ALABAMA DEPARTMENT OF PUBLIC HEALTH

HIPAA PRIVACY AND SECURITY POLICY

Applicability. This policy is intended to implement and be read in conjunction with the Health Insurance Portability and Accountability Act (HIPAA) and implementing 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, Professional Conduct Policy, and Information Security Manual.

This policy is to be followed by all state office bureaus and divisions and all county health departments to the extent that these units are subject to the requirements of HIPAA. The policy directly incorporates the subjects listed below:

1. Treatment/Payment/Health Care Operations exceptions
2. Patient's rights
3. Disclosures of Protected Health Information (PHI)
4. Verification of patient identity
5. Concept of "Minimum Necessary"
6. Procedure for redaction of records
7. Electronic HIPAA Log ("e-HIPAA Log")
8. Identifying and disclosing information to Business Associates
9. Student/Intern/Volunteer access to PHI
10. Methods of communicating PHI via e-mail, text message, and fax
11. Procedures for copiers containing hard drives
12. Use of mobile devices in working with PHI
13. Securing paper records containing PHI
14. Proper disposal of PHI
15. Breaches and sanctions for improper disclosures or violations of confidentiality
16. Mitigation of harm caused by improper disclosure
17. Requirements and methods for HIPAA training

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

1. "Department" includes all state office bureaus and divisions, all county health departments, and employees and volunteers of the Department.
2. "HIPAA" will be read to imply the appropriate portions of the statute or regulation.
3. "Privacy Officer" is the Departmental officer charged with the responsibility to ensure compliance with the privacy provisions of HIPAA.
4. "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.

5. "Security Officer" is the Departmental officer charged with the responsibility to ensure compliance with the security provisions of HIPAA.

TREATMENT/PAYMENT/HEALTH CARE OPERATIONS EXCEPTIONS

Access to treatment and efficient payment of health care, 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.

PATIENT RIGHTS

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 2013 NOPP is located in the Document Library and can be found on the Department web site at: http://adph.org/publications/assets/Privacy.pdf

PATIENT/CLIENT ACCESS TO 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 (Social Work 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.

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 or CHR1 Patient Log.

Oral Requests. Oral, in person requests should be documented in the e-HIPAA Log and the applicable progress note or CHR1 Patient Log.

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 thirty (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 or CHR1 Patient Log.

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 (Social Work 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.

ACCESS TO LABORATORY REPORTS

The HIPAA Privacy rule has been amended to allow patients, patient's designees and patient's personal representatives to view or be provided a copy of the patient's lab report, including an electronic copy, with limited exceptions. In light of this change, 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. For additional information on disclosures regarding laboratory records, please contact the Office of Compliance.

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 C: "Request to Amend or Limit Protected Health Information."** Such requests must be recorded as a progress note in the file and entered on the e-HIPAA Log. A completed request to amend or limit PHI should be forwarded to the Department Privacy Officer immediately.

Upon receipt of the same, the request shall be acknowledged in writing by appropriate clinic personnel. The request shall be evaluated by appropriate personnel and a recommendation made to the Privacy Officer for consultation. If a request is unusual, an Automated Report of Incidents and Accidents (ARIA) should be made. 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 thirty (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 patient's/client's file and recorded in the e-HIPAA Log.

Amendments or alterations 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.

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 Amend or 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.

Requests for restrictions should be forwarded to the Privacy Officer immediately. The Privacy Officer will make the final determination about whether a restriction will be granted within 30 days of the request.

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 and the request form must be maintained in the patient's medical record for a minimum of six (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 place or affix a clear indication of the restriction on the patient's medical record and the e-HIPAA Log.

REQUEST 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.

Procedure.

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 E: "Request for Accounting of Disclosures."** Patients making their request for an amendment by telephone or e-mail must be forwarded a copy of "Form E." The request form must be maintained in the patient's medical record.
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 (Form E) 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 thirty (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 to determine if the appropriate conditions have been satisfied.

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 CHR-3.

REQUESTS FOR PATIENT/CLIENT INFORMATION REGARDING RESEARCH/MARKETING

Any request made to the Department requesting PHI for research or marketing purposes should be forwarded to the Privacy Officer immediately. 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.

REQUESTS FOR INFORMATION OF DECEASED PATIENTS/CLIENTS

While information regarding deceased patients/clients can still be provided for approved research purposes, information on individuals who have been deceased for a period of longer than 50 years is no longer considered PHI. Additionally, the Department is now allowed to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior express preference of the individual that is known to the Department. If there are any questions regarding whether to release a decedent's information, please contact the Privacy Officer.

DISCLOSURES

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.

Verification of identity can be accomplished by: (1) presentation of picture I.D., (2) signature comparison, or (3) other appropriate method.

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.

MINIMUM NECESSARY

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.

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.

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.

Exceptions: 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 or his/her legal representatives.
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.

REDACTION OF PHI

1. After reviewing the requested record and determining that it contains releasable information, the custodian of records shall make a copy of all pages containing the ***restricted*** information.
2. The custodian of records shall then color over the restricted information on the reproduced copy with a black marking pen in a neat manner.
3. The custodian of records shall then reproduce a copy of this page, which shall be the page that is released to the requester.
4. The custodian of records shall then dispose of the first copy by shredding or placing in a secure shredder bin.
5. The custodian shall ensure that the restricted information is not visible on the copy.

DOCUMENTING DISCLOSURES
USE OF 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.

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.adph.org.)
2. Authorized releases based upon subpoena or judicial process.
3. Authorized releases to law enforcement, national security, public health disease control, jail or prison officials, death disclosures, emergencies, abuse investigatory agencies and research.
4. Requests to limit releases of PHI.
5. Requests to view PHI.
6. Requests to amend or correct PHI.
7. Requests for accounting of PHI.

Instructions on access to the e-HIPAA log are attached as "**Form B."**

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-Department 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. If the request for PHI is approved, remember to log any disclosures in the e-HIPAA Log for any patient whose records are accessed.

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.

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 knows 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 and contact the Office of Compliance. 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 Compliance.

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

Data Use Agreements. All data use agreements must be approved by the Office of Compliance prior to execution. 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.

BUSINESS ASSOCIATES

A "**Business Associate**" is a person or entity who **creates, receives, maintains or transmits** PHI for the Department.

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 electronic protected health information (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**."

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. Every clinic site, area office, state level bureau office, and home health subunit at the county level shall set out the names of the students or volunteers who are authorized to access PHI. The list of names shall be maintained on a chart entitled, "Students/Volunteers Authorized to Receive/Access Protected Health Information." This chart documents the name of the individual authorized to access PHI, the date that the individual's authorization began, and the date that the authorization was terminated. The chart should be easily accessible and available to the Office of Compliance and Office of Program Integrity, upon request. **Only students and volunteers who have been identified, reviewed the HIPAA policy, and trained on HIPAA Privacy and Security shall be permitted access to PHI.**

A copy of the chart is attached as "**Form A: Students/Volunteers Authorized To Receive/Access Protected Health Information**."

METHODS OF COMMUNICATING PHI

E-MAIL PROCEDURES

Information below regarding the sending of e-mails must be read in its entirety.

Sending PHI by e-mail exposes the PHI to two risks:

1. The e-mail 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 e-mail 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. Limit the information you include in an e-mail to the minimum necessary for your clinical purpose.
2. Whenever possible, avoid transmitting highly sensitive PHI (for example, mental health, sexually transmitted disease, or HIV information) by e-mail.
3. Never use automatic forwarding with your Department e-mail account.
4. Never send PHI by e-mail unless you have verified the recipient's address (for example, from a directory or a previous e-mail) and you have checked and double-checked that you have entered the address correctly.
5. Always include a privacy statement notifying the recipient of the insecurity of e-mail and providing a contact to whom a recipient can report a misdirected message.

Required Privacy Statement: *"This e-mail 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 e-mail and destroy all copies of the original message."*

SENDING E-MAILS IN LOTUS NOTES

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 e-mails to employees in the bureaus and other county health departments.)

SENDING E-MAILS TO OUTSIDE PROVIDERS

E-mails sent to individuals outside of the Department, including other state agencies, MUST be encrypted. The Department has chosen SYMANTEC software encryption and devised rules for e-mail communication that will automatically encrypt e-mails that fulfill particular criteria. This may mean that individuals that receive e-mails from you will be asked to create and utilize a username and password to receive e-mails containing PHI.

SENDING E-MAILS TO PATIENTS

The Department may send unencrypted e-mails to patients as long as the patient is properly advised of the risk. If patients are notified of the risk and still prefer unencrypted e-mail, the patient has a right to receive PHI in that way, and the Department is not responsible for unauthorized access to PHI while in transmission to the individual based on the individual's request. **The Privacy Officer must be notified of a patient's request for unencrypted e-mail prior to disclosure**. The relevant section of the CHR-3 pertaining to e-mails must be completed prior to communicating with the patient through e-mail in this manner. The consent must be updated at each patient visit.

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 CHR-3 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. 555-123-4567@txt.att.net)

Appointment reminders must not be sent to a patient from an employee's personal cell phone. Appointment reminders for WIC are excluded from this requirement.

FAX SHEETS/FACSIMILE COMMUNICATIONS

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:
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. Immediately document the incident by filing an ARIA report and call to notify the Privacy Officer at 334-206-2648. Finally, verify the fax number with the recipient before attempting to fax the information again.

ALL faxes must include an appropriate fax cover sheet. Fax cover sheets accompanying disclosures of PHI shall carry the statement:

> CONFIDENTIAL HEALTH INFORMATION ATTACHED:
> 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 patient 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 is privileged and confidential and is intended for use only by the recipient listed above. If you are neither the intended recipient nor the employee or agent of the intended recipient responsible for the receipt of this information, you are hereby notified that the disclosure, copying, use, or distribution of this information is strictly prohibited and may be a violation of the Health Insurance Portability and Accountability Act (HIPAA). If you have received this transmission in error, please notify the sender immediately by telephone to arrange for the return of the transmitted documents or to acknowledge their destruction."
>
> A copy of an appropriate fax cover sheet is attached as "**FORM G**."

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.*

MOBILE DEVICES

Every member of the Department who utilizes a laptop computer or mobile electronic device (e.g. Blackberry, flash drive, smart phone, hand held PC, 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 Information Security Manual.

Protection of Confidential Data

Every Department staff member issued a laptop, smart phone, Blackberry, flash drive or other mobile device must use reasonable care to protect Department data as defined in the current Information Security Policy. 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 mobile devices against unauthorized access. Prior to use or display of confidential data via laptop computer or other mobile device, the following security measures must be in place.

A. 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.

B. Encryption must be enabled on laptop computers that have encryption capability and that transmit confidential Department information, such as PHI. Laptops shall be protected with antivirus software and updated daily if supported by the device. NOTE: Lotus Notes e-mail is protected with centralized anti-virus and anti-spam software. This protection may not apply to e-mail systems outside of Lotus Notes.

C. Only Department employees are permitted to use Department issued mobile devices. Department issued devices must NOT be allowed to be used by individuals not directly employed by the Department.

The use of unprotected mobile devices to access or store confidential data is prohibited regardless of whether the equipment is owned or managed by the Department.

The Division 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 data mobile devices.

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 mobile device is lost or stolen, the theft or loss must be reported immediately to 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.

SECURING PAPER RECORDS

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.

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.

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. Therefore, **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. The placement of PHI in a recycle bin, dumpster or trashcan will be considered a HIPAA violation.**

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 faxed to the Office of Compliance at (334) 206-3763 and the fax cover sheet should state that the information contained within the fax is provided for the purpose of supplementing an ARIA report. 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.

SANCTIONS FOR EMPLOYEES VIOLATING CONFIDENTIALITY

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

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

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 six (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 six (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.

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 of a 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.

TRAINING

It is mandatory that all employees receive HIPAA Privacy and Security Awareness training.

Current employees must view the current version of the HIPAA Refresher training video or on-line presentation regarding HIPAA compliance and electronically document completion. Supervisors shall provide appropriate materials to accompany the training video, if applicable.

New employees must view the most current HIPAA Awareness and HIPAA Refresher training and electronically document completion. New training materials, as they are produced, will be made and distributed by the Privacy Officer.

Students and Volunteers must view a merged HIPAA Privacy and Security Awareness and Refresher training and electronically acknowledge completion. Additionally, access to PHI must be documented in the student/volunteer folder, and maintained by that division, bureau or clinic, in written or electronic form, for at least six (6) years after the student/volunteer separates or longer if required by other applicable Department policies.

COMPLAINTS/QUESTIONS

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

PRIVACY OFFICER
Samarria Dunson, J.D., CHC, CHPC
201 Monroe Street, Suite 1698
Montgomery, AL 36104
334-206-9324
Samarria.Dunson@adph.state.al.us
www.adph.org/compliance
www.adph.org/complianceeducation

ACTING SECURITY OFFICER
Leslie Hay
201 Monroe Street, Suite 1698
Montgomery, AL 36104
(334) 206-5010
Leslie.Hay@adph.state.al.us

FORM A

STUDENTS/VOLUNTEERS AUTHORIZED TO RECEIVE/ACCESS PROTECTED HEALTH INFORMATION

NAME	DATE AUTHORIZATION BEGAN	DATE AUTHORIZATION TERMINATED	COMMENTS

**APPLIES IN A NON-EMERGENCY OR NON-DISASTER SETTING

FORM B

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 such as releases of records for Treatment, Payment, and Health Care Operations.**

Instructions for accessing the e-HIPAA Log can be found in the document library.

FORM C

REQUEST TO AMEND OR LIMIT PROTECTED HEALTH INFORMATION

Patient Name: _____ Date of Birth: _____
Address where you want the amendment response sent:
_____

NOTICE TO PATIENT: Your request to amend or limit your 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 or limits to your protected health information maintained by any other Health Care Provider, a separate request must be submitted to that provider.

REQUESTED AMENDMENT:

I request that ADPH amend or limit (describe the information you would like amended or restricted):
_____
_____
_____

I request the amendment or 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 amend or limit:
_____

I would like this information amended or limited 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 or limit the release of your record, please complete the attached form (FORM D), and return it to us, to identify any persons or entities that we need to notify of the amendment or limitation to your protected health information.

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 or limitation 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 785
Montgomery, AL 36104
(334) 206-2648

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

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 records of _____.
[Name of patient]

Signed: _____ _____
Name – (Title, if legal representative) *Date*

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

_____	_____
Name	**Name**
_____	_____
_____	_____
Address	**Address**
_____	_____
Phone Number	**Phone Number**
_____	_____
Name	**Name**
_____	_____
_____	_____
Address	**Address**
_____	_____
Phone Number	**Phone Number**
_____	_____
Name	**Name**
_____	_____
_____	_____
Address	**Address**
_____	_____
Phone Number	**Phone Number**

FORM E

REQUEST FOR ACCOUNTING OF DISCLOSURES

Patient Name _____ Date of Birth: _____
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 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 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************************