Adventist HealthCare

TRAINING

Lab Location:	All Laboratories	**Date Distributed:**	2025
Department:	All Departments	**Due Date:**	See MTS assigned due date
		Implementation:	**In effect currently**

Name of procedure:
AHC.L41 HIPAA Policy
Description:
Please read the attached HIPAA Policy and take the quiz.

Document your compliance with this training update by taking the quiz in the MTS system.

AHC.L41 HIPAA Policy

Copy of version 7.0 (approved and current)

Last Approval or Periodic Review Completed	9/18/2024
Next Periodic Review Needed On or Before	9/18/2026
Effective Date	9/18/2024

Uncontrolled Copy printed on 5/29/2025 4:36 PM

Printed By Demetra Collier (110199)

Organization Adventist HealthCare

Approval and Periodic Review Signatures

Type	Description	Date	Version	Performed By	Notes
Approval	Lab Director	9/18/2024	7.0	 Nicolas Cacciabeve	
Approval	Laboratory System Operations Director	9/18/2024	7.0	 Robert SanLuis	
Periodic review	Lab Service director	11/1/2023	6.0	 Robert SanLuis	
Approval	Lab Director	11/15/2021	6.0	Nicolas Cacciabeve	
Approval	Lab Service director	11/10/2021	6.0	 Robert SanLuis	
Approval	QA approval	11/8/2021	6.0	Leslie Barrett (104977)	
Approval	Lab Director	12/5/2019	5.0	Nicolas Cacciabeve	
Approval	Core lab approvals	12/4/2019	5.0	 Robert SanLuis	
Approval	QA approval	11/27/2019	5.0	Leslie Barrett	
Approval Captured outside MediaLab	Lab Director	5/15/2018	4.0	Nicolas Cacciabeve	Recorded on 3/13/2019 by Leslie Barrett (104977) when document added to Document Control
Periodic review Captured outside MediaLab	Designated Reviewer	5/15/2018	4.0	Nicolas Cacciabeve	Recorded on 3/13/2019 by Leslie Barrett (104977) when document added to Document Control

Approvals and periodic reviews that occurred before this document was added to Document Control may not be listed.

Prior History

Updated prefix 11/16/21

Version History

Version	Status	Type	Date Added	Date Effective	Date Retired
7.0	Approved and Current	Major revision	9/12/2024	9/18/2024	Indefinite
6.0	Retired	Major revision	11/8/2021	11/15/2021	9/18/2024
5.0	Retired	Major revision	11/27/2019	12/18/2019	11/15/2021
4.0	Retired	First version in Document Control	3/13/2019	5/17/2018	12/18/2019

Non-Technical SOP

Title	**HIPAA Policy**	
Prepared by	Leslie Barrett	Date: 7/31/2009
Owner	Robert SanLuis	Date: 5/11/2018

Laboratory Approval		
Print Name and Title	**Signature**	**Date**
Refer to the electronic signature page for approval and approval dates.		
Local Issue Date:	Local Effective Date:	

TABLE OF CONTENTS

1. PURPOSE

This policy explains the controls, processes and procedures to obtain, maintain, use and disclose patient protected health information (PHI) in a manner that protects patient privacy and complies with Health Insurance Portability and Accountability Act (HIPAA.)

2. SCOPE

All employees are required to conduct the company's business honestly, ethically, and with the highest degree of integrity.

3. RESPONSIBILITY

All staff must comply with all applicable laws and regulations that govern our business operations, including but not limited to those laws, rules and regulations governing test reimbursement under the Medicare and Medicaid programs.

All staff is required to complete compliance training on an annual basis.

4. DEFINITIONS

Health Insurance Portability and Accountability Act (HIPAA): Legislation that protects PHI by providing standards for billing transactions, diagnosis and CPT codes, and establishing rules to regulate the use and disclosure of PHI.

Protected Health Information (PHI): All individually identifiable patient health information obtained, maintained, used or disclosed, regardless of its format (oral, electronic, and paper). PHI is the patient health information we use every day to do our job – the personal and medical information that relates to specific patients. Examples include completed requisitions, patient reports, and completed insurance claim forms.

Use: the release of PHI to persons within Quest Diagnostics or the hospital

Disclose: the release of PHI to any person or entity external to Quest Diagnostics or the hospital

Obtain: to receive PHI from a person or entity external to Quest Diagnostics or the hospital

Maintain: to store PHI within Quest Diagnostics or hospital systems and documents.

PHI Breach: The acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI and that requires notice to the patient pursuant to this Procedure.

Potential PHI Breach: An incident that may or may not be a PHI Breach but must be reviewed and analyzed through this Procedure.

PI Breach: The unauthorized acquisition of or access to personal information by a person or organization as defined by state laws.

Personal information (PI): State laws have been enacted that protect citizens against identity theft. For purposes of this SOP, it shall mean a person's name (first name or first initial together with last name) in combination with any one, or more, of the following data:

- Social Security Number (or in the case of non-U.S., federal identification number)
- Driver's License Number (or State Identification Card Number)
- Account Number (to a financial account), Credit Card or Debit Card Number
- Employee ID Number (as assigned by an individual's employer)
- Date of Birth
- Maiden Name of the Individual's Mother
- Medical Information (any individually identifiable health information regarding the individual's medical history or medical treatment or diagnosis)
- Health Insurance Information (insurance policy or subscriber numbers, applications for insurance, claim histories and appeals)

5. PROCEDURE

A. General guidelines
1. We are obligated to keep and maintain privacy when we obtain, maintain, use or disclose PHI.
2. We are allowed to utilize PHI in the normal course of business without the patient's authorization. This is defined by HIPAA as
   a. Treatment (example - sending results to the patient's physician)
   b. Health care operations (example - specimen collection)
3. Inappropriate use or disclosure of PHI must be reported to a supervisor and will result in disciplinary action.
4. Only the amount of PHI necessary to complete a task should be utilized.

B. General PHI controls
1. Physical Security
   a. Restricted access to Laboratory areas by non-employees
   b. Use of employee identification
   c. Appropriate destruction of material that contains PHI (shredder boxes)
   d. Secured areas for reports, specimens, and other documents that contain PHI.
   e. Return of keys and other security items by terminated employees.
2. System Security
   a. Protection of username and password by employee. (LIS security agreement)
   b. Scheduled password changes required
   c. Computer access limited based on job assignment
   d. Appropriate use of test systems vs 'live' data
3. Process Security
   a. Training for staff to recognize and protect PHI
   b. Procedures to ensure appropriate use of PHI
   c. Procedures to respond to inappropriate or accidental disclosure of PHI
   d. Method to report potential non-compliance
4. Off-site Security
   a. Prohibit sending or storing PHI on non-Quest / Hospital computers
   b. Procedures to avoid theft or removal of PHI from facility
   c. Procedure to eliminate inadvertent disclosure of PHI to non-employees
   d. Procedures to control removal of PHI from premises

C. Laboratory specific guidelines
1. Do not discuss patient information outside the Laboratory area (i.e., hallway, cafeteria, lounge)
2. Be aware of your surroundings when discussing PHI with patient, physician or staff, especially in areas that are open to the public (OP lab and phlebotomy).
3. Keep computer monitors and other displays with PHI positioned away from viewing by non-employees.
4. Always log out of computer systems when leaving the workstation.
5. PHI applies to <u>all</u> patients. Inappropriate access of your own, your family member, friend or co-worker's information or results is prohibited.

D. Patient Rights
1. Patients have certain rights concerning their PHI and how it is used, disclosed, obtained and or maintained by Quest Diagnostics.
2. If the report contains results relating to drug and alcohol abuse, AIDS, and sexually transmitted diseases, physician approval is required before releasing to the patient.
3. Refer to the Client Service procedure 'Release of Patient Laboratory Results' requirements to provide test results to a patient.

E. Potential PHI Breaches
1. If you receive notification of or identify an unauthorized acquisition, access, use or disclosure of PHI in oral, electronic or paper form, complete a PHI Incident Form (see step 3). Ask the individual to destroy the hard copy **after** obtaining the information to complete the form.

   If PHI was faxed to an incorrect phone number AND the fax location is known, contact the receiver to request destruction of the document. Complete a PHI Incident form (see step 3).

   If PHI was faxed to an incorrect phone number AND the fax location is NOT known, complete a FAX cover sheet with the following message:
   "Our records indicate that we have inadvertently sent you a fax from Adventist HealthCare. **Please destroy**."
   Fax this to that same phone number. Complete a PHI Incident form (see step 3).

   Note: If PHI in paper form is delivered to the wrong address and is returned in the original, ***unopened*** envelope
   - This is NOT a PHI breach
   - The event must be investigated. Complete a Quality Variance (QV) form and attach the ***unopened*** envelope

2. If any of the following occurs, document on a QV form and complete the PHI Incident form (See step 3):
   a. PHI is found in public
   b. PHI is securely transmitted (VPN, Internet w/ encryption etc), but to the wrong client/party
   c. Documents, equipment or other media that contain PHI have been lost
   d. Documents or electronic media (laptops, hard drives, CDs, tapes mobile or removable media) are not properly destroyed
   e. PHI was potentially breached as a result of internal/external hacker, or unauthorized access by contractor
   f. PHI was breached in oral, electronic or paper form by an employee in violation of the Company's Privacy of Protected Health Information Policy
   g. The PHI disclosure involves a large volume of patients or unusual circumstances

3. Complete the PHI Incident form (See appendix A for instructions.

4. Print the form (see appendix A for instructions) and **immediately** give the form to a Laboratory supervisor or manager. If no supervisor or manager is onsite, the form should be given to the Group Lead or incharge technologist. The Group Lead / incharge tech must immediately notify the on-call administrative supervisor.

5. The Supervisor will alert the Laboratory Director and Compliance Officer. Any accidental disclosure or PHI breach must be investigated for root cause. The Compliance Officer will coordinate the investigation and recommend any additional action required.

F. Potential PI Breaches
[Note: Incidents involving PHI (healthcare related information) are typically PHI breaches; PI breaches more typically involve employee information.]

1. If you receive notification of or identify an unauthorized acquisition, access, use or disclosure of PI in oral, electronic or paper form, complete a Potential PI Breach Reporting Form.

2. Give the PI Breach Reporting form **immediately** to a Laboratory supervisor or manager. If no supervisor or manager is onsite, the form should be given to the Group Lead or incharge technologist. The Group Lead / incharge tech must immediately notify the on-call administrative supervisor.

3. The Supervisor will alert the Laboratory Director and Compliance Officer. Any accidental disclosure or PI breach must be investigated for root cause. The Compliance Officer will coordinate the investigation and recommend any additional action required.

6. RELATED DOCUMENTS

- Quest Diagnostics, *our*Quest *on*line intranet site, https://questdiagnostics.sharepoint.com/sites/intranet
  - Radar Potential Privacy Incident Reporting Form
- Release of Patient Laboratory Results, Client Service/OP Lab procedure
- Verbal Release of Test Results to Outside Locations, Laboratory policy

7. REFERENCES

- Quest Diagnostics Compliance Policies/Procedures, Privacy of Protected Health Information (PHI), 02/24.
- Quest Diagnostics Incorporated Corporate SOP 702A PHI and/or PI Breaches
- Corporate Policy Manual HIPAA Privacy and Notice of Privacy Practices Policy AHC.4.30

8. REVISION HISTORY

Version	Date	Reason for Revision	Revised By	Approved By
		Supersedes SOP L052.000		
000	1/18/2010	Title page: Updated owner Section 4: Added PHI Breach definitions Section 5: Item E updated terminology, added unopened envelope, added 2.a,e,f, and items 3,4,5 Section 6: Added Potential PHI Breaches policy Section 7: Removed SOP 701A, added SOP 702A Section 9: added PHI Incident form	L. Barrett	L. Loffredo
001	2/26/2010	Section 5: Item E,1 added PHI breach by fax Section 9: added PHI Breach Destroy Fax form	L. Barrett	L. Loffredo
002	6/10/2014	Section 4: Added PI definitions Section 5: Item E updated to match revised PHIIT, Item F added Section 6: Added lab policy and fax forms Section 9: Added corporate PI breach reporting form and updated PHIIT form Footer: version # leading zeros dropped due to new EDCS in use as of 10/7/13.	L. Barrett	L. Loffredo
3	5/11/2018	Updated owner Header: Added other sites Section 9: Updated App A, added note	L Barrett	R SanLuis
4	11/27/19	Header: Changed WAH to WOMC Section 5.E.1: Revised for unknown FAX location Section 6: Removed 'FAX sent in error' forms, updated QD intranet website Section 9: Moved QD form to Related Documents	L Barrett	R SanLuis
5	11/8/21	Header: Deleted site names, added All Labs Footer: Updated prefix to AHC	L Barrett	R SanLuis
6	9/12/24	Step 2 added complete QV form Step 3: Removed PHIIT reporting tool and replaced with PHI incident form Step 4: added reference to Appendix A Added Appendix A- Instructions for locating and completing the PHI incident form	D Collier	R SanLuis

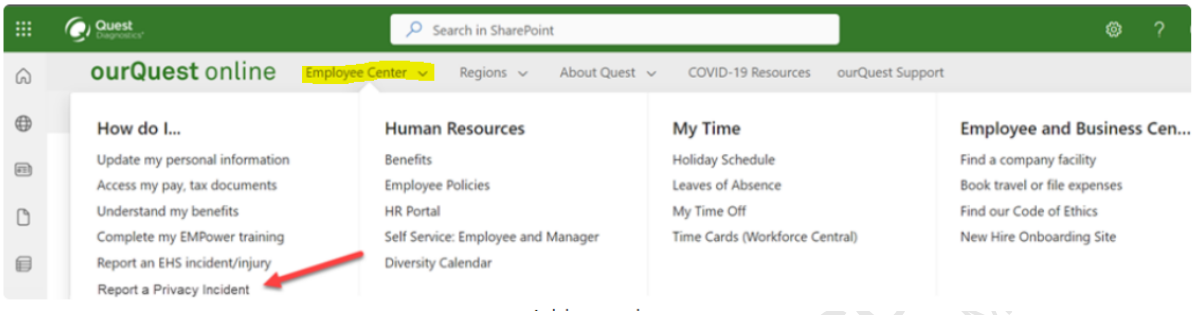
9. ADDENDA AND APPENDICES

Appendix A: Radar First PHI incident reporting form

Appendix A: Radar First PHI reporting Form

To report a PHI incident:

1. Go to "ourQuest online" or right click this link and open hyperlink: https://questdiagnostics.sharepoint.com/sites/intranet
2. Select the "Employee Center" dropdown
3. Select "Report a Privacy Incident"



4. Complete the form and print before hitting the submit button.
   - Right click with your mouse
   - Select Print
   - Change printer to "Save as PDF"
   - Save the form to your desktop

5. "Submit" the form on the Quest intranet site.
6. Print the form from your desktop. Attach the printed form to a completed QV and **immediately** give it to your supervisor or Group Lead.