Lab Location:	GEC, SGMC & WOMC	**Date Distributed:**	3/16/2021
Department:	All staff	**Due Date:**	Within 30 days of assignment

Name of procedure:
HIPAA Policy   SGAH.L41 v5
Description:

There is no change to this SOP.

This update is intended to

- re-inforce the rules regarding the process to obtain, maintain, use and disclose patient protected health information (PHI)

- remind staff that failure to comply is considered misconduct and will result in disciplinary action

Read the SOP and document your compliance with this training update by taking the quiz in the MTS system.

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

In ADDITION certain states may include:

- 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 user name 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 all 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 'Patient Requesting 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 Tracking (PHIIT) Tool 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 PHIIT Tool 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 PHIIT Tool 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 PHI Incident form:
     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 PHIIT Tool form (see Related Documents) as follows:
     o Today's Date
     o Business Unit

       ○ Date Incident Occurred
       ○ Date Incident Discovered
       ○ Date Incident Reported
       ○ Discovered by: Check the appropriate box and record the person's name
       ○ Reported By: Name and contact information for person reporting
       ○ Did this involve 500 or more patients? Yes or No
           ▪ **If yes, contact the Privacy Office immediately**
       ○ Category: Check the appropriate box and sub-category
       ○ Type of Data Discovered: Check the appropriate box and add details
       ○ Detailed Description of the Event – describe what happened, continue on the second page if more space is needed
       ○ Complete applicable area(s) and indicate information that was disclosed
       ○ Was PHI returned, destroyed or removed? Yes or No
       ○ Was PHI protected because the incorrect recipient did not disclose it to another party? Yes or No
       ○ Behavior of the Recipient
       ○ Corrective Actions
       ○ Employee Error Type
       ○ Name of Person Completing the Form
       ○ Contact Information of Person Completing the Form

4. Give the PHIIT 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.

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
   [<u>Note</u>: **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 Compliance Policies/Procedures, *our*Quest *on*line intranet site, Communities, Compliance
  https://questdiagnostics.sharepoint.com/sites/DigitalWorkplace/Pages/Home.aspx
  - PHI Incident Tracking (PHIIT) Tool Form
- Patient Requesting 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), 06/08.
- Quest Diagnostics Incorporated Corporate SOP 702A PHI and/or PI Breaches

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 zero's 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

9.   ADDENDA AND APPENDICES
None