




POLICY ID# 2022-002
CLEARED BY: Jamie Cook
DATE: 7-1-2022

Scott Harris, M.D., M.P.H.
STATE HEALTH OFFICER

MEMORANDUM

TO: Medical Officers
District Administrators and Assistant District Administrators
Bureau, Division, Office, and Branch Directors

FROM: Scott Harris, M.D., M.P.H. 
State Health Officer

DATE: July 1, 2022

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policy #2022-002
(Replaces Policy #2018-001)

Attached is the revised HIPAA Privacy and Security Policy (Policy #2022-002). Additions were made that will enhance both the physical and logical security of protected health information and electronic protected health information (ePHI). Facility security requirements were added to provide a framework for actions and practices intended to enhance physical security at each Alabama Department of Public Health facility. In addition, technological guidelines and restrictions involving software and devices were added to ensure the security of all ePHI. Required forms and flow charts were also added to ensure compliance and offer guidance.

This policy must be circulated to all employees. Supervisors are responsible for ensuring that current employees read the revised 2022 policy and complete all HIPAA training activities.

SH/PK
Attachment

**ALABAMA DEPARTMENT OF PUBLIC HEALTH
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
(HIPAA) PRIVACY AND SECURITY POLICY**

TABLE OF CONTENTS

SECTION 1 - POLICY

1.1 Applicability 1-1
1.2 Definitions..... 1-1

SECTION 2 - TREATMENT/PAYMENT/HEALTH CARE OPERATIONS

2.1 Treatment/Payment/Health Care Operations 2-1

SECTION 3 - PATIENT RIGHTS

3.1 Notice of Privacy Practices..... 3-1
3.2 Patient/Client Access to View PHI in Their Records or in Designated
Record Sets 3-1
3.3 Access to Laboratory Reports..... 3-4
3.4 Amendment to Patient's/Client's Protected Health Information 3-4
3.5 Requests by the Patient to Limit Releases of PHI 3-5
3.6 Requests by the Patient/Client for an Accounting of PHI 3-6
3.7 Requests for Alternative Means of Communication..... 3-8
3.8 Requests for Patient/Client Information Regarding Research and Marketing..... 3-8
3.9 Requests for Information on Deceased Patients/Clients..... 3-8

SECTION 4 - MINIMUM NECESSARY RULE

4.1 Minimum Necessary Disclosures and Access 4-1
4.2 Situations in which the Necessary Rule Does NOT Apply 4-2

SECTION 5 - GENERAL STANDARDS FOR HANDLING PHI

5.1 Face-to-Face Discussions 5-1
5.2 Telephone Calls 5-1
5.3 Visual Access to PHI Displayed on Computer Screens..... 5-1
5.4 Paper Records and Files 5-2

5.5	Outgoing Mail	5-2
5.6	Faxing	5-2
5.7	General Email Procedures.....	5-3
5.8	Email Procedures for Sending Emails to Non-Departmental Staff.....	5-4
5.9	Text Messaging Procedures	5-6
5.10	Facility Security and Protecting PHI.....	5-7

SECTION 6 - DISCLOSURES

6.1	Verification of Patient Identity	6-1
6.2	Documenting Disclosures in the Electronic HIPAA Log “e-HIPAA Log”	6-2
6.3	Redaction of PHI	6-2

SECTION 7 - OTHER REQUIREMENTS RELATED TO USE AND DISCLOSURE OF PHI

7.1	Procedure for External Audits and Investigations	7-1
7.2	Limited Data Sets.....	7-1
7.3	Data Use Agreement.....	7-2
7.4	Business Associate Agreements	7-3
7.5	Students/Volunteers/Interns with Access to PHI.....	7-3
7.6	Visitors in Workplace	7-4

SECTION 8 - DOCUMENT RETENTION AND STORAGE

8.1	Digital Copy Machines	8-1
8.2	Mobile and Portable Storage Devices.....	8-1
8.3	Laptop Inventory Procedure.....	8-3
8.4	Reporting Loss/Theft of Equipment or Data	8-4
8.5	Proper Disposal of PHI	8-4

SECTION 9 - REPORTS OF BREACHES OF CONFIDENTIALITY

9.1	Sanctions for Employees Violating Confidentiality.	9-1
9.2	Disclosures by Whistleblowers.....	9-3
9.3	Refraining from Intimidation or Retaliation.....	9-3
9.4	Students, Volunteers, Interns, or Externs.....	9-3
9.5	Business Associates	9-3
9.6	Mitigation of Harm Caused by Wrongful Releases of PHI	9-4
9.7	Employees Receiving Unauthorized Disclosures of E-PHI and PHI	9-5

SECTION 10 - TRAINING

10.1	Current Employees.....	10-1
10.2	New Employees	10-1
10.3	Students, Volunteers, Interns, and Externs	10-1

SECTION 11 - FORMS

- A. Electronic HIPAA Log “e-HIPAA Log”
- B. Request to Amend
- C. Request to Limit Protected Health Information
- D. Request for Accounting of Disclosures
- E. Amendment Acceptance – Notification Form
- F. BAA Flow Chart
- G. Data Use Agreement Flow Chart
- H. Fax Cover Sheet
- I. Workforce Tracking Form

SECTION 1 POLICY

1.1 Applicability

This policy is intended to implement and be read in conjunction with the Health Insurance Portability and Accountability Act (HIPAA) and implementation regulations found at 45 C.F.R. Sections 160 and 164. It also should be read in conjunction with the Department's current Employee Handbook, Employee Responsibilities in Responding to Legal Documents Policy, Professional Conduct Policy, and Information Security Manual. This policy is to be followed by all Departmental offices, bureaus, and divisions, and all county health departments.

1.2 Definitions

Unless otherwise specified, the definitions found in the HIPAA regulations are to be used in this policy.

1. "Authorization" a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment or health care operations, or to disclose protected health information to a third party specified by the individual.
2. "Confidential" the principle of keeping secure and private from others, information given by or about an individual in the course of a professional relationship.
3. "Department" includes all Departmental offices, bureaus, divisions, district offices, county health departments, and employees and volunteers.
4. "Business Associate" is a person or entity who creates, receives, maintains, or transmits personal health information for the Department.
5. "Disclosure" the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.
6. "E-HIPAA Log" is a database in Lotus Notes in which any requests for records that are not for treatment, payment, or operations are to be entered.
7. "Electronic Protected Health Information" (e-PHI) is any individually identifiable health information saved, produced, or transferred in electronic form.
8. "HIPAA" will be read to imply the appropriate portions of the statute or regulation.
9. "Privacy Officer" is the Departmental officer charged with the responsibility to ensure compliance with the privacy provisions of HIPAA.

10. “Personal Identifying Information” (PII) directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.), or which is intended to identify specific individuals in conjunction with other data elements (i.e., indirect identification). (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)
11. “Protected Health Information” (PHI) is any individually identifiable health information, including demographic data, held or transmitted by a covered entity. Common identifiers include: name, date of birth, social security number, diagnosis, and address.
12. “Security Officer” is the Departmental officer charged with ensuring compliance with HIPAA security provisions as it pertains to e-PHI.

SECTION 2

TREATMENT/PAYMENT/HEALTH CARE OPERATIONS

2.1 Treatment/Payment/Health Care Operations

Access to treatment and efficient payment, both of which require the disclosure of PHI, are essential to provide good health care. Additionally, certain health care operations are necessary to support treatment and payment. To avoid interfering with an individual's access to health care or the payment of health care, the Privacy rule permits a covered entity to use and disclose PHI for treatment, payment, and health care operations activities without the patient's consent. Examples include the following scenarios:

1. A health care provider may provide a copy of a patient's medical record to a health care specialist who needs the information to treat the patient.
2. A health care provider may disclose PHI about an individual as part of a claim for payment to a health plan.
3. Information may be disclosed to conduct quality assurance activities and case management.

Note: A patient's consent is required to disclose PHI to obtain social services.

SECTION 3 PATIENT RIGHTS

3.1 Notice of Privacy Practices

The Notice of Privacy Practices (NOPP) has been revised to comply with 2013 amendments to the HIPAA Federal Regulations. Employees must ensure that only updated notices are provided to patients/clients.

The NOPP must be posted in a conspicuous location within each county health department, laboratory, and any bureau or division that serves the public. Each page shall be visible. A copy of the current NOPP is located in the Document Library and can be found on the Department web site at:

<https://www.alabamapublichealth.gov/blog/assets/privacypractices.pdf>

3.2 Patient/Client Access to View PHI in Their Records or in Designated Record Sets

A patient/client has the right to access PHI in their designated record set. Designated record sets include, at a minimum, the patient's medical and billing records maintained by the Department. A patient/client must be allowed to view his or her PHI in a secure and non-obtrusive manner within the clinic and to request to have corrections made if they can demonstrate that the information in the record is inaccurate. This section addresses those requests. It does not address requests by others, even on behalf of the patient/client, such as attorneys or other representatives. **Requests made by individuals other than the patient/client should be reported to the Office of General Counsel for approval prior to the release of the requested records.**

Exception:

Psychotherapy Notes. A patient does not have the right to access psychotherapy notes relating to himself or herself, except:

1. To the extent the patient's treating professional approves such access in writing.
2. The patient obtains a court order authorizing such access.

Note: State and Federal Subpoena Information

Alabama law does not recognize social workers as mental health professionals. Therefore, social worker notes may be produced to an Alabama state court as they are NOT considered psychotherapy notes.

Federal law recognizes social workers as mental health professionals. If a federal subpoena is received, social worker notes are NOT to be provided.

Requests made by a patient/client to view their own record may be made in person or in writing. If the request is in writing, there is no particular form required; however, the statement must be both signed and dated by the patient/client and contain all of the items listed below:

1. A request to view the records.
2. The name of the patient/client clearly documented.
3. A statement of the specific records requested to be viewed.
4. The date and time when the viewing is proposed.

Written Requests. Written requests should be followed up by records personnel establishing an appropriate time for viewing. Written requests should be documented in the e-HIPAA Log and the applicable progress note.

Oral Requests. Oral, in person requests should be documented in the e-HIPAA Log and the applicable progress note.

Requests to view records should be granted by the appropriate person when the identity of the patient/client is established. If a patient indicates that he or she has been treated by more than one clinic, the clinic that received the request should immediately forward a copy of the request to the other clinic(s) designated by the patient. The purpose is to assist the patient with their request when they have been treated at multiple health department clinics and minimize any burden on the patient to access their records.

If the patient does not request access from any other clinic, the clinic that received the initial request should process the request and send a copy of the request form to the Privacy Officer. If the clinic has any concern or question regarding whether to comply with the request, the Privacy Officer should be consulted immediately. Any denial of a request to view records must be done in writing with prior approval from the Privacy Officer.

A patient's request for access to PHI must be acted upon as soon as reasonably possible, but not more than 30 days after receiving the request.

The Office of General Counsel must be notified if a patient requests access to his or her PHI for litigation or some other unusual purpose.

Process for Viewing Records. Viewing shall only be allowed for the patient requesting to view their information. At the date and time for viewing, the requestor should be properly identified. Reasonable time should be given to the patient/client to view and make notes from the record. Copies may be made for the patient/client for the usual and

customary charge as established in other policies. Records must not be removed from the secure area. The patient/client should be monitored by appropriate personnel to make sure the record is in no way altered by addition or deletion of any information or by any marks by the patient/client. Viewing must be noted in the e-HIPAA Log and the applicable progress note.

Denial of Right to Access. A patient/client may be denied access under the limited circumstances listed below. Denials should be noted in the progress notes and the e-HIPAA Log. The following exceptions should be narrowly construed and rarely used:

1. Inmate Information. The Department, acting under the direction of a correctional institution, may deny, in whole or in part, an inmate's request to obtain a copy of PHI. This denial may occur if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the patient or of other inmates, or the safety of any officer, employee, or other person at the correctional institution responsible for the transporting of the inmate.
2. Information from Other Source. The Department may deny a patient's access to PHI if the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
3. Endangerment. The Department may deny a patient access in the event a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person. Access may not be denied on the basis of sensitivity of the health information or the potential for causing emotional or psychological harm.
4. Reference to Other People. The Department may deny a patient access if the PHI makes references to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person. Access can be denied if the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm to the other person.
5. Personal Representative. The Department may deny access if the request is made by a patient's/client's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.
6. Psychotherapy Notes. The Department may deny access to psychotherapy notes if: (1) the patient's treating professional does not approve access in writing, and (2) the patient does not have a court order authorizing such access.

The Department must, to the extent possible, give the patient/client access to any other PHI requested, after excluding the PHI to which access is being denied.

Unless an exception applies, including the exceptions previously stated in this policy, a patient/client should be granted access to the entire medical record, including records received from other providers that were used to make treatment decisions.

3.3 Access to Laboratory Reports

Patients, patient's designees, or patient's personal representative can be provided a copy of the patient's lab report, including an electronic copy, with limited exceptions. The Bureau of Clinical Laboratories has been provided specific guidance on the procedures for disclosure. Requests for laboratory records must be in writing and copies should be provided within 30 days of the patient's request.

3.4 Amendment to Patient's/Client's Protected Health Information

The Department will permit patients to request amendments to their PHI, or a particular record, contained in a designated record set.

Requests to amend or in any way alter patient/client PHI must be made in writing by completing **FORM B: Request to Amend Protected Health Information**. All requests must be recorded as a progress note in the file and entered on the e-HIPAA Log.

If the request is for an amendment other than a name change due to marriage or divorce, the request shall be evaluated by appropriate personnel and a recommendation made to the Privacy Officer for consultation. The Privacy Officer shall advise and the final decision on whether to grant the request is to be made by appropriate clinic personnel no later than 30 days after receipt of a request. Notice of the decision must be given to the requestor in writing. Copies of responses to requestors must be placed in the client's/client's file and recorded in the e-HIPAA Log. Amendments to the record must be made only by appropriate personnel, all of which must be documented in the patient's file as a progress note and recorded in the e-HIPAA Log.

The Department may deny a patient/client request for amendment, if it determines that the PHI or record that is the subject of the request is any of the following:

1. The record was not created by Department personnel.
2. The record is not available for inspection by the individual pursuant to their right to access.
3. The record is accurate and complete.

A clinic, bureau, or division that is informed by another covered entity of an amendment to a patient's PHI must amend the PHI in designated record sets.

Requests for amendments, and documentation of the response to such requests, must be maintained in a patient's/client's medical record for a minimum of six (6) years.

3.5 Requests by the Patient to Limit Releases of PHI

Patients/clients have the right to make reasonable requests to limit the release of PHI. Requests should be made in the same manner as requests to alter or amend PHI. They must be made in writing by completing **FORM C: Request to Limit Protected Health Information**. Requests to limit or restrict information will not apply to entities required to receive the information as mandated by law (i.e. public health oversight, protection of the President of the United States, qualifying government agencies, investigating complaints of abuse or neglect).

The Department is not required to agree to any request to limit or restrict the use and disclosure of PHI. However, if the Department agrees to a restriction, it may not use or disclose PHI in violation of the restriction, except in emergency situations when the PHI is needed to treat the patient. If restricted PHI is disclosed to a health care provider for emergency treatment, the clinic disclosing the information must request that the health care provider that received the information not further use or disclose the information.

The Department may not disclose PHI subject to a restriction, except to provide emergency treatment or unless required by law or regulation.

Documentation of all such requests and actions taken must be entered in the progress notes and in the e-HIPAA Log. The Privacy Officer will make the final determination about whether a restriction will be granted within 30 days of the request. The request form must be maintained in the patient's medical record for a minimum of 6 years.

Requests for restrictions should only be granted in rare instances in which the facts and circumstances indicate such a restriction is necessary to protect the patient.

A restriction on the use and disclosure of PHI can be terminated if:

1. The patient requests the termination in writing.
2. The patient orally agrees to or requests the termination and the oral request or agreement is documented in the patient's medical record and communicated to the Privacy Officer.
3. The Department informs the patient that it is terminating its agreement to a restriction.

If the restriction is granted, a clinic must mark the restriction in the patient's medical record and the e-HIPAA Log.

3.6 Requests by the Patient/Client for an Accounting of PHI

Patients/clients have the right under HIPAA to make reasonable requests for an accounting of the non-routine releases of PHI to other parties. Requests for such should be granted when appropriately made and not otherwise restricted by HIPAA.

Documentation of all such requests for accounting must be entered in the progress note and in the e-HIPAA Log.

The accounting must include all disclosures made by a clinic in the six (6) years prior to the date of the request (unless limited at the request of the patient), including disclosures to or by business associates. *The first accounting provided to a patient/client in a calendar year shall be free of charge to the patient/client.*

Accounting Requirements. The accounting must include all disclosures, except for the following:

1. To carry out treatment, payment, and health care operations.
2. Incident to a use or disclosure otherwise permitted or required by the Privacy Regulations.
3. Pursuant to the patient's authorization.
4. For national security or intelligence purposes.
5. To correctional institutions or law enforcement officials to provide them with information about a person in their custody.
6. As part of a limited data set.
7. Incident occurred prior to the compliance date.

Examples of disclosures subject to the accounting requirement include disclosures for, or pursuant to: (1) research, unless authorized by patient; (2) subpoenas, court orders, or discovery requests; (3) abuse and/or neglect reporting; or (4) communicable disease reporting.

1. Verification of the requester's identity must be obtained prior to granting the request for an accounting.
2. Any clinic that receives a request for an accounting of disclosures must provide the patient with **FORM D: Request for Accounting of Disclosures**.

3. If a patient indicates that he/she has been treated by more than one clinic, the clinic that received the request must immediately forward a copy of the request to the other Department clinics designated by the patient. If the patient does not request an accounting from any other clinic, the clinic that received the initial request must process the request and send a copy of the request form and copy of the accounting of disclosure form to the Privacy Officer.
4. Clinics must designate a custodian of records and appropriate designee who will be responsible for processing requests for accountings or disclosures and recording the same on the e-HIPAA Log.
5. For each disclosure that must be recorded, the accounting must include the following information:
 - a. The date of the disclosure.
 - b. The name of the entity or person who received the PHI and, if known, the address of such entity or person.
 - c. A brief description of the PHI disclosed.
 - d. A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure.
6. A copy of the Request for Accounting of Disclosures Form must be forwarded to the Privacy Officer and will be maintained for six (6) years.
7. If, during the period covered by the accounting, a clinic has made multiple disclosures of PHI to the same person or entity for a single purpose, or pursuant to a single authorization, the accounting may, with respect to such multiple disclosures, provide:
 - a. The information set forth in Section 5 above for the first disclosure during the accounting period.
 - b. The frequency, periodicity, or number of the disclosures made during the accounting period.
 - c. The date of the last such disclosure during the accounting period.
8. The Department must act on the patient's request for an accounting no later than 30 days after receipt of such request.

Suspension of Accounting. A patient's right to receive an accounting of disclosures may be suspended at the request of a health oversight agency or law enforcement official if certain conditions are satisfied. If a clinic receives a request to suspend patient's right to receive an accounting from a health oversight agency or law enforcement official, the Privacy Officer must be contacted by email to determine if the appropriate conditions have been satisfied.

3.7 Requests for Alternative Means of Communication

Department clients/patients may sometimes request that staff communicate with them in a specific manner by using a specific phone number or mailing location. The Department must accommodate any reasonable request. A request for alternative means of communication must be noted in the progress notes and the Authorization for Services and Billing.

3.8 Requests for Patient/Client Information Regarding Research and Marketing

Any request made to the Department requesting PHI for research or marketing purposes should be forwarded by email to the Privacy Officer within 2 days of receipt. With the exception of approvals made by the Department's Institutional Review Board (IRB), no requests should be acted upon until written permission by the Privacy Officer has been provided.

3.9 Requests for Information of Deceased Patients/Clients

While information regarding deceased patients/clients can still be provided for approved research purposes or in some instances with a valid authorization from their personal representative or through a court order, information on individuals who have been deceased for a period of longer than 50 years is no longer considered PHI.

SECTION 4 MINIMUM NECESSARY RULE

The Department holds the PHI of its clients and patients in trust to be used only in their best interest or as otherwise required by law. Thus, when using or disclosing PHI or requesting PHI from another covered entity, the Department will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This includes requests made on a routine and recurring basis.

4.1 Minimum Necessary Disclosures and Access

The Department may not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary for another entity to accomplish the purpose of the use, disclosure, or request.

Department personnel who are directly involved in a patient's treatment and care (e.g., physicians, nurses, social workers, and appropriate clerical staff) or employees who require full access to the record to perform their job functions (e.g. auditors) may have access to a patient's entire record. Department personnel who are not directly involved in a patient's treatment may not have unlimited access to a patient's PHI. It is a violation of the minimum necessary rule for a health care provider to access the PHI of patients with whom the provider has no treatment relationship, unless for research purposes as permitted by the Privacy Regulations and Departmental Policy.

Each Bureau Director, District Administrator, or their designee must assign at least one individual per bureau or location, to perform a quarterly review of user access logs for systems that contain PHI. The assigned individuals should work with the Information Security Officer to determine which systems need to be reviewed and develop a procedure for their access log reviews. The reviews should be completed in conjunction with the quarterly ADPH HIPAA Privacy and Security Risk Assessment/Compliance Walkthroughs referenced in section 5.10. The forms can be found in the Document Library.

Department personnel may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when: (a) making disclosures to public officials as required by law, if the public official represents that the information requested is the minimum necessary for the stated purpose; (b) the information is requested by another covered entity; (c) the information is requested by an employee of the Department or a business associate of the Department providing professional services, if the employee or business associate represents that the information is the minimum necessary for the stated purpose(s); or (d) documentation submitted by a researcher that the information is preparatory to research, related to research on a decedent, or the disclosure has been approved by the Department IRB or cleared by the DOAR Committee.

4.2 Situations in which the Necessary Rule Does NOT Apply

The minimum necessary rule does not apply in some instances. Those instances are listed below:

1. Disclosures to, or requests by, a health care provider for treatment.
2. Uses or disclosures made to the patient.
3. Uses or disclosures made pursuant to an authorization.
4. Disclosures made to the Secretary of the U.S. Department of Health and Human Services for compliance and enforcement of the Privacy and Security Regulations.
5. Uses and disclosures required by law.
6. Uses and disclosures required for compliance with HIPAA standardized transactions.

With respect to business associates of the Department, the Department will limit the PHI disclosed or requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

SECTION 5 GENERAL STANDARDS FOR HANDLING PHI

5.1 Face-to-Face Discussions

Employees must take reasonable steps to protect the privacy of all face-to-face discussions of PHI, whether inside or outside of the office. When possible, employees should use enclosed offices or interview rooms for discussions involving PHI. If enclosed offices or rooms are not available, employees should take reasonable precautions to ensure that their conversations are not overheard. In all cases, discussions of PHI should be limited to only that PHI which is necessary to conduct the business at hand.

Employees must ensure that devices such as Alexa, Siri, Google Nest, or any other voice assistant cannot hear and record discussions that involve PHI.

5.2 Telephone Calls

Before discussing PHI over the telephone with a patient, employees must confirm his or her full name, date of birth, and social security number.

Employees must honor any previously authorized requests by the patient to use alternative means of communications.

Telephone calls should be made in private locations where possible. The employee should be aware of their surroundings and take reasonable precautions to ensure the conversation is not heard by nearby persons.

If the employee reaches the patient's voicemail and leaves a message, the message should only include the name of the health department, and name and phone number of the person to be called back. No other information, such as the name of the program from which the employee is calling or the fact that test results have been received should be disclosed, since that may compromise patient confidentiality if someone else retrieves the message.

5.3 Visual Access to PHI Displayed on Computer Screens

Employees must ensure that PHI displayed on computer screens is adequately shielded from view by unauthorized persons. Polarized screens or other screen overlay devices that shield information on the computer screen should be used when possible.

Computer workstations must be locked when not in use, and PHI must be cleared from the screen when it is not being used.

Laptop computers, mobile devices, and other electronic storage devices containing PHI must be stored in a secured location at all times.

Secure locations are places such as locked offices, locked desk drawers, or a user's home. A locked car or trunk is NOT considered a secure location.

5.4 Paper Records and Files

Department employees who work with PHI must be aware that they are working with sensitive information and that the information must be kept in a secure manner. Therefore, at the end of the work day, individuals who have utilized records containing PHI must ensure that the records are not left unattended at their work stations and that the information is locked away to prevent access by non-Departmental employees or employees who do not have a work related need to know the information. Additionally, employees are not allowed to take records outside of their work location without prior supervisor approval.

Medical records storage locations must be kept secure at all times. Several methods exist to ensure the security of these records including, but not limited to, traditional key access, swipe card access, and keypad access. Automatic store room closers must also be utilized. Medical records must not be kept in storage sheds protected by a single lock, nor should they be stored in an equally unsecured location.

5.5 Outgoing Mail

Hand-mail containing PHI should be mailed in a sealed envelope or other secure container, properly addressed to the recipient with the words "Confidential" on the outer envelope or package.

Mail that is delivered outside the ADPH courier service containing PHI should be mailed first-class in a sealed envelope or other secure container, properly addressed to the recipient with the words "Confidential" on the outer envelope or package. As budgets allow, it is recommended that PHI be mailed certified mail, return receipt.

All outgoing mail containing PHI must have a return name and address on the outer envelope, so that misdirected mail can be returned to the sender.

5.6 Faxing

Faxing of PHI is permitted but not recommended. Faxing of PHI is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of PHI.

In the event that a fax is sent to the wrong recipient, follow these steps:

1. Fax a notice to the incorrect fax number explaining that the information has been misdirected and ask for confirmation in writing that the information has been destroyed.
2. Immediately document the incident by filing an ARIA report and call to notify the Privacy Officer at 334-206-9324. Finally, verify the fax number with the recipient before attempting to fax the information again.

ALL faxes that contain PHI must use **Form H** as a fax cover sheet.
You must include a contact person's name and phone number.

5.7 General Email Procedures

ADPH provides certain employees with a Lotus Notes email account for conducting Departmental business. The following must be done to allow users to use email safely and effectively:

1. Change the email default password.
2. Employees should check their email each business day.
3. When sending an email, ALWAYS verify the recipient's address, and make sure that it is entered correctly before clicking send.
4. When sending a message to an email group, always review the recipients in the group. Remove any recipient who should not receive your email. Always review email groups to make sure recipients are current.
5. Do NOT add ADPH employee email or group accounts to your personal address book.
6. If an email that contains PII or PHI is sent to the wrong recipient, notify the Lotus Notes Administration team IMMEDIATELY. A Privacy and Security ARIA report must be completed.
7. The size limit for an outgoing email is 25 megabytes.
8. To send a file larger than 25 megabytes, consider using the Department's secure FTP site. Contact the Support Desk for assistance if needed.

9. If a message could be perceived as ADPH business or opinion, add a disclaimer to the signature block when not officially representing ADPH.
10. Although the use of the Lotus Notes system to occasionally send personal emails is not prohibited, you should consider whether the content of the email is appropriate to send from your Department email account. Also, remember there is no privacy when using the Lotus Notes System. Email within the system is Departmental property. As such, all email is subject to review by appropriate personnel.
11. Employees must NOT use their ADPH email account or password for personal business in conjunction with commercial websites.
12. If you receive an email that appears to be fraudulent, contact the Support Desk. DO NOT FORWARD THE EMAIL.
13. If you believe that your Department email address has been spoofed (when an email header has been forged using your email address as the sender), contact the Support Desk.
14. Text messages sent from your Lotus Notes account should be for Departmental business only. Like email, text messages are also subject to review by appropriate personnel.
15. Text messages should not contain any personal or health information, which includes the patient's name, date of birth, address, appointment type, diagnosis, medication, or any other PII or PHI.

5.8 Email Procedures for Sending Emails to Non-Departmental Staff

Sending PHI by email exposes the PHI to two risks:

1. The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list.
2. The email could be captured electronically en route.

HIPAA requires that reasonable steps be taken to protect against these risks but acknowledges that a balance must be struck between the need to secure PHI and the need to ensure that clinicians can efficiently exchange important patient care information. You must continue to observe the following rules:

1. All Department or work related emails must be sent using Lotus Notes.
2. Limit the information you include in an email to the minimum necessary for your clinical purpose.

3. When sending an email that contains PHI, you MUST:
 - Add the word “CONFIDENTIAL” to the subject line
 - Force encryption by adding [Encrypt] in the subject line when emails are sent outside ADPH email system, or when responding to an unencrypted email that contains PHI.
4. Whenever possible, avoid transmitting highly sensitive PHI (for example, mental health, sexually transmitted disease, or HIV information) by email.
5. Never use automatic forwarding with your Department email account.
6. Never send PHI by email unless you have verified the recipient’s address (for example, from a directory or a previous email) and you have checked and double-checked that you have entered the address correctly. If you are using an email group, make sure to exclude any recipients in the group to whom you should not send PHI.
7. Never send e-PHI to a personal email address without written permission from the patient on appropriate ADPH forms or permission from the Privacy or Security Officer.
8. Never send or forward an email that contains PHI to your own personal email address.
9. Always include a privacy statement notifying the recipient of the insecurity of email and providing a contact to whom a recipient can report a misdirected message.

Required Privacy Statement: *“This email message contains CONFIDENTIAL medical communications. This message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.”*

Sending emails between Lotus Notes Users. All employees may continue to send PHI within Lotus Notes to other Lotus Notes users. (Ex. county health department staff can continue to communicate PHI through Lotus Notes emails to employees in the bureaus and other county health departments.) You must put “Confidential” in subject line.

Sending emails to employees at the Jefferson County Health Department (@jchd.org) or the Mobile County Health Department (@mchd.org): These email addresses are considered outside of the Department for encryption purposes. You must follow the directions in No. 3 above to ensure the confidentiality of the information being sent.

Sending Emails to Patients. The Department may send unencrypted emails to patients. Patients have the right to receive PHI or other sensitive information via unencrypted e-mail. However, the risks of sending and receiving unencrypted emails must be explained to the patient, and he or she must have opted out of receiving encrypted emails on the Authorization for Services and Billing or applicable Home Health Authorization for Services and Billing. The relevant section of the Authorization for Services and Billing pertaining to emails must be completed prior to communicating with the patient through email in this manner. The consent must be updated at each patient visit.

5.9 Text Messaging Procedures

1. The text messaging function in Lotus Notes should only be used to send messages on behalf of ADPH. **Do not use to text personal messages.**
2. Text messages to patients about their appointments can only come from your Lotus Notes work email.
3. Make sure that the patient has marked the Authorization for Services and Billing indicating that they would like to receive text message reminders.
4. Enter “Cell Number” as a 10-digit number (Ex.) 5551234567@txt.att.net.
5. Double check the phone number and address to ensure that you have typed in the correct criteria.
6. Do not use the patient’s name or any other identifiers (date of birth, social security number, medical record number, etc.) in the text message.
7. Diagnosis information cannot be provided to the patient via text message.
8. Do not copy “cc” or blind copy “bcc” to a text message appointment reminder.
9. Only inform the patient about their appointment date, time, and place. Do not mention health conditions, medications, or vaccines in the subject line or text message.

Use the following cell phone provider SMS email addresses to send text messages:

AT&T: cellnumber@txt.att.net
Verizon: cellnumber@vtext.com
T-Mobile: cellnumber@tmomail.net
Sprint PCS: cellnumber@messaging.sprintpcs.com
Virgin Mobile: cellnumber@vmobl.com
US Cellular: cellnumber@email.uscc.net
Nextel: cellnumber@messaging.nextel.com

Boost: cellnumber@myboostmobile.com
Alltel: cellnumber@message.alltel.com
Mint Mobile: @tmomail.net
Cricket Wireless: @mms.cricketwireless.net
Consumer Cellular (AT&T): @mms.att.net
Consumer Cellular (T-Mobile): @mailmymobile.net
Metro PCS: @mymetropcs.com
Xfinity: @vtext.com
Google Fi: @msg.fi.google.com

Texting Appointment Reminders. While appointment reminders are considered to be an aspect of “treatment,” HIPAA requires appropriate safeguards for confidential information that is transmitted electronically, typically encryption. However, text messages are transmitted over wireless networks which may or may not be secure. Therefore, prior to sending text message appointment reminders, patients must specifically indicate on the Authorization for Services and Billing that they will accept appointment reminders via text message and must provide the phone number and service where they would prefer the text message be sent. (Ex. 5551234567@txt.att.net)

Appointment reminders must not be sent to a patient from an employee’s personal cell phone.

5.10 Facility Security and Protecting PHI

The secure handling of PHI involves protecting the locations where PHI is kept, whether in paper form or electronic form. To ensure the protection of PHI within a facility, the following safeguards and procedures must be implemented and followed where applicable.

1. All ADPH facilities must have written facility security procedures.
2. Facility security procedures should include, but are not limited to:
 - a. Protection of mobile and portable systems, such as laptops or handheld devices including items, but not limited to:
 - i. Secure storage of sensitive data;
 - ii. Access to system(s), application(s), and data in the event of theft; and
 - iii. Encryption of data, passwords, and other sensitive information.
 - b. Locking doors during non-business hours with limited access.
 - c. Locking buildings.
 - d. Use of a swipe card, personal password, or personal identification number (PIN) for building access by each individual with authorization to access sensitive data.
 - e. Documentation of the use and distribution of keys and swipe cards to the building.
 - f. No duplication of keys.
 - g. Use of fence, well-lit with security lights.

- h. Use of security guards or cameras for fence.
- i. Use of combination locks.
- j. Monitor security alarm systems.
- k. Secure equipment access.
- l. Security monitoring.
- m. Security system – access limited to personnel with keyless coded entries.
- n. Documentation of lost keys or swipe cards.
- o. Do NOT leave doors propped open.
- p. Completing custodial work or maintenance work during business hours if ADPH staff cannot be present to escort and supervise the work.
- q. Confidentiality agreements with non-ADPH custodial workers and maintenance workers.
- r. Non-ADPH custodial workers and maintenance workers must be restricted from accessing areas where PHI/PII is stored unless an ADPH staff member is present to escort and supervise the worker(s).
- s. Completion of a quarterly ADPH HIPAA Privacy and Security Risk Assessment/Compliance Walkthrough form.

SECTION 6 DISCLOSURES

Prior to making any permitted disclosure of PHI, you must verify the identity of the person requesting the PHI and the authority of such person or entity to receive such disclosure. Obtain any documentation, statements, or representations that are a condition of the disclosure from the person or entity making the request.

6.1 Verification of Patient Identity

Any questions regarding verification or reliance on identity or authority should be directed to the Office of General Counsel. The Office of General Counsel must be contacted prior to responding to any request by law enforcement or prosecutorial officials, if possible.

Prior to making a disclosure or processing a patient request permitted by this Policy, Department personnel must consider and comply with both items listed below:

1. Verify the identity of a person requesting PHI and the authority of any such person to have access to PHI, if the identity or any other such authority of such person is not known to the Department staff member processing the request.
2. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting PHI when such documentation, statements, or representation is a condition of the disclosure or processing.

After consultation with the Office of General Counsel, the Department may rely on the items listed below to release records:

1. An administrative request, including a HIPAA compliant administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used.
2. Appropriately executed documentation of an IRB or Department Overview and Approval of Research (DOAR) Committee waiver or alteration of the authorization requirement.
3. A request by a public official upon presentation of his/her badge or other official credentials if in person or on appropriate letterhead if the request is in writing.

6.2 Documenting Disclosures in the Electronic HIPAA Log “e-HIPAA Log”

Each office, clinic, and bureau that provides hands-on health care shall utilize the Department’s electronic HIPAA Log (e-HIPAA Log). Access to the link for the e-HIPAA Log shall be limited to appropriate record clerks, supervisory personnel, or employees who require access to make reports.

Employees that enter requests in the e-HIPAA Log should be familiar with and reference the policy, Employee Responsibilities in Responding to Legal Documents.

The log shall be used to document the disclosure of certain non-routine PHI releases as detailed below. In addition, each of the non-routine releases of PHI listed below shall be noted in the appropriate patient/client file and shall be cross referenced to the e-HIPAA Log. The e-HIPAA Log shall be used to document the items listed below:

1. Unauthorized releases of PHI. These unauthorized releases must be documented in the ARIA System. (To complete an ARIA report, log in to www.alabamapublichealth.gov).
2. Authorized releases based upon subpoena or judicial process.
3. Third party authorizations.
4. Authorized releases to law enforcement, national security, public health disease control, jail or prison officials, death disclosures, emergencies, abuse investigatory agencies, and research.
5. Requests to limit releases of PHI.
6. Requests to view PHI.
7. Requests to amend or correct PHI.
8. Requests for accounting of PHI.

Instructions on access to the e-HIPAA Log are attached as “**Form A.**”

6.3 Redaction of PHI

1. After reviewing the requested record and determining that it contains information that must be redacted, the custodian of records shall make a paper or electronic copy of all pages containing the *restricted* information. The custodian of records shall then color over the restricted information on the reproduced copy with a black marking pen in a neat manner or by using the redaction tool in Adobe.

2. The custodian of records shall then reproduce a copy of the page(s), which shall be the page(s) that is released to the requester.
3. If the redaction was done with a black marking pen, the custodian of records shall then dispose of the first copy by shredding or placing in a secure shredder bin.
4. The custodian shall ensure that the restricted information is not visible on the copy.

SECTION 7

Other Requirements Related to Use and Disclosure of PHI

7.1 Procedure for External Audits and Investigations

Individuals requesting PHI for the purpose of performing an audit or investigation must meet HIPAA requirements in order to access PHI held by the Department. If a non-Departmental staff member requests to view PHI to perform an audit or investigation, you should take the steps listed below:

1. Ask for a copy of their badge and business card.
2. Notify your supervisor who will contact the Office of General Counsel and provide them with a copy of the badge and business card.
3. Approval must be granted prior to allowing access to PHI.

Do not provide external auditors or investigators access to your passwords or log in information. If access to Department systems is necessary, the Security Officer must be notified and will work to develop a means of access to necessary systems.

7.2 Limited Data Sets

A clinic or bureau may use and disclose a limited data set without patient authorization only for the purposes of research, public health oversight, or health care operations if the clinic or bureau enters into a data use agreement with the intended recipient of the limited data set.

A clinic or bureau may use PHI to create a limited data set, or disclose PHI to a business associate to create a limited data set on behalf of the clinic or bureau.

If a clinic or bureau is aware of a pattern of activity or practice of the limited data set recipient that constitutes a material breach, it must seek to end the violation, as applicable, complete an ARIA report, and contact the Office of General Counsel. If such steps are unsuccessful, the clinic or bureau must discontinue disclosure of PHI to the recipient and report the problem to the Office of General Counsel.

A limited data set is PHI that does not directly identify the patient, but which contains potentially identifying information.

Creating a Limited Data Set. In order to create a limited data set, the following direct identifiers of the patient or of relatives, employers, or household members of the patient must be removed:

1. Names
2. Postal address information, other than town, city, state, and zip codes
3. Telephone numbers
4. Fax numbers
5. Email addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voiceprints
16. Full-face photographs and comparable images

The patient's date of birth should only be disclosed if the Department and the recipient of the information agree that it is needed for the recipient's purposes.

7.3 Data Use Agreements.

All data use agreements must be approved by the Office of General Counsel prior to execution. The agreement must be entered into the contract database as a Memorandum of Understanding with an email approval from the Office of General Counsel attached. A flowchart to assist employees with understanding whether a Data Use Agreement is necessary is attached as "**FORM G**" and the template can be located in the contract system library.

A Data Use Agreement must:

1. Establish the permitted uses and disclosures of the limited data set.
2. Establish who is permitted to use or receive the limited data set.
3. Provide that the recipient of the information will:
 - a. Not use or further disclose the information other than as permitted by the agreement.
 - b. Use appropriate safeguards to prevent use or disclosures other than as permitted by the agreement.
 - c. Report to the Department any uses or disclosures the recipient is aware of that is not provided for by the agreement.
 - d. Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient.
 - e. Not seek to identify or contact patients.

7.4 Business Associate Agreements

The HIPAA Rules require that covered entities and business associates enter into a Business Associate Agreement (BAA) to ensure that business associates will appropriately safeguard PHI. A business associate may use or disclose PHI only as permitted or required by its BAA or as required by law.

As of 2013, business associates are directly liable under the HIPAA Rules and subject to civil and criminal penalties for making uses and disclosures of PHI that are not authorized by agreement or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard (e-PHI) in accordance with the HIPAA Security Rules.

A flowchart to assist employees with understanding whether a BAA is necessary is attached as “**FORM F**” and the template and cover letter can be found in the contract database library.

7.5 Students/Volunteers/Interns with Access to PHI

The Department will identify those students and volunteers, as appropriate, in its workforce that need access to PHI to carry out their duties. **Only students, volunteers, and interns who have been identified, reviewed the HIPAA policy, and trained on HIPAA Privacy and Security shall be permitted access to PHI.** Refer to the Student Intern/Volunteer Policy for further guidance and instructions.

Interns must use Lotus Notes to send out any Departmental emails;
use of private email accounts is prohibited.

7.6 Visitors in the Workplace

Refer to the Workplace Visitor Policy.

SECTION 8 DOCUMENT RETENTION AND STORAGE

8.1 Digital Copy Machines

Copiers now come standard with hard drives installed. With the press of a button, jobs can be reprinted on demand. Many copiers allow users to reprint any job on the printed job list. Copiers that have a print-and-hold feature store the documents until someone erases them. In order to protect stored data on copiers from unauthorized disclosure, it is important to ensure that images stored are properly removed from machines upon completion of print jobs, when the device is transferred, becomes obsolete, or is no longer usable as a result of damage. *For more information on how the Department handles leased copiers, refer to the Departmental Copier Procedure located in the ADPH Security Manual.*

8.2 Mobile and Portable Storage Devices

Every member of the Department who utilizes a laptop computer, portable storage device, or mobile electronic device (e.g. Blackberry, flash drive, smart phone, tablet, hand held PC, hard drive, etc.) is responsible for the Department data stored, processed, and/or transmitted via that laptop or device, and for following the security requirements set forth in this policy and in the most current ADPH Security Manual.

Every Department staff member issued a laptop, tablet, smart phone, Blackberry, flash drive, portable storage device, or mobile device must use reasonable care to protect Department data as defined in the current ADPH Security Manual. Protection of confidential data against physical theft or loss, electronic invasion, or unintentional exposure include protections such as password authentication, encryption, and remote sanitization capability that work together to secure these devices against unauthorized access. ADPH employees who were issued Department devices **MUST** use them whenever accessing or transmitting confidential or sensitive data, since these devices will have the required data protections. For privacy and security reasons, it is also recommended that employees use Department issued devices whenever conducting business on behalf of ADPH.

Prior to the use or display of confidential data via laptop computer, portable storage device, or other mobile device, the following security measures must be in place or followed:

1. A laptop or other mobile device must require a password to authenticate the user. Mobile devices must be configured to timeout after 15 minutes of inactivity and require re-authentication before access to services on or by the device will be permitted. The authentication mechanism(s) must not be disabled.

2. Passwords must be a minimum of 14 alphanumeric and special characters, and they must be changed every 60 days. The storage of passwords in web browsers is prohibited. A password manager will be provided for users to store their passwords.
3. Encryption must be enabled on laptop computers that have encryption capability and that transmit confidential Department information, such as e-PHI. Laptops shall be protected with antivirus software and updated daily if supported by the device. NOTE: Lotus Notes email is protected with centralized anti-virus and anti-spam software. This protection may not apply to email systems outside of Lotus Notes.
4. Only Department employees are permitted to use Department issued devices. Department issued devices must NOT be allowed to be used by individuals not directly employed by the Department.
5. Personal storage devices, such as USB drives and portable hard drives, are prohibited for use on all Department computers and equipment. Exceptions must be approved by the Bureau of Information Technology. Contact the Support Desk for assistance if needed.
6. The use of any mobile devices, storage devices, or other electronics to transfer or store information from systems that access, store, or transmit e-PHI is strictly prohibited without authorization, regardless of whether the devices are owned or managed by the Department.

If authorized, ADPH staff members **MUST** use encrypted Department issued storage devices when transferring or storing e-PHI or sensitive data. Please contact the Security Officer or the Bureau of Information Technology with any questions.

7. All Department issued USB storage devices or portable hard drives that contain e-PHI, or other sensitive data **MUST** be encrypted. The use of unencrypted USB storage devices or portable hard drives that contain confidential or sensitive information is strictly prohibited, and any exceptions must be approved by the Privacy Officer or the Information Security Officer. If it is discovered that employees are downloading or otherwise storing confidential or sensitive Department data on unencrypted devices, disciplinary action and possible termination will occur.
8. Department owned portable hard drives must NOT be permitted to automatically “backup” the system they are plugged into and must be password protected and encrypted if accessing or storing e-PHI. Due to limited storage capability on servers, do not backup systems to Department servers.
9. The use of Cloud-based file storage and sharing services (Dropbox, Google Drive, and FTP sites) is prohibited unless they meet

the criteria outlined by the Alabama Office of Information Technology. For questions about their use, please contact the Support Desk for assistance.

10. The use of personal software or personal cloud-based software for conducting ADPH business is prohibited. The Department must hold the ownership and licenses for software used on its behalf.
11. Connecting personal devices including, but not limited to: laptops, tablets, smart phones, iPods, MP3 players, and gaming consoles to Department computers or the Department network is prohibited. Exceptions must be approved by the Bureau of Information Technology. Contact the Support Desk for assistance.
12. Visual and audio recordings within the clinic areas are strictly prohibited.
13. Using cameras or mobile devices to take pictures or videos of content displayed on computer monitors is strictly prohibited.
14. Using a smart speaker such as, Amazon Echo or Google Nest, is prohibited in ADPH facilities.

The Bureau of Information Technology can be contacted to determine if appropriate protections are already in place or assist with enabling the security measures for laptops or other electronic devices.

8.3 Laptop Inventory Procedure

ADPH staff members will have the time period from the fifteenth of each month until the end of each month to log their laptops into the network. This will allow the monthly inventory to run and ensure that the laptops have the most current Windows updates for that month.

An "Inventory Successful" pop-up notice will appear once the inventory has completed. The message will ask users to leave their laptops on and connected to the network for another hour. The laptop must stay on for at least 1 hour to ensure that all the Microsoft updates are downloaded and installed to the laptop.

There will be a Chronic Laptop Delinquency Report generated. This report will list all laptops that have not logged into inventory for 3 consecutive months. The list will be reviewed by designated IT staff, and then sent to bureau directors and property managers. The laptops on the list will be disabled from the network, and users will be notified of their delinquent status. Those laptops may be reviewed to determine if they are still needed by the staff member. If a staff member no longer needs the laptop, it must be returned to IT.

8.4 Reporting Loss/Theft of Equipment or Data

Department employees who possess Department owned laptop computers and other portable electronic or mobile devices are expected to secure them whenever they are left unattended. In the event a Department-owned or controlled laptop or other device is lost or stolen, the theft or loss must be reported immediately to your supervisor, your IT support personnel (if not available contact Help Desk), and the Department Privacy and Security Officers by filing an ARIA report. An ARIA report must be made within 24 hours of knowledge that the device is lost or stolen. If an employee loses a device during a weekend, they must report that device as lost or stolen the following business day.

8.5 Proper Disposal of PHI

HIPAA requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, in any form. This means that the Department must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. Employees are not allowed to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons.

Paper-based PHI must only be disposed of by utilizing a shredding machine or by placing the documentation in a secured shred bin. PHI must NOT be placed in a recycle bin. Floppy disks and compact disks (CD) may also be placed in secure shred boxes for disposal. Placing PHI, in any form, in a recycle bin, dumpster, or trashcan is considered a HIPAA violation.

SECTION 9 REPORTS OF BREACHES OF CONFIDENTIALITY

Breaches or suspected breaches of PHI must be reported immediately to the Privacy Officer by use of the ARIA System. Accompanying the completion of the ARIA, any additional information necessary to supplement the report must be emailed to the Privacy Officer. The Privacy Officer maintains a registry of breaches and suspected breaches and is responsible for overseeing each incident to a satisfactory conclusion. The reporter will be contacted by the Privacy Officer for follow up. All breaches found to be valid must be corrected, necessary retraining made, errant procedures corrected, and responsible employees disciplined. Where appropriate, remediation of harm may be required.

9.1 Sanctions for Employees Violating Confidentiality

Employees who negligently or willfully violate this policy shall be subject to disciplinary action. Additionally, the Department will work with appropriate authorities to seek the maximum penalty for employees participating in willful breaches of information.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at Levels 1, 2, 3, and 4 depending on the seriousness of the violation.

Level	Description of Violation
1	<ul style="list-style-type: none"> • Unintentional disclosure to covered entity.
2	<ul style="list-style-type: none"> • Repeated occurrence of Level 1 offense. • Accessing information that you do not need to know to do your job. • Intentionally granting access to or use of your computer, laptop, tablet, or other ADPH issued devices to an unauthorized person. • Sharing computer access codes (user name and password). • Leaving computer unattended while being able to access personal health information and/or personal identifying information. • Unintentional disclosure of sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security

	Officer, Privacy Officer, Chief Medical Officer, and/or authorized designee.
3	<ul style="list-style-type: none"> • Repeated occurrence of any Level 2 offense (does not have to be the same offense). • Failing to report potential HIPAA breach. • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name and password). • Failing/refusing to comply with a remediation resolution or recommendation.
4	<ul style="list-style-type: none"> • Repeated occurrence of any Level 2 offense (does not have to be the same offense). • Repeated occurrence of any Level 3 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or other.

Recommended Disciplinary Actions

In the event an employee violates ADPH's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Action
1	<ul style="list-style-type: none"> • Written Counseling. • Retraining on privacy/security awareness. • Retraining on ADPH privacy and security policies. • Retraining on the proper use of internal or required forms.
2	<ul style="list-style-type: none"> • Written Warning or Written Reprimand. • Retraining on privacy/security awareness. • Retraining on ADPH privacy and security policies. • Retraining on the proper use of internal or required forms.
3	<ul style="list-style-type: none"> • Written Reprimand or Suspension. • Retraining on privacy/security awareness. • Retraining on ADPH's privacy and security policies. • Retraining on the proper use of internal or required forms.
4	<ul style="list-style-type: none"> • Termination of employment. • Civil penalties as provided under HIPAA or other applicable federal/state/local law. • Criminal penalties as provided under HIPAA or other applicable federal/state/local law.

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. Bureau Directors and District Administrators shall work with the Human Resources Director to ensure consistency prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contractual relationship.

9.2 Disclosures by Whistleblowers

An employee shall not be subject to sanctions for the inappropriate disclosure of PHI if an employee believes in good faith that the Department has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Department potentially endangers one or more patients, workers, or the public; and the disclosure is to (i) a health oversight agency or other public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department; or (ii) an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards of misconduct by the Department.

9.3 Refraining from Intimidation or Retaliation

The Department may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any patient or other person for (i) filing of a complaint with the Secretary of the U.S. Department of Health and Human Services; (ii) testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing conducted by the Secretary of the U.S. Department of Health and Human Services; or (iii) opposing any act or practice made unlawful by this subchapter, provided the patient or person had a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule.

9.4 Students, Volunteers, Interns, or Externs who violate the Department's Privacy policies will not be permitted to provide further assistance to the Department.

9.5 Business Associates that demonstrate a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under his/her/its contract with the Department may have their BAA terminated by the Department. The Department will ensure that the business associate takes

reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, the Department shall:

1. Terminate the contract.
2. Report the problem to the Secretary of the U.S. Department of Health and Human Services or other applicable government agency.

Documentation regarding sanctions or discipline imposed for a violation of this Privacy and Security Policy must be retained in the employee's personnel file in written or electronic format, for at least 6 years post separation. Copies of such documentation should be forwarded to the Privacy Officer. Documentation of any sanction imposed against a business associate should be retained by the Privacy Officer for the minimum retention period of 6 years.

When imposing sanctions for the inappropriate use and disclosure of the PHI, the Privacy Officer will be involved in each case conference or other meetings regarding the incident to provide input. This inclusion will assist the Department in ensuring that employee discipline is handled in a consistent manner throughout the Department as it relates to HIPAA issues. The Privacy Officer and the Office of Human Resources may consider whether the use or disclosure was made as a result of: (a) carelessness or negligence, (b) curiosity or concern, or (c) the desire for personal gain or malice. The Department may report egregious and willful violations to the U.S. Department of Justice for appropriate action.

The Department will **not** impose sanctions against employees or business associates for: (a) engaging in whistleblower activities, (b) submitting a complaint to the Secretary of the U.S. Department of Health and Human Services, (c) participating in an investigation, or (d) registering opposition to a violation of the Privacy Regulations.

9.6 Mitigation of Harm Caused by Wrongful Releases of PHI

The Department will mitigate, to the extent practical, any harmful effect that is known to the Department resulting from the use or disclosure of PHI in violation of the Department's Privacy Policy by the Department, one of its clinics or bureaus or Department personnel.

In mitigating any potential harmful effects, the following procedure should be followed:

1. Clinics and bureaus must take all practical steps to mitigate the harmful affects of a confirmed inappropriate use or disclosure. The type of mitigation that occurs will be based on the facts and circumstances of each case based on the following factors:
 - a. Knowledge of where the information has been disclosed.
 - b. How the information might be used to cause harm to the patient or

- another individual.
- c. What steps can actually have a mitigating effect under the facts and circumstances of any specific situation.
2. Clinics and bureaus must investigate the cause of the inappropriate use and/or disclosure and take corrective actions to prevent such uses and/or disclosures from re-occurring.
 3. Clinics and bureaus must notify the Privacy Officer immediately so that the Privacy Officer can provide guidance related to inappropriate uses and disclosures, mitigation efforts, and investigation of the incident. If legal action is threatened, or is a consideration, the Office of General Counsel must be notified immediately upon such knowledge.

Where it is determined after investigation there was harm to a patient/client occasioned by a breach of confidentiality, the Privacy Officer shall recommend appropriate remediation which shall be made within the discretion of the administrator or director of the clinic or bureau which breached the PHI.

9.7 Employees Receiving Unauthorized Disclosures of E-PHI or PHI

If you receive an unauthorized disclosure in any form, i.e., fax, email, U.S. postal mail, or in any other form, that contains e-PHI or PHI, you must report it immediately to the Privacy Officer by use of the ARIA System. Accompanying the completion of the ARIA, any additional information necessary to supplement the report must be email to the Privacy Officer. The reporter will be contacted by the Privacy Officer and/or Security Officer for follow up.

SECTION 10 Training

It is mandatory that all employees receive HIPAA Privacy and Security Awareness training. In order to ensure all employees are given access to the training, the Workforce Tracking Form must be completed and routed to the Privacy and Security Officer, See **Form I**. This form will also ensure that all employees are checked to ensure compliance with the Office of the Inspector General for Health and Human Services monthly sanction checks.

- 10.1 Current employees** must view the current version of the HIPAA Refresher training regarding HIPAA compliance and electronically document completion. Employees must also view refresher training and other appropriate training produced by the Office of General Counsel.
- 10.2 New employees** must view the most current HIPAA Awareness and HIPAA Refresher training and electronically document completion.
- 10.3 Students, Volunteers, Interns, and Externs** must view current HIPAA Privacy and Security Awareness and Refresher training and electronically acknowledge completion.

COMPLAINTS/QUESTIONS

Any questions relating to this policy should be directed to the following individuals:

PRIVACY OFFICER

Pamela Kendrick, CHPC
201 Monroe Street, Suite 1540
Montgomery, AL 36104
334-206-9324
pamela.kendrick@adph.state.al.us

SECURITY OFFICER

Lori Earle, MBA, MISM, HCISPP
201 Monroe Street, Suite 1698
Montgomery, AL 36104
(334) 206-5010
lori.earle@adph.state.al.us

SECTION 11
FORMS



FORM A

ELECTRONIC HIPAA LOG “e-HIPAA Log”

The e-HIPAA Log shall be used to document non-routine disclosures of PHI. In addition, each of the non-routine releases of PHI listed below shall be noted in the appropriate patient/client file and shall be cross referenced to the e-HIPAA Log. The e-HIPAA Log shall be used to document the items listed below.

U	Unauthorized Release	DHR	Release to DHR	ER	Emergency Disclosure
SP	Subpoena/Judicial Process	NSA	National Security Release	J	Jail/Prison Officials
LE	Law Enforcement	P/GO	Release to Protect President/Officials	D	Death Disclosure
REQ	Request to Limit PHI Releases	AMD	Request to Amend/Correct PHI	VIE	Request for Viewing
ACCT	Request for Acct of PHI Releases	PH	Public Health Disease Control		

This does not include routine disclosures for:

**Release of records for Treatment, Payment, and Health
Care Operations.**

Instructions for accessing the e-HIPAA Log can be found in the Document Library.



FORM B

REQUEST TO AMEND
PROTECTED HEALTH INFORMATION

Patient Name: _____

Date of Birth: _____ SSN: XXX-XX- _____

Address where you want the amendment response sent:

NOTICE TO PATIENT: Your request to amend protected health information (such as health records, name, address, and social security number), in any form **only** applies to the information maintained by the Alabama Department of Public Health (hereinafter "ADPH"). If you would like to request amendments to your protected health information created and maintained by any other health care provider, a separate request must be submitted to that provider.

REQUESTED AMENDMENT:

I request that ADPH amend (describe the information you would like amended):

I request the amendment described above to be made to the protected health information in my designated record set (medical record) maintained or created by ADPH.

Date of record or information you would like to amend: _____

I would like this information amended because (state specific reason for request):

FOR AMENDMENTS: I am attaching proof that my record should be amended because it is false, inaccurate or incomplete. **PLEASE NOTE: No form will be considered unless you provide sufficient proof that the record that you intend to be amended is false, inaccurate, or incomplete.** [An example of an appropriate attachment would be your birth certificate to prove that the date of birth in your file is wrong]

[Signature/Title, if legal representative*]

Date

*May be requested to submit evidence of representative status.

REQUEST APPROVED:

If ADPH approves your request to amend your record, and we need to notify other persons or entities of the amendment to your protected health information, please complete the attached **FORM E** and return it to us.

REQUEST DENIED:

By: _____
Signature Title Date

Reason for Denial:

- The information was not created by ADPH.
- The information is not part of your Designated Record Set.
- The information is not available for your inspection pursuant to the ADPH's policy regarding individual access because _____
- The information is accurate and complete.

If your request for an amendment to your protected health information is denied, you may submit a written statement of your disagreement with the denial. Send the statement of disagreement to:

Privacy Officer
Alabama Department of Public Health
201 Monroe Street, Suite 1540
Montgomery, AL 36104
(334) 206-9324

After submitting your disagreement in writing, you will be given an opportunity for a hearing on why your request was denied. You will receive sufficient notice of the time and place that the hearing will be held.

*****Retain for minimum of 6 years*****



FORM C

**REQUEST TO LIMIT
PROTECTED HEALTH INFORMATION**

Patient Name: _____

Date of Birth: _____ SSN: XXX-XX- _____

Address where you want the amendment response sent:

NOTICE TO PATIENT: Your request to limit your protected health information **only** applies to the information maintained by the Alabama Department of Public Health (hereinafter "ADPH"). If you would like to request a limitation of your protected health information created and maintained by any other health care provider, a separate request must be submitted to that provider.

REQUESTED AMENDMENT:

I request that ADPH limit (describe the information you would like restricted):

I request the limitations described above to be made to the protected health information in my designated record set (medical record) maintained or created by ADPH.

Date of record or information you would like to limit: _____

I would like this information limited because (state specific reason for request):

[Signature/Title, if legal representative*]

Date

*May be requested to submit evidence of representative status.

REQUEST APPROVED:

By: _____
Signature Title Date

REQUEST DENIED:

By: _____
Signature Title Date

Reason for Denial:

- The information was not created by ADPH.
- The information is not part of your Designated Record Set.
- The information is not available for your inspection pursuant to the ADPH's policy regarding individual access because _____
- The information is accurate and complete.

If your request to limit your protected health information is denied, you may submit a written statement of your disagreement with the denial. Send the statement of disagreement to:

Privacy Officer
Alabama Department of Public Health
201 Monroe Street, Suite 1540
Montgomery, AL 36104
(334) 206-9324

After submitting your disagreement in writing, you will be given an opportunity for a hearing on why your request was denied. You will receive sufficient notice of the time and place that the hearing will be held.

*****Retain for minimum of 6 years*****



FORM D

REQUEST FOR ACCOUNTING OF DISCLOSURES

Patient Name: _____

Date of Birth: _____ SSN: XXX-XX- _____

Address where you want the accounting response sent:

NOTICE TO PATIENT: Your request for an accounting of disclosures of your protected health information is **only** applicable to the information maintained by the Alabama Department of Public Health. If you would like to request an accounting of disclosures of your protected health information created and maintained by any other health care provider, a separate request must be submitted to that provider.

REQUEST FOR ACCOUNTING OF DISCLOSURES:

I request an accounting of disclosures of the protected health information in my designated record set (medical record) from _____ to _____ (not to exceed six [6] years) maintained by the Alabama Department of Public Health.

I understand that the first accounting in a twelve (12) months period is free of charge, but that I can be charged a reasonable fee for any additional accountings.

I understand that the accounting must include all disclosures, **except** for disclosures:

- To carry out treatment, payment, and health care operations.
- Incident to a use or disclosure permitted by the Privacy Regulations.
- Pursuant to the individual's authorization.
- To persons involved in the individual's care or for a facility directory.
- For national security or intelligence purposes.
- To correctional institutions or law enforcement officials to provide them with information about a person in their custody.
- As part of a limited data set.
- That occurred prior to the compliance date.

Signature [Title, if legal representative]*

Date

*May be requested to submit evidence of representative status.

*****Retain for minimum of 6 years*****



FORM E

AMENDMENT ACCEPTANCE – NOTIFICATION FORM

I request and authorize the Alabama Department of Public Health to notify the health care providers or entities listed below of the amendment(s) to the medical record of:

Patient Name: _____

Date of Birth: _____ SSN: XXX-XX- _____

List of Providers/Entities that need to be notified of Amendment:

Name

Address

Phone Number

Name

Address

Phone Number

Name

Address

Phone Number

Name

Address

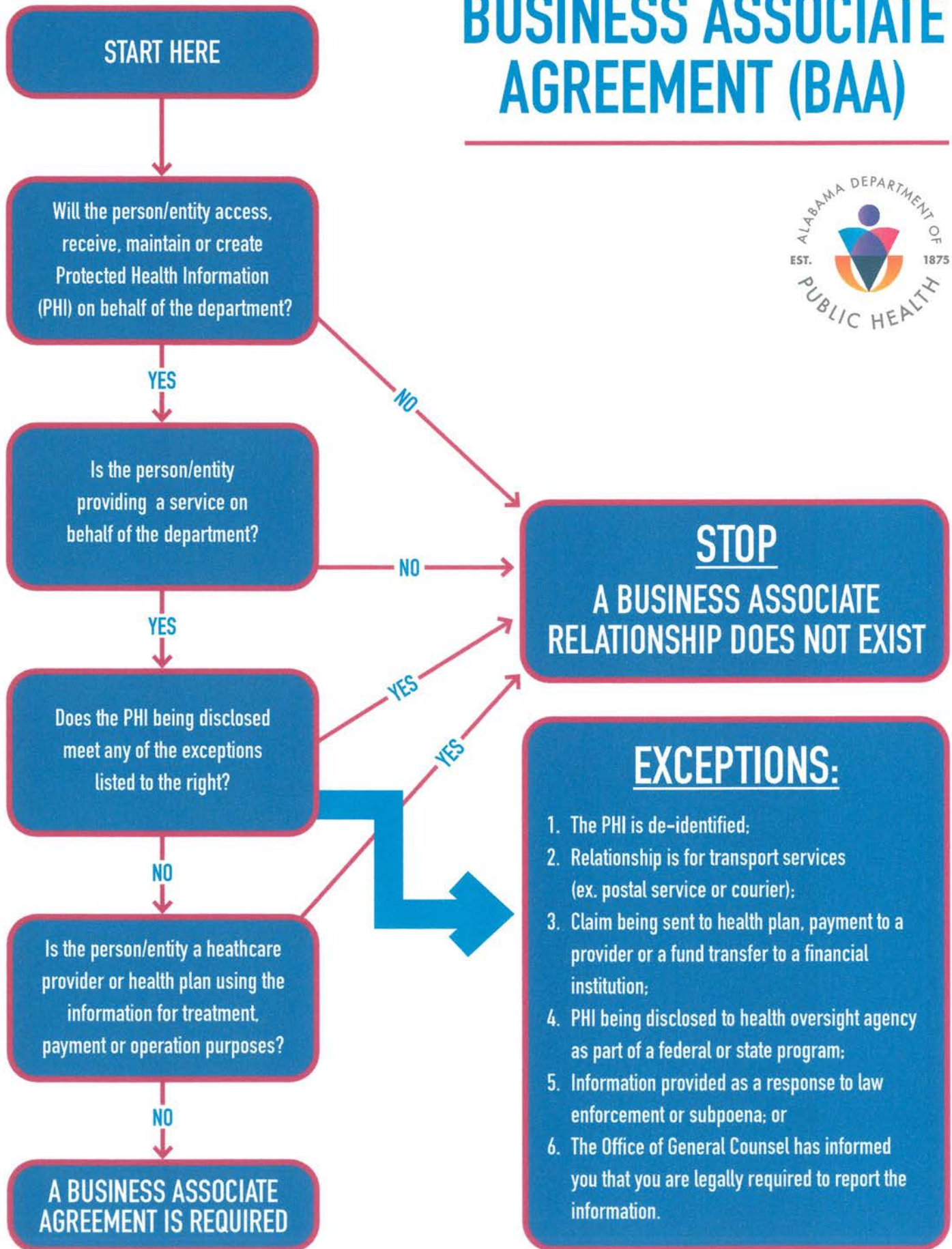
Phone Number

[Signature/Title, if legal representative*]

Date

*May be requested to submit evidence of representative status.

FORM F
**BUSINESS ASSOCIATE
AGREEMENT (BAA)**



Data Use Agreement (DUA)

FORM G

Does the data to be shared include any of the following?

- Names
- Geographic subdivisions smaller than a State
- Elements of dates (except year) related to an individual
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security Numbers (SSN)
- Medical record numbers (MRN)
- Health plan beneficiary numbers

- Account numbers
- Certificate / license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Biometric identifiers
- Web universal resource locators (URLs)
- Internet Protocol (IP) address numbers
- Full-face photographic images
- Any other unique identifying number

YES

NO

Was patient authorization obtained for this disclosure?

YES

Because authorization was obtained for the disclosure, a DUA is not necessary.

HIPAA does not apply and a DUA is not necessary for HIPAA purposes.

NO

Are elements of PHI restricted to ONLY the following?

- Geographic subdivisions smaller than a State
- Elements of dates (except year) related to an individual

YES

The data constitutes a Limited Data Set and a Data Use Agreement that complies with HIPAA requirements must be executed.

NO

PHI that does not constitute a Limited Data Set will be shared. Either patient authorization must be obtained or a waiver of authorization must be approved by the Institutional Review Board (IRB) in order to share the PHI. A DUA will NOT suffice to share data.

Does the other institution require a non-HIPAA DUA?

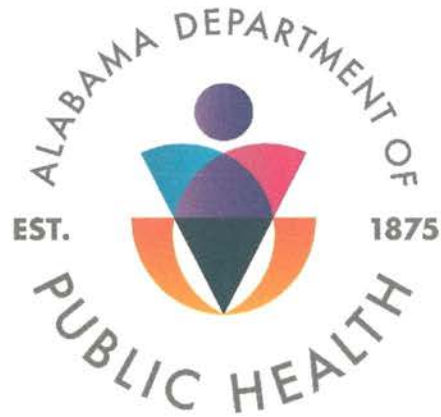
YES

A generic DUA may be executed but should not refer to a Limited Data Set.

NO

DUA is not required.





TO: _____

FAX NO: _____ PHONE NO: _____

FROM: _____
(Name of employee sending fax)

LOCATION: _____
(County Health Department, Bureau or Office)

PHONE NO: _____

DATE: _____

PAGES (including cover sheet): _____

Health care information is personal and sensitive. It is being faxed to you after appropriate authorization from the patient or under circumstances that do not require patient authorization. Maintain this information in a safe, secure and confidential manner. Re-disclosure without additional consent or authorization, unless permitted by law, could subject you to penalties under Federal and/or State law.

The information contained in this facsimile transmission may contain confidential information, which may be protected health information as defined by the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule. This transmission is intended for the exclusive use of the individual or entity to whom it is addressed and may contain information that is proprietary, privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient (or an employee or agent responsible for delivering this facsimile transmission to the intended recipient), you are hereby notified that any disclosure, dissemination, distribution or copy of this information is strictly prohibited and may be subject to legal restriction or sanction. Please notify the sender to arrange the return or destruction of the information and all copies. If you are not able to notify the sender, please contact the Department's Privacy Officer at 334-206-5874.

**Alabama Department of Public Health
HIPAA Compliance Workforce Hire/Transfer/Separation Form**

Employee Information

Full Name	_____		
	Last	First	M.I.
Work Location	_____		
	Address		

	City	State	Zip
	_____	_____	_____
	Bureau or County	Telephone Number	
	_____	_____	
Job Title	_____		
Supervisor	_____		

Employee Type

ADPH Employee (Yes or No) _____	Contractor (Yes or No) _____
Other (Please Describe) _____	
Has the employee completed HIPAA Privacy and Security Training? (Yes or No) _____	
Has the employee completed Security Awareness Training? (Yes or No) _____	
Employment Start Date	_____
Employee Transfer Date	_____
Employee Separation Date	_____

Instructions: Please submit this form to the Privacy Officer at PrivacyOfficer@adph.state.al.us and the Information Security Officer at SecurityOfficer@adph.state.al.us whenever a workforce member is hired, transferred, or separated.