, including checking these devices on a regular basis for documentation containing confidential information.

- e) Each LDH workplace must foster workforce awareness of the potential for inadvertent visual disclosure of confidential information.

4. Electronic

- a) Each LDH workplace must take reasonable and necessary steps to assure that confidential information in electronic form cannot be accessed by individuals who do not have a job-related reason for accessing that particular confidential information. Such reasonable safeguards include but are not limited to individualized password for access to personal computers, laptops, personal digital assistants (PDAs) and other similar devices and password protected screen savers.
- b) Each LDH workplace must take reasonable and necessary steps to assure that all personal computers, laptops (including hard drives, disks, CDs, tapes, and other similar devices), and PDAs and other similar devices in which confidential information is stored is backed up on a regular basis and stored in a manner not inconsistent with this policy.
- c) Each LDH workplace must take reasonable and necessary measures to assure that all confidential information stored on personal computers, laptops (including hard drives, disks, CDs, tapes, and other similar devices), PDAs and other similar devices is destroyed on a timely basis, documented and consistent with all applicable record retention requirements and all such devices must be completely wiped clean of all confidential information prior to disposal of the device.
- d) Each LDH workplace must foster workforce awareness of the potential for inadvertent disclosure of confidential information contained within personal computers, laptops, PDAs and other similar devices.

C. Safeguarding Confidential Information - LDH Workforce Practices

1. LDH Databases

- a) LDH will implement a role-based access (RBA) or other method for all LDH databases.
- b) RBA is a form of security allowing access to data based on job function in accordance with LDH security procedures. Workforce members shall be assigned to an RBA group that will be designed to give members access to the minimum necessary information to fulfill their job functions.

- c) Other methods may also be developed to assure that workforce members have access only to information which is necessary to do their jobs for LDH.
 - 1. Implementation of role-based access and LDH Policy #22, "Minimum Necessary Information," will promote administrative safeguards.
 - 2. Conducting internal reviews periodically will permit LDH to evaluate the effectiveness of safeguards.
 - (a) LDH managers and supervisors should use the LDH Safeguards Assessment Tool to conduct annual reviews in order to evaluate and improve the effectiveness of their current safeguards.
 - (b) Development and implementation of department-wide security policies will enhance administrative safeguards.
- 2. GroupWise or Other Email Systems
 - a) All communications containing confidential information using Group Wise or other email systems will comply with LDH Policy #22, "Minimum Necessary Information" and not contain any confidential information within its caption (i.e. RE: or Subject).
 - b) All communication containing confidential information using Group Wise or other similar systems will contain a verification message or device to assure that it was received by the party it was intended for.
 - c) All communication containing confidential information using Group Wise or other similar systems will contain a confidentiality message to assure that if it was inadvertently sent to someone other than the intended recipient that that individual has been warned not to read the information and to return it immediately.
 - d) LDH may develop an encryption methodology for all external electronic messages.
- 3. Faxing, Scanning or Other Similar Methods of Electronic Disclosure of Information
 - a) All communications containing confidential information using faxing, scanning or other similar methods of electronic disclosure of information will comply with LDH Policy #22, "Minimum Necessary Information," and not contain any confidential information within its caption (i.e. RE: or Subject).
 - b) All communications containing confidential information using faxing, scanning or other similar methods of electronic disclosure of information will contain a verification message or device to assure that it was received by the party to whom it was intended to be sent.

- c) All communications containing confidential information using faxing, scanning or other similar methods of electronic disclosure of information will contain a confidentiality message to assure that if inadvertently sent to someone other than the intended recipient that the individual has been warned not to read the information and to return it to the sender immediately.
 - 4. Workforce HIPAA Privacy Training, Confidentiality Form and Access Form
 - a) Prior to being given access to any confidential information in the possession of LDH, all members of LDH workforces are required to:
 - 1) Receive the required HIPAA Privacy Training; and
 - 2) Sign LDH HIPAA Privacy form #801P, "Privacy Statement of Understanding Form";
 - b) Prior to receiving access to a LDH database, a member of LDH workforce must:
 - 1) Demonstrate a need for access to that LDH database,
 - 2) Receive login ID(s) and password(s) for each LDH database that the workforce member is seeking access, and
 - 3) Sign the required forms necessary for receiving such access to a LDH database.
 - c) No workforce member shall give their login ID(s) or password(s) to anyone other than those authorized to have their login ID(s) and password(s) (IT System Administrators and/or the workforce member's supervisor). No workforce member shall use another workforce member's login ID or password to gain access to any LDH database.
- D. Safeguarding Confidential Information – Client or Participant's or Their Personal Representative's Waiver

A client, participant or their Personal Representative may expressly waive any or all of the above safeguards as they relate to their PHI. This waiver does not and cannot apply to access to any LDH database.

Policies:

LDH Policy #17 - "General Privacy Policy"

LDH Policy #18 - "Client and Participant Privacy Rights"

LDH Policy #19 - "Use and Disclosures of Client or Participant Information"

LDH Policy #20 - "De-identification of Client and Participant Information and Use of Limited Data Sets"

LDH Policy #21 - "Uses and Disclosures for External Research Requests, Internal Research Needs and Waiver of Privacy Rights for Research Purposes"

LDH Policy #22 - "Minimum Necessary Information"

LDH Policy #23 - "LDH Business Associate Relationships"

LDH Policy #25 - "Enforcement, Sanctions, and Penalties for Violations of LDH HIPAA Privacy Policies"

Forms(s):

LDH Safeguards Assessment Tool

LDH HIPAA Privacy form #801P, "Privacy Statement of Understanding"

References:

45 CFR 164.502(a)

45 CFR 164,508-164.512 42 CFR Part 2

Contact(s):

State of Louisiana

The Louisiana Department of Health Office of the Secretary

Privacy Office

P.O. Box 629

Baton Rouge, LA 70821-0629 Phone : 1-877-559-9664

Email : privacy-dhh@dhh.la.gov

VIII. REVISION HISTORY

Date	Revision
April 14, 2003	Policy created
August 8, 2017	Policy reviewed
June 5, 2019	Policy reviewed