District 2 Public Health
David N. Westfall, M.D., MPH, CPE, Health Director
1280 Athens Street • Gainesville, Georgia 30507
PH: 770-535-5743 • FAX: 770-535-5958 • www.phdistrict2.org

Banks, Dawson, Forsyth, Franklin, Habersham, Hall, Hart, Lumpkin, Rabun, Stephens, Towns, Union and White Counties

HIPAA POLICY ON CONFIDENTIALITY
Policy # 183
Effective 4/03
Reviewed January 3, 2012

PURPOSE:

The HIPAA Policy on confidentiality is intended to protect and insure confidentiality and protection of client's health information. Confidentiality is an ethical and legal issue. Employees of District 2 Public Health, especially those working with confidential health information, must be extremely vigilant about protecting the client's records. Federal Law protects the client's right to privacy.

The Department of Public Health (DPH) Policy states that it is the Policy of DPH to respect and acknowledge the privacy and confidentiality of its clients. Furthermore, as a unified Human Service team, it is the policy that the client information and records be considered as being Department Information and Records, and as such, may be shared with authorized Department staff on a *need to know basis*. "Need to know basis" is outlined in the Privacy notice given out to each client. Confidential client information may be released to persons or entities outside of the Department only with proper authorization or as specified in the Privacy notice given to each client.

GENERAL POLICY:

All client health information is confidential and will not be released or communicated by any employee to anyone other than the client, without valid written permission or as specified in the Privacy Notice, in a court order signed by a judge or in a life-threatening situation. All requests for Release of Protected Health Information (PHI) outside of these parameters will be routed to the County or to the District Privacy Officer or designee. The Privacy Officer or designee is authorized to release information and/or make decisions about access to PHI. Release to appropriate "third parties" must have documented evidence of reasonable steps taken to verify the identity of the person receiving/requesting the PHI. No individually identifying information will be transmitted to any individual or outside agency that is not a Business Associate without an authorized Release of Information signed by the client or the client's legal guardian.

Individually identifying information and confidential information shall only be released to private insurance companies with the signed authorization of the client or his legally responsible agent on a need to know basis. Information (such as lab test results) shall be released to employees, law enforcement agencies, or judicial systems, (only) with a written authorization signed by the client or legally responsible agents which specifies to whom the information shall be sent and the purpose for sending such information. Verbal information about the clients is often exchanged between service

providers of different agencies in order to make referrals or to provide continuity of care. This information must be treated with the same concern as written information. It is not necessary to obtain written authorization if such is done in an effort to further the health and welfare of the client and if there is no risk that the shared information will result in harm to the client. Casual conversation outside of the Public Health Department about the clients must be avoided at all times.

Federal and State Regulations, which are more restrictive than this District 2 Policy, shall take precedence. The County Privacy Officer or designee may consult with the District Privacy Officer or County Attorney prior to releasing any information at any time. This Policy is a requirement for all Public Health employees and must be signed and dated following review.

SANCTIONS:

Violation of this Policy may result in disciplinary action up to and including termination of employment.

APPROVED BY _____ **ON THIS DAY OF** _____
District 2 Health Director Date

TO BE SIGNED BY EMPLOYEE AND KEPT ON FILE:

I, _____, have read a copy of District 2 Public Health's *HIPAA Policy of Confidentiality* and I understand the procedure to follow for *protecting client health information and access to medical records.*

I understand and agree that in the performance of my duties as an employee of District 2 Public Health, I must hold medical information in confidence. I understand that violation of confidentiality of medical information will result in punitive action, which may be dismissal. I understand that I cannot disclose or discuss any confidential information that I may learn while working here.

_____ _____
Employee Name, Title Date

DISTRICT 2 PUBLIC HEALTH
MANUAL ON HIPAA POLICIES AND PROCEDURES
POLICY # 183

INTRODUCTION

The Health Insurance Portability and Accountability Act was enacted into law in 1996 with specific implications for health care providers. The law effects all healthcare organizations and providers, which includes public health authorities, insurers, clearinghouses, billing agencies, information system vendors, service organizations, universities and physicians. The Privacy part of HIPAA was implemented April 2003 and the Computer Security part will be implemented October 2004.

Training and compliance of the HIPAA rules is mandatory. Therefore District 2 Public Health will incorporate a review of these policies and procedures in orientation and quality assurance programs. District 2 Public Health is required to have documented training for all members of its workforce in the policies and procedures required by the Privacy Rule. It is the District and County Privacy Officers responsibility to assure training requirements are met and continued on an ongoing basis.

Sanctions will apply to employees who fail to comply with District 2 Public Health's policies and procedures. Sanctions include progressive disciplinary action up to dismissal from employment. The Federal government may impose civil penalties, which include imprisonment for deliberate violation of the privacy rules.

District 2 Public Health may not retaliate against any person for exercising a right under the Privacy Rule, or for filing a complaint, participating in an investigation, or opposing any unlawful act relating to the Privacy Rule.

REFERENCES:

HIPAA: Title II, Subtitle F, Sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996.
Records, Computers and the Rights of Citizens; Report of the Secretary's Advisory Committee on Automated Personal Data Systems, H.E.W., July 1975.
Various State and Federal Laws and regulations, a list of which can be obtained from the Department of Human Resources Office of Evaluation and Research.

PURPOSE OF HIPAA POLICIES AND PROCEDURES

To protect and insure confidentiality and protection of client's health information. Confidentiality is an ethical and legal issue. Employees of District 2 Public Health, especially those working with confidential health information must be extremely vigilant about protecting the client's records. Federal Law protects the client's right to privacy.

It is the policy of the Department of Community Health (DCH) to respect the right of privacy of every individual and, in doing so, to safeguard the protected health information (PHI) of every individual whose information is used or disclosed by DCH and by its contractors. DCH policy is to ensure compliance with all applicable laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to establish and maintain a standard of best practices in safeguarding protected health information. Furthermore, as a unified human service team, it is the policy that the client information and records are department information and records and as such, may be shared with authorized department staff on a need to know basis. A need to know basis is outlined in the Privacy Notice given to each client. Confidential client information may be released to persons or entities outside the department with proper authorizations or as specified in the Privacy Notice given to each client.

GENERAL POLICY

All client health information is confidential and will not be released or communicated by any employee to anyone other than the client, without valid written permission or as specified in the Privacy Notice, in a court order signed by a judge or in a life-threatening situation. All requests for release of protected health information (PHI) outside of these parameters will be routed to the District or County Privacy Officer, or designee. The Privacy Officer or designee is authorized to release information and/or make decisions about access to PHI. Release to appropriate "third parties" must have documented evidence of reasonable steps taken to verify the identity of the person receiving the PHI. No individually identifying information will be transmitted to any individual or outside agency that is not a business associate without an authorized release of information signed by the client or the client's legal guardian.

Individually identifying information and confidential information shall only be released to private insurance companies with the signed authorization of the client or his legally responsible agent on a need to know basis. Information (such as lab test results) shall be released to employees, law enforcement agencies or judicial systems with a written authorization signed by the client or legally responsible agent which specifies the person or agency to whom the information to be sent and the purpose for sending such information. Verbal information about clients is often exchanged between service providers of different agencies in order to make referrals or to provide continuity of care. This information must be treated with the same concern as written information. It is not necessary, however, to obtain a written authorization, provided it is done to further the health and welfare of the client and there is no risk that the shared information will result in harm to the client. Casual conversation outside of the public health department about clients must be avoided at all times.

Federal or state regulations, which are more restrictive than this District policy, shall take precedence. The Privacy Officer or designee may consult with the District Privacy Officer or County Attorney prior to releasing any information at anytime. This policy is a requirement for all Public Health employees and must be signed and dated following review. This policy will be filed in employee's personnel file at the District Office.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

APPROVED _____ _____
District Health Director Date

TO BE SIGNED BY EACH EMPLOYEE AND KEPT ON FILE

I, _____ have read a copy of District 2 Public Health's Policy on Confidentiality and understand the procedure to follow for protecting client health information and access to medical records.

I understand and agree that in the performance of my duties as an employee of District 2 Public Health, I must hold medical information in confidence. I understand that violation of confidentiality of medical information will result in punitive action, which may be dismissal. I understand that I cannot disclose or discuss any information that I may learn while working here.

_____ _____
Signature of Employee Date

DISTRICT 2 PUBLIC HEALTH
UNAUTHORIZED RELEASE OF PROTECTED HEALTH INFORMATION

PURPOSE

To protect and insure confidentiality and protection of our client's health information. Confidentiality is an ethical and legal issue. Employees of District 2 Public Health, especially those working with confidential health information must be extremely vigilant about protecting the client's records. Federal law protects the client's right to privacy.

It is the policy of the Department of Community Health (DCH) to respect the right of privacy of every individual and, in doing so, to safeguard the protected health information (PHI) of every individual whose information is used or disclosed by DCH and by its contractors. DCH policy is to ensure compliance with all applicable laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to establish and maintain a standard of best practices in safeguarding protected health information. Furthermore, as a unified human service team, it is the policy that the client information and records are department information and records and as such, may be shared with authorized department staff on a need to know basis. A need to know basis is outlined in the Privacy Notice given to each client. Confidential client information may be released to persons or entities outside the department with proper authorizations or as specified in the Privacy Notice given to each client.

GENERAL POLICY

Our client's privacy is a high priority and we take unauthorized release of our client's personal health information seriously. If you observe or have knowledge of any unauthorized release of protected health information from District 2 Public Health you must immediately report this release to the District or County Privacy Officer. Failure to do so may result in discipline by the Privacy Officer as an accomplice to the unauthorized release. The responsibilities of the Privacy Officer will become a critical component of his/her PMF.

PROCEDURES

- Once the Privacy Officer has knowledge of an alleged unauthorized use or disclosure of PHI, he/she shall immediately begin a thorough investigation of the unauthorized release of PHI. This may be performed through confidential interviews with staff members, inspection of release logs and/or access logs, and any other methods(s) the Privacy Officer deems appropriate. It may also be necessary for the Privacy Officer to ask for assistance from another staff member in conducting the investigation; if so, he/she shall ask for assistance from a staff member he/she has concluded is not party to the alleged unauthorized release of PHI.

- The investigation may find a systemic issue with District 2 Public Health's policies and procedures on handling PHI, or the investigation may find a personnel issue, or both. The Privacy Officer upon concluding the investigation shall recommend policy changes to the Health Director.

The following illustrates how the Health Director and the District Privacy Officer may make changes:

- Policy changes: the Privacy Officer may find the practice policies and/or procedures require adjustment(s). The Privacy Officer shall make the necessary modifications to the practice policies by adding addendum(s) to the current policies, and shall notify all employees of the change(s) through inter-office memorandum. This shall be done as expeditiously as possible.

- Personnel changes: the Privacy Officer may find that one or more employees either does not understand or refuses to abide by District 2 Public Health's policies and procedures on maintaining the privacy and confidentiality of PHI. It may be necessary for employees to be disciplined by the Privacy Officer for violations of the practice policies. The Health Director and Privacy Officer shall determine the severity of the punishment based on the severity of the unauthorized release. However, the following provides a guide as to how the Privacy Officer may discipline the employee(s):

    - *First Offense:* Re-training on District 2 Public Health's policies and procedures governing privacy of PHI and verbal reprimand/counseling with a note of the verbal reprimand filed in the employees' personnel file.

    - *Second Offense:* Written reprimand from the Privacy Officer with one copy given to the employee(s) and one copy kept in the employees' file.

    - *Third Offense:* Suspension from duties without pay for a period to be determined by the Privacy Officer but not to exceed two (2) weeks.

    - *Fourth Offense:* Termination of the employee.

In all cases the Privacy Officer shall document in writing the unauthorized use(s) or disclosure(s) of PHI, the perpetrator(s), and what action(s) (if any) were taken as a result of the violation(s).

DISTRICT 2 PUBLIC HEALTH
DISCLOSURE AUTHORIZATIONS/LIMITATIONS

PURPOSE

To protect and insure confidentiality and protection of our client's health information. Confidentiality is an ethical and legal issue. Employees of District 2 Public Health, especially those working with confidential health information must be extremely vigilant about protecting the client's records. Federal law protects the client's right to privacy.

It is the policy of the Department of Community Health (DCH) to respect the right of privacy of every individual and, in doing so, to safeguard the protected health information (PHI) of every individual whose information is used or disclosed by DCH and by its contractors. DCH policy is to ensure compliance with all applicable laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to establish and maintain a standard of best practices in safeguarding protected health information. Furthermore, as a unified human service team, it is the policy that the client information and records are department information and records and as such, may be shared with authorized department staff on a need to know basis. A need to know basis is outlined in the Privacy Notice given to each client. Confidential client information may be released to persons or entities outside the department with proper authorizations or as specified in the Privacy Notice given to each client.

GENERAL POLICY

The patient has the right to authorize a release of information pertaining to their treatment or payment to other providers or entities. The patient also has the right to put limits on what information can or cannot be released and to whom that applies.

PROCEDURES

<u>Authorized Release</u>

- Before releasing any protected health information the patient must fill out an Authorization to Release Information form and it must be signed.

- If the entire medical record is to be disclosed, a written explanation why the entire medical record may be disclosed is required. Psychological notes, drug or alcohol abuse notes, AIDS and other STD related information, all laboratory and x-ray reports, consultation reports, and other outpatient reports are all included on the Authorization to Release Information form.

- If an expiration of the authorization is known, it must be indicated on the form or the authorization will be in effect until written revocation of the authorization is received by the Privacy Officer.

- The authorization is to be verified and given to the Privacy Officer for approval and action.

- The authorization will be noted as to the disclosure date, the person distributing the protected health information, and how it was distributed (fax, mail, etc.).

- The authorization will be added to the medical record and the date it is added will be recorded on the authorization form.

- If/when a letter of revocation is received, it will be attached to the authorization form and the date and time the revocation is processed will be noted on the authorization form in the patient's record.

Limited Release

- If the patient elects to limit the disclosure of his/her protected health information and indicates such on the Privacy Notice acknowledgement, he/she must make arrangements to speak with the Privacy Officer or designee to discuss the limits requested and the medical records will be marked accordingly upon approval and action of the Privacy Officer.

- If the patient later elects to remove the limited disclosure restrictions, he/she must inform the Privacy Officer in writing indicating that the restrictions can be removed from the medical record. The Privacy Officer will note the medical records accordingly.

DISTRICT 2 PUBLICH HEALTH
PATIENTS WHO REFUSE AUTHORIZATON

There may be times when you ask a patient for his/her authorization, they will refuse to grant such an authorization. When this does occur, you should inquire why the patient does not want (County) Board of Health to use his/her protected health information in the manner set forth in the authorization. Your response to the patient's reason(s) will vary depending on the situation; however, at no time should you condition treatment or other activity at District 2 Public Health on the patient's willingness to sign an authorization.

If the patient refuses to sign the authorization, ask if the patient understands the use(s) as listed on the authorization form. Inform the patient that District 2 Public Health is limited to those uses; any use outside the explanation on the form is a violation of federal regulation. You may also explain to the patient the benefit(s) to District 2 Public Health or to the community for using that information. However, you should not harass the patient into signing the form. Remember, if at any time you need assistance in explaining the authorization to the patient, find the Privacy Officer and ask him/her to help you.

Even after your explanations the patient may still refuse to sign the authorization form. If you believe further discussion would not change the patient's mind, simply note your attempt to have the patient sign the authorization form on the form itself (including date, time and your name) and pass the unsigned form to the Privacy Officer.

DISTRICT 2 PUBLIC HEALTH
HANDLING PHI IN THE OFFICE/CLINIC

PURPOSE

To ensure the confidential and appropriate handling of protected health information (PHI) in public and non-public areas of the office/clinic where patients and other unauthorized persons are found.

GENERAL POLICY

District 2 Public Health shall utilize reasonable effort to protect privacy and limit disclosure of such information. Generally, if the information identifies the individual and relates to his/her health status (or the payment for health services), the information is considered PHI. Reasonable effort does not imply a mandate for major reconstruction or changes that are cost prohibitive to the clinic/facility. Reasonable effort may include restructuring and/or reorganizing clinic/information flow in areas where information is collected from and given to patients; improving personnel practices and habits in day to day activities to better prevent random disclosure of PHI; initiating stricter practices to safeguard patient records stored/utilized in public/non-public areas; relocating medical record storage to a more secure area; closer supervision of patients in routing them from waiting areas to clinical areas and check-out; and incorporating more opportunities to allow patient choice in how and where they give and receive protected health information. The following procedures address these areas and are to be followed in limiting disclosure of protected health information.

PROCEDURES – PUBLIC AREAS

Waiting Area/Front Desk

At no time should protected health information be discussed, posted, or in any way revealed in the public waiting area/front desk of the facility.

- Establish protective barrier through reasonable means to separate public waiting area from front desk.
- Whenever practical, keep doorway(s) closed to front office area to prevent access by unauthorized persons or utilize signs to prevent entry by unauthorized persons.
- Utilize separate private area to answer questions or discuss protected health information i.e. financial interviews, payment concerns.
- Kindly defer all questions regarding patient's health status, reason for visit, etc. to the health care provider.
- Patient sign in sheets will include no protected health information (Attachment A); and will be changed periodically throughout the day (minimum of twice a day is recommended).
- To eliminate patient interviews at the front desk, utilize patient enrollment forms to collect information on new patients or update information on established patients.

- Keep all completed patient enrollment forms, records, etc. away from front desk area and public view and always out of reach i.e. table behind desk, shelf or shielded area underneath counter, closed file folder, record holder facing away from waiting area.

- Position computer monitors away from public areas at all times to prevent anyone from viewing information on computer screens, or utilize privacy filters on monitor screen.

- If feasible, place shredder in front desk area for immediate destruction of protected health information that is no longer necessary to be maintained in the client record, i.e. patient enrollment form after data has been entered in computer.

- Use reasonable caution when making/receiving phone calls in front desk area to prevent conversation from flowing into waiting area i.e. speak in low tones; closing sliding glass door at front window (if applicable).

- When at all possible, never leave front desk unattended.

- At the close of business day, place all patient records, and any other materials containing PHI in a preferably locked file cabinet in the front office/medical records room out of view and access of unauthorized persons i.e. cleaning services, maintenance.

- Lock door(s) to front desk/medical records room before leaving.

Clinical/Exam Areas

Care and caution must be exercised at all times to assure privacy and confidentiality of PHI in hallways, waiting areas, laboratory, multi-use and/or private exam areas of the facility.

Hallways/Waiting Areas

- County Privacy Officers will enforce reasonable efforts to provide escort or clear directions for leading patients to laboratory/exam rooms and check out area to maintain minimum risk of patients wandering unsupervised in areas where PHI may be accessed/overheard.

- Charts must not be left unattended in rolling carts, on tabletops, in open unlocked file cabinets, or anywhere in full view or accessible to unauthorized persons in hallways and waiting areas.

- When chart holders are used, charts must be placed in chart holders with identifying information facing away from hallways and public areas.

- Doors to exam rooms should be closed during interview or exam to reduce risk of conversation flowing into hallways and waiting areas.

- All staff must exercise caution to avoid conversation in hallways and waiting areas regarding protected health information.

Laboratory/Multi-use Clinic Areas

- Use reasonable caution when placing patients in areas where space must be shared with other patients while receiving care. For example, ask patient if he/she minds having blood drawn in the lab with other patients present.

- Use a private exam room or other appropriate location for patients who request it.

- Lab slips, lab results, specimen labels, notes, etc. must be handled with caution to prevent random disclosure of PHI in the laboratory setting or other multi-use areas of the clinic i.e. kept in the patient record and out of arms reach of patients, specimen containers with patient names on labels should be turned away from view of patients.

- Position computer monitors away from public areas at all times to prevent anyone from viewing information on computer screens, or utilize privacy filters on monitor screen.

- For lab results that are not immediately available, inform patient of options for him/her to receive test results i.e. by mail, public health nurse will call them or they can call and request it by identifying themselves using their name or a test number. (HIV test results are given face to face according to procedures in the OCGA § 31-22-9-2.)

- Lab results available on-site should be given in a private exam room or other private area.

- All staff must exercise caution to avoid conversation in laboratory/multi-use clinic areas regarding protected health information.

Private Office/Exam Room

- During clinic hours when records are in use and patients are in and out of private offices/exam room's records must be safeguarded at all times to prevent accidental disclosure of PHI. A file cabinet, desk drawer, or shielded area behind desk may be used to store records between patients when records require additional documentation, data entry into computer, quality assurance review, etc.

- If the nurse must take a phone call from another patient or in regard to another patient while in the exam room with a patient, he/she should excuse himself/herself and take the call in another room or write down the name and number and return the call at a later time. Extreme caution must be taken when speaking with or about patients in the presence of other patients.

- Position computer monitor away from patient to prevent patient from viewing information on computer screen.

- Private office/exam room doors should be closed when interviewing patients to reduce the risk of conversation from flowing into hallways or waiting areas.

- If other health department staff needs to speak with the nurse while she is in a private office/exam room with a patient, they should either call the nurse if a phone is accessible in the room or knock on the door and wait for the nurse to answer.

- If the front desk needs to locate a patient while they are in the clinic area, discretion must be exercised to contact staff in the lab and exam areas without using patient's name in hallways, waiting areas, or over the intercom. Contacts to staff to inquire of the whereabouts of the patient should be initiated via telephone or having a staff person from the front desk walk back to the clinic area to leave message with clinical staff to locate patient and give message.

- Family members, friends, sales representatives, maintenance workers, cleaning service, other visitors must no be in clinical areas during office hours without good reason and authorization of the Privacy Officer.

- If emergency repairs or clean up are necessary in the clinic area during business hours the County Nurse manager will consult with the Privacy Officer to establish accommodations for these while making a good faith effort to abide by the privacy policies to protect the privacy of patients who may be in the facility at the time.

- When private offices/exam rooms are not in use they must be maintained in orderly fashion with no protected health information in view at any time.

- On a periodic basis the Privacy Officer should walk through the clinic areas (lab, multi-use clinic rooms, private offices/exam rooms, etc.) at close of business day and check to see that no PHI is inadvertently left out in view of cleaning service, maintenance workers, etc. who may have valid and authorized reasons to be in clinic areas after hours.

PROCEDURES – NON-PUBLIC AREAS

Billing Office

Reasonable efforts must be exercised at all times to assure that PHI in the billing office is protected from view and access by unauthorized persons who may be in the building during office hours as well as after hours. PHI in the billing area may include patient medical record, patient logs, superbills, bills from private providers, remittance advices, EOB's, letters, etc.

- The billing office should be established in a private area with reasonable protective barrier to separate area from unauthorized persons.

- Whenever practical, keep doorway(s) closed to billing office to prevent access by unauthorized persons or utilize sign to prevent entry by unauthorized persons.

- If office must be unattended, always lock door before leaving.

- Use reasonable caution when making/receiving phone calls to/from patients, private physicians, insurance companies, Medicaid, Medicare, etc. to prevent conversation from flowing into public areas i.e. speak in low tones, keep door closed.

- Utilize private area to answer questions or discuss protected health information with patients if this cannot be accommodated in the billing office.

- Safeguard PHI at all times to prevent disclosure of protected patient privacy. Financial records i.e. superbills, bills, remittance advices; EOB's, letters, etc. should be maintained under lock and key when not in use.

- Secure holding areas i.e. file drawer, desk drawer, shielded space behind desk which are out of arms reach must be utilized when records are in use to prevent access by unauthorized persons.

- At no time should protected health information be left open and/or unattended on a desk, computer table, etc.

- Position computer monitors away from public areas at all times to prevent anyone from viewing information on computer screens, or utilize privacy filters on monitor screen.

- At close of business day, place all PHI in locked file **room and preferably in locked file cabinet.**

- Lock door to billing office before leaving for the day.

Medical Records Room

The medical records room must be secure at all times with every reasonable effort made to maintain privacy of patient records during and after business hours.

- The medical records room should be located in an area isolated from public areas whenever possible and be equipped with locks to prohibit access from unauthorized persons.

- When practicable the door to the medical records room should remain closed during business hours limiting access to unauthorized persons. If this is not reasonable a sign with appropriate message (Do not enter, authorized personnel only) should be placed in the doorway as notification to unauthorized persons.

- Patient records must be stored in a locked file **room and preferably in a locked file cabinet** when not in use i.e. lunch breaks, after hours, etc.

- Labels on medical records should include only minimum information as necessary to identify patient to whom the record belongs. Labels must be typed and current fiscal year should be indicated on chart.

- The Privacy Officer must ensure that an appropriate and confidential system is in place to assure that patient records are securely removed and routed from the front desk/record room to a secure location in the clinic area and appropriately handled by clinical staff while delivering services to patients. All health department staff must be fully trained and familiar with the clinic's internal routing system for patient records from front desk/record room to lab, private office/exam room, WIC office, patient education/counseling areas, check-out and back to front desk/record room.

- When medical records are in route from one internal location to another they must be in the possession of authorized personnel only. Patients will not be asked to carry their record from one area to another.

- Specific secure locations must be designated in each area (front desk/check-in, laboratory, multi-use clinical area, private office/exam room, WIC office, counseling areas, check-out/billing office, etc.) for holding records when they are not in use.

- Whenever possible medical records should be completed and returned to the record room no later than the following day the service is provided, date entry and/or billing completed or necessary documentation is added to the record. Records should not be held by personnel for extended periods of time without good reason and authorization from Privacy Officer.

- Removal of medical records from the facility for reasons other than the delivery of services in the home or other non-traditional site is prohibited without good reason and authorization from the Privacy Officer. When records are removed from the facility to provide services off-site, policies/procedures for removal of PHI from the facility must be followed.

- At the close of business day the Privacy Officer or his/her designee will assure that file cabinets in the records room will be locked and the door to the room will be closed and locked (when applicable).

Staff Lounge/Break Room/Kitchen/Restrooms

- Whenever practical keep doorways closed in common areas where staff may frequent when not interfacing with patients or utilize signs to prevent and/or discourage entry by unauthorized persons.

- Family members visiting staff in the clinic must be accompanied at all times when they are in the building including when they are in areas designated for the comfort and personal utilization of staff.

- Charts, lab slips, and/or any other form of protected health information must not be left unattended in lounge, break areas, kitchen, restrooms, etc.

- Staff are discouraged from using break and personal areas of the building for discussing or sharing information regarding the care and/or condition of patients. Such discussions or consultations should be done in secure locations in the clinical area or private offices where the potential for disclosure through verbal communications is minimized.

SANCITONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
REMOVAL OF PROTECTED HEALTH INFORMATION FROM THE CLINIC

PURPOSE

To provide guidelines for the removal of Protected Health Information (PHI) from the facility in a way that protects the client's confidentiality in accordance with the Health Insurance Portability and Accountability Act of 1996.

Definitions:

PHI:	Individually identifiable health information that is: 1) Transmitted by electronic means, 2) Maintained in any medium described in the definition of electronic media (Sec. 162.103), and 3) Transmitted or maintained in any other form or medium.
Electronic Media:	The mode of electronic transmission. It includes the internet (wide-open), Extranet (using internet technology to link a business with information only accessible to collaborating parties), leased lines, dial up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media. (Sec. 162-103)
Mobile Media:	Any type of storage media that is easily transported from one place to another. Examples include disks, CD-ROMS, magnetic tape, laptops, and Personal Digital Assistants (PDA's).

GENERAL POLICY

All reasonable efforts must be taken to protect and ensure client's PHI remains secure and confidential when removed, stored or transported away from the facility.

Where electronic media is concerned, it is recommended that all files containing PHI be stored on file servers rather than hard drives of desktops computers, laptop computers, and other mobile media. This greatly simplifies the protection of PHI as well as improves the ability to provide backup and recovery of the PHI. It is recognized however, that there are situations that require PHI to be stored on media other than file servers. In such situations, adherence to the following procedures is required.

PROCEDURES

Removing/Transporting PHI from the Facility

- Approval must be obtained from the Privacy Officer before any PHI can be removed from the facility.
    - The Privacy Officer may grant standing approval for employees who regularly remove PHI from the facility in the performance of their jobs. It is recommended that the Privacy Officer maintain a log of these approvals.

- From time to time employees may need to remove PHI from the facility; prior to removal they must obtain permission from the Privacy Officer.

- The removal of the PHI from the facility must be logged using the attached log sheet or another log sheet developed by the Privacy Officer. Recommended fields to log include:

  - ID number of media
  - Creation date
  - Created by
  - Contents
  - Location where normally stored
  - Name of borrower
  - Date borrowed
  - Date returned
  - Date of destruction (when applicable)
  - Method of destruction (when applicable)
  - See Attachment B, sample log for a model log sheet

- Secure the records according to DCH policy for transport, in a locked or sealed container.

- You will be held personally responsible for the security of PHI in your possession and if a breach of confidentiality occurs you are liable.

- Upon returning the PHI to the facility, update the log.

Storage Facility

- Notify Privacy Officer of need to move records to a secure storage facility.

- Privacy Officer will assure that storage facility is a secure location with access being limited to authorized personnel or covered business partners only by way of key, security id or key card.

- Upon approval by the Privacy Officer procedure for REMOVING/TRANSPORTING PHI FROM THE FACILITY must be followed.

Mobile Media

- Personal Digital Assistants (PDA'S) containing PHI must be password protected so that a password is required to boot the PDA.
- Laptop computers containing PHI must be physically secured when not in use or when left unattended. This may be accomplished by placing the laptop in a locked cabinet/closet, leaving the laptop in a locked office, or use of a cable and lock type security system that allows the laptop to be secured to furniture.

- As an additional means of protection, it is highly recommended that a file system encryption technology be used to encrypt files containing PHI. This technology would require the use of a key, PIN, or both to gain access to the information in the file.

- Disks, CD's, Magnetic Tape and similar storage media containing PHI must be logged and tracked for accountability according to the procedure for REMOVING/TRANSPORTING PHI FROM THE FACILITY.

    - Media of this type must be:

        - Clearly labeled to include Name of Owner, Contents and a Confidentiality Statement.

        - Assigned a sequential number by the Privacy Officer.

        - Destroyed in compliance with the POLICY ON DESTRUCTION OF PROTECTED HEALTH INFORMATION when no longer needed.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

.

DISTRICT 2 PUBLIC HEALTH
PATIENT CHECK-IN AND CHECK-OUT

PURPOSE

To ensure the privacy of our patient's health information.

GENERAL POLICY

To ensure the privacy of our patient's health information, District 2 Public Health shall utilize best efforts for privacy during the check-in and check-out process. This may include the installation of physical dividers, using written enrollment forms, or interviewing patient in a private interview area. Employees should never orally discuss a patient's private health information or income verification while at the front desk and in hearing distance of other individuals.

Further, at no time should any employee leave any forms or other items that contain the patient's health information on the top of the counter at the front desk or any other location where individuals in the waiting room can view them. "Sign-in" sheets will only be used to collect limited information such as the patient's name, time of arrival, whether they are a new or established patient, and if there are any changes in their insurance, address, telephone number, etc.

PROCEDURES

Sign-In

The receptionist will instruct the patient to sign in on the sign in form (Attachment A) located at the front desk and have a seat. The receptionist will review the sign in sheet to determine if the patient is a new patient or an established patient and prepare the forms for the patient to complete.

New Patient

When a new patient comes into the office for the first time he/she is given a Notice of Health Information Practices (Attachment M) which outlines our standards on how their medical information is protected as well as outlines their rights to view and copy their medical information. The Notice includes a perforated acknowledgement that the patient should sign; listing any restrictions they wish for their protected health information. This Notice is given to the patient in addition to our other "standard" forms for new patients, such as the new patient information form, insurance information form, and Consent for Treatment form. The patient is instructed to have a seat, read and fill out the forms, sign and return them to the front desk when completed. The perforated section of the Notice must be placed in the left side of the chart directly behind the Eligibility form so that the signed Notice and easily be retrieved.

If the patient has any questions about the Notice or wishes to request restrictions on their health information, the receptionist if well-trained may answer the patient's questions or call the clinics Privacy Officer.

For patients who refuse to sign the Notice of Health Information Practices, indicate on the form that we attempted to provide the information but the patient refused to sign on the perforated section and sign

your name. Then proceed to provide services under the assumption that they had signed. We will not deny services because they are unwilling to sign the acknowledgment of the Notice.

Established Patient

When an established patient comes into the clinic, the receptionist will give the patient forms for established patients, such as the established patient information form, change of insurance, and Consent for Treatment form. The patient should be instructed on how to fill out the forms, returning them to the front desk when completed.

The receptionist will verify that District 2 Public Health has a current Notice of Health Information Practices signed by the patient and on file. If not, the receptionist will follow the instructions for a new patient check-in above, and then skip below to the next step.

Registration

Once the patient has completed the necessary forms and returned them to the receptionist, the receptionist will remove the forms from the top of the desk and place them in a location where individuals in the waiting room cannot view them (e.g., below the top of the desk, on the opposite side of the computer terminal, etc.). The receptionist will ask the patient to return to the waiting room to wait for his/her name to be called. The receptionist can then enter the new or updated information into the patient record system.

Call Back

When an exam room is ready a nurse or other staff member will go to the waiting room and call the next patient's name. At no time will this individual announce the reason for the patient's visit, any symptoms the patient may be experiencing, or any tests to be conducted on the patient. The employee is limited in saying the patient's name and the physician's name that will see the patient; no other health-related information should be given to the patient.

If the patient asks the nurse or other employee a question regarding their health status, inform the patient the employee will answer their questions after they enter the exam room and close the door. Inform the patient this is to protect their privacy.

Check Out

After the patient has completed their visit and is back in the waiting room the receptionist will present the patient with a statement of how much they owe (if necessary) and ask how they would like to make payment (cash, check, credit card). If the patient wants to discuss more sensitive patient information regarding their account, the receptionist should make a judgment call to take the patient to a more confidential area.

At no time shall the receptionist or other employee leave a patient's bill, drug prescription, or other item unattended at the front desk. If the patient is not ready to accept these items, the receptionist will keep them behind the counter at the front desk until the patient is present to accept these items.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
THE NOTICE OF PRIVACY PRACTICES FOR PROTECTED HEALTH INFORMATION

PURPOSE

To assure every effort is made to adhere to the Health Insurance Portability and Accountability Act of 1996 to provide individuals with adequate notice of the uses and disclosures of protected health information that may be made by District 2 Public Health and of the individual's rights and District 2 Public Health's responsibilities with respect to protected health information.

GENERAL POLICY

In a direct treatment relationship it is our responsibility to make a good faith effort to obtain and individual's written acknowledgement of receipt of District 2 Public Health's Notice of Privacy Practices no later than the date of the first service delivery and must post the notice in a clear and prominent location at the service delivery site. This notice must be available on request for individuals to take with them.

PROCEDURES

- The Notice of Privacy Practices and the name of and phone number of the current Privacy Officer are to be posted in a clear and prominent location in all health departments in District 2 and copies for the clients to take with them will be available at each client check-in site.
    - If District 2 Public Health should revise the Notice of Privacy Practices the revised notice will be posted in a clear and prominent location and the revised copies will be made available to clients.
- When a client presents for service he/she will be given a copy of the Notice of Privacy Practices and will be asked to sign an acknowledgement of receipt of the notice.
    - When the client signs the acknowledgement of receipt, it is to be attached to the client's paper record or in the case of service without paper record the receipt will be placed in alphabetical order in file cabinet in medical record room. There is no time limit on retention of this form at this time.
    - If the client refuses to sign this receipt the employee is to sign the Attempt to Obtain Signature form and file this in the client's record or in file cabinet in alphabetical order in medical record room in case of service without paper record.
    - If the client requests to limit the disclosures of his/her medical records the client is to be given the name and phone number of the health department's Privacy Officer. They are to check the appropriate block on the receipt form which is to be given to the health department's Privacy Officer by an employee.
- In emergency situations the notice is required to be provided when it is reasonably practicable after the emergency situation.

- All requests for limited disclosure of private health information will be handled by the health department's Privacy Officer.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
TELEPHONE REQUESTS FOR PHI

PURPOSE

To ensure the privacy of our patient's health information when disclosing private health information over the telephone.

GENERAL POLICY

Telephone conversations present the most difficulty in protecting our patient's privacy. To ensure the privacy of our patients health information District 2 Public Health shall utilize best efforts to verify the person calling by telephone requesting protected health information, is indeed the person they state they are and also verify that we have permission to provide the caller with the requested information.

PROCEDURES

You should always be on guard when you speak on the telephone. Never assume the caller is who they say they are; treat callers as people who are impersonating patients in an attempt to again access to personal health information. This is true even if you know the patient or recognize his/her voice; you simply do not know who is calling.

If The Caller Is The Patient:

If a caller claims to be a patient of your health department you must take reasonable steps to verify his/her identity. Therefore, before you reveal any personal health information over the telephone (including billing issues); you must take several steps to verify the identity of the caller. You should ask the caller a few questions, such as the following:

1. What are the last four digits of your Social Security Number?
2. What is your date of birth?
3. What is your mailing address?
4. What is your maiden name?
5. What was the service provided and what was the date?

If the caller **cannot** answer questions, he/she must come to the health department for PHI requested.

Once you have verified their identity by using the above questions, you may disclose personal health information to the patient.

Treatment Provider

Use your best effort to verify the person calling is another treatment provider of the patient. Suggested ways to do this are:

1. Tell the caller we will call them back at their published phone number.
2. Check the patient's record to see if they have been referred to this treatment provider or they have listed this treatment provider in their medical history.

If you feel uncomfortable disclosing the requested information to the caller refer the caller to the Privacy Officer.

If you feel sure the caller is another treatment provider you may share any information as long as it relates to the treatment of that patient, but it should comply with the "minimum necessary" standards. Log the disclosure in the Disclosure of Protected Health Information Log.

If The Caller Is Not The Patient And Not Another Treatment Provider

You can only provide protected health information to the patient or to another treatment provider. You are not permitted to disclose any protected health information to anyone else, unless you have written authorization from the patient or unless the disclosure is required by law. This includes spouses, children, friends, attorneys, or other "representatives" of the patient.

If the caller isn't the patient or another treatment provider of the patient, ask:

1. Who they are?
2. What information they are requesting?
3. Why do they need this information?
4. Check the medical record to see if there is an authorization to release this information.
5. If not, explain to the caller that we are not permitted to disclose this information without authorization from the patient.

If the caller is not satisfied, offer to refer him/her to the Privacy Officer who will explain why the health department is limited in what we can reveal over the telephone.

If a spouse is calling to make a payment on an account, you may take the information but you cannot reveal any information, including the current balance. In this situation you may say, "I would be happy to take this information, but I cannot disclose any information to you". This will also include parent(s) requesting information concerning daughter/son who are old enough to request services and have signed a Consent to Treatment form.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
MAIL DISTRIBUTION

PURPOSE

To assure every effort is made for adherence to the Health Insurance Portability and Accountability Act of 1996 and the Open Records Act OCGA § 50-18-70 et seq., and the Open Meetings Act OCGA § 50-14-1 et seq. Amendments effective July 1, 1999.

GENERAL POLICY

Adherence to District 2 Public Health's policy of Confidentiality is expected when receiving and distributing mail containing protected health information. Properly completed and signed authorizations must be obtained to release protected health information unless specifically mandated through State Public Health Law or regulations for internal public health use as stated in the Privacy Notice.

PROCEDURES

Incoming Mail

- The designated staff will stamp the date on the envelopes or package of all mail/courier received in this office the day it arrives.

- The front office staff will deliver the stamped, unopened envelopes or package to the designated program staff, support staff or person to whom the mail is addressed.

- The designated or authorized staff will open the mail, stamp the date on the front page of the material received, attach the envelope and review it for requests, due dates or deadline.

- Should the information have requests pertinent to the Open Records or Open Meetings Acts, the person opening the mail will immediately deliver it to the person it is addressed to. If this person is not available the information should be given to the Privacy Officer or Supervisor on duty. Otherwise, the staff will distribute the mail to their program personnel. If the program personnel are out of the office the secretary will notify them or their supervisor of any urgent requests or immediate due dates.

- The designated staff will not open mail marked PERSONAL or CONFIDENTIAL without the written authorization of the person the mail is addressed to.

- The front office staff will sign for all registered mail and notify the appropriate person or designated secretary or program staff immediately.

- Mail or courier packages that are not specifically addressed to a person or program should be opened by the front office staff, reviewed and delivered according to content.

- If the designated employee or program staff is not available, the front office staff will deliver the mail to the staff designated as backup.

- Incoming mail for staff should be located in a secure area that is protected from public view and available only to the staff.

Example:

PROGRAM MANAGER	DESIGNATED SECRETARY/SUPPORT STAFF	BACKUP STAFF
Susan Doe Director of Nursing & Clinical Services	Debbie Fawn	Cassandra Deer
Wendy LeFleur Women's Health Programs	Tessie Honey	Cassandra Deer
Amy Flannigan Child Health Programs	Cassandra Deer	Debbie Fawn
Joy Granger Chronic Disease Programs	Debbie Fawn	Tessie Honey

In the event an unauthorized person receives mail containing PHI, they should notify the Privacy Officer for that agency immediately.

Outgoing Mail

- Envelopes or packages must be sealed with the mailing address and return address clearly written on the outside of the envelope/package.

- Place in the centrally designated location for the facility.

- Assure proper postage is stamped clearly above the address in the upper right hand corner of the envelope or package.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
FAXING PROTECTED HEALTH INFORMATION

PURPOSE

To provide guidelines for receipt, use and dissemination of protected health information by facsimile. The information may include population-based activates, individual healthcare, prevention of injury, transmission of disease, premature mortality, promotion of health including community health needs assessments, status of the community through public health surveillance and epidemiological research, developing public policy and responding to public health needs and emergencies.

GENERAL POLICY

Adherence to District 2 Public Health's Policy of Confidentiality is expected with the use of facsimile when transmitting patient health information. Properly completed and signed authorizations must be obtained to release patient information unless specifically specified through State Public Health Law or regulations for internal public health use. An authorization transmitted via fax machine is acceptable with verification for signature. In medical emergencies the information may be released without authorization when the provider or business associate requesting the information is required by law to treat the individual or when there are substantial communication barriers or threats of the health of the public. Health Departments may fax medical records using a Notice of Confidentiality on the agency letterhead. When using faxed duplicates instead of the original medical record, destroy the copied material once the use is completed. Fax users must be instructed on the proper procedures for handling of confidential information. It is recommended that specific patient healthcare information be faxed only when the data are to be used for patient care. HIPAA provisions allow facsimile of data for treatment, payment and healthcare operations without an authorization. Use of the fax for these reasons should only occur when the original document or mail-delivered photocopies will not serve the purpose. Fax machines must be located in a secure area that is protected from public view and available only to those employees legitimately entitled to access protected health data.

PROCEDURES

For Transmitting PHI

- Use a cover letter, health department letterhead with confidentiality statement, for each fax transmission and retain it in correspondence.

- Verify by telephone when possible the availability of the receiver and log the fax transaction.

- Notify recipients of any misdirected or returned fax and file an incident report.

- When the faxed information is to be included in a medical record, it must be clearly legible, complete, accurate, and dated with appropriate signatures as indicated.
- Faxed data must include:
  Date and time of fax transmission
  Sending facility's name and address
  Sending facility's telephone and fax number

Sender's name
Receiving facility's name and address
Receiving facility's telephone and fax number
Authorized receiver's name
Number of copies sent
Statement regarding disclosure
Statement regarding confidentiality

If a fax transmission fails to reach the recipient, check the internal logging system of the fax machine to obtain the recipient's fax number. Give the Privacy Officer the fax or letter. The Privacy Officer will then contact the requestor to get more details about the information requested and/or the intended use of the information. For information requested related to a legal proceeding, a copy of an official judicial subpoena or court or is required.

For Receiving and Handling of Fax

- Remove any incoming material
- Count the number of pages received
- Follow any instructions on the cover letter
- Insure that the information is routed to the intended receiver in a prompt and secure manner.
- If the recipient is not available to receive the information, seal the faxed documents in an envelope and set aside for pickup, or deliver to the recipient's private mail or pick up basket.
- If the County Privacy Officer deems necessary, following receipt of a misdirected fax, send a request using the incorrect fax number, explain the misdirected information and ask for destruction of all documents received from the said facility. Complete an incident report and forward to District Privacy Officer.

Examples of Confidentiality Statements

"The information contained in this facsimile message is privileged and confidential information intended for the use of the addressee listed above. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this Tele-copied information is strictly prohibited. If you have received this facsimile in error, please destroy it and immediately notify us by telephone by calling us at the number above.

"The information contained in this facsimile message is privileged and confidential information intended for the use of the addressee listed above. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are herby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this facsimile is strictly prohibited. If you have received this facsimile in error, please destroy it and immediately notify us by telephone by calling us at the number above."

"This facsimile may contain confidential or privileged information and is intended only for the recipient named above. Receipt of this transmission by any person other than the intended recipient does not

constitute permission to examine copy or distribute the accompanying material. If you receive this facsimile in error, please notify us by telephone and return the original facsimile to us by mail."

"This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the dissemination, distribution or copying of this communication is strictly prohibited. If you received this communication in error, please notify us immediately by telephone and return the original message to us at the above address. Thank you."

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
E-MAIL REGARDING PROTECTED HEALTH INFORMATION

PURPOSE

To assure that client protected health information (PHI) confidentiality and privacy is maintained in accordance with the Health Insurance Portability and Accountability Act of 1996.

GENERAL POLICY

Our clients' PHI is considered private and confidential and as such should remain secure at all times. Whereas every attempt is made to provide security for our e-mail system it is not considered to be a completely secure environment. Therefore, every attempt should be made to de-identify PHI and adhere to the minimum necessary rule when sending PHI through email.

PROCEDURES

PHI in E-mail

- Staff will de-identify PHI where applicable
- Staff will send minimum necessary information
- Email addresses must be verified; do not use group addresses
- Add a confidentiality statement to the body of the email message
- Send PHI as an attachment
- E-mail should be destroyed in accordance with the Destruction of PHI Policy

Receiving PHI in E-Mail in Error

- Print the e-mail and attachments containing PHI
- Delete the email and attachments containing PHI
- Empty e-mail trash
- Notify Privacy Officer of incident providing printed documents containing sender name, sender location and PHI received

Example Confidentiality Statement

"This message and any included attachments are from (your health department name) and are intended only for the addressee(s). The information contained herein may include privileged or otherwise

confidential information. Unauthorized review, forwarding, printing, copying, distributing or using such information is strictly prohibited. If you receive this message in error or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by email. Thank you."

SANCTION

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTICT 2 PUBLIC HEALTH
PATIENT ACCESS TO PROTECTED HEALTH INFORMATION

PURPOSE

To protect and insure confidentiality of our patients' protected health information.

GENERAL POLICY

The HIPAA Privacy Rule requires a health care organization to give a patient access to (inspect and obtain a copy of) the protected health information it keeps on that patient in a "designated record set", for as long as it is maintained in the "designated record set". Patients have a right to protected health information that is used to make decisions about such things as their healthcare and insurance claims. According to the Privacy Rule the protected health information must be provided within 30 days of the request.

The Georgia Open Records Act (OCGA § 50-18-70(b), provides the medical records are exempt in their disclosure would be an invasion of privacy. Since a patient's access to their own medical records would not be an invasion of privacy, all requests by patients to access their own protected health information shall be permitted, under the Georgia Open Records Act. Furthermore, access to the protected health information will be permitted within 3 business days as required by the Act.

PROCEDURES

Identify The Requestor By Asking Them:

1. Who they are – ask to see their driver's license, employment ID or other picture identification?

2. What information they are requesting?

3. Why do they need this information?

Once you are assured the requestor is the patient, then you may disclose the information. Please refer to The Georgia Open Records Act for more information.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
PERSONAL REPRESENTATIVE'S ACCESS TO PROTECTED HEALTH INFORMATION

PURPOSE

To protect and insure confidentiality of our patients' protected health information.

GENERAL POLICY

The HIPAA Privacy Rule requires a health care organization to give a patient's personal representative access to (inspect and obtain a copy of) the protected health information it keeps on that patient in a "designated record set" for as long as it is maintained in the "designated record set". Personal representatives have a right to protected health information that is used to make decisions about such things as the patient's healthcare and insurance claims. Personal representatives as defined in the Georgia Medical Consent Law, OCGA § 31-9-2 are defined as:

1. Any person authorized to give such consent for the adult under a healthcare agency complying with Chapter 36 of Title 31, the "Durable Power of Attorney for Health Care Act".

2. In the absence or unavailability of a living spouse, any parent, whether an adult or a minor, for his minor child.

3. Any married person whether an adult or a minor for himself and for his spouse.

4. Any person temporarily standing in *loco parentis*, whether formally serving or not, for the minor under his care; and any guardian for his ward.

5. Any female regardless of age or marital status, for herself when in connection with pregnancy or the prevention thereof, or child birth.

6. Upon the inability of any adult to consent for himself and in the absence of any person to consent under 2-5 above, the following persons in the following order of priority:

    A. Any adult child for his/her parents

    B. Any parent for his/her adult child

    C. Any adult for his/her brother or sister

    D. Any grandparent for his/her grandchildren

According to the Privacy Rule, the HIPAA rights including the right to sign a Notice of Health Information Practices, an authorization form and access rights, all flow to whomever has the "right to make health care decisions". The question then becomes whether the minor patient has the right to make his/her own health care decisions. Please refer to the Georgia Medical Consent Law.

It is the policy of District 2 Public Health to abide by this rule according to the following procedures:

PROCEDURES

The County Privacy Officer or treating provider will make decisions regarding a personal representative's request to access the patient's protected health information. The District Privacy Officer or County Privacy Officer (if not the person making the initial decision) will review decisions regarding a denial to allow a personal representative to access the patient's protected health information, if the personal representative appeals the decision and requests a review, and if the appeal meets the appeal guidelines (see exceptions - non reviewable below).

Requests for access to protected health information must be acted on within the following timeframes:

- Within 30 days of receipt of request, if maintained or accessible on-site
- Within 60 days of receipt of request, if not maintained or accessible on-site
- Up to an additional 30 day extension is allowable if you are unable to act on the request within the deadline, but you must provide the personal representative a written reason for the delay and the date by which you will complete your action on the request. This written statement describing the reason must be provided within the standard deadline. You may only extend the deadline once per request for access.

If the same protected health information is maintained at more than one location, you are only required to produce the information once per request for access.

There are eight exceptions to this requirement. If these exceptions apply, covered entities may deny access, but are not required to do so. You may provide all of the information requested or evaluate the requested information, consider the circumstances surrounding the personal representative's request, and make a determination as to whether that request should be granted or denied, in whole or in part. If you deny access, in whole or in part, you must, to the extent possible, give the personal representative access to any other protected health information requested after excluding the protected health information to which you have a ground to deny access. The eight exceptions are as follows:

Exceptions- Non Reviewable:
(If you deny access, personal representative does not have a right for a review.)

Psychotherapy Notes- notes recorded by a health care provider who is a mental health professional documenting contents of conversation during a counseling session and that are separated from the remainder of the patient's medical record.

Anticipation of a Legal Proceeding- information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

CLIA- information that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988.

Clinical Trial- information that was obtained in the course of a clinical trial or research, if the patient agreed to the denial of access in consenting to participate. Once the trial or research is completed, the personal representative's right of access is reinstated.

Promise of Confidentiality - (all three must apply)

1. Information obtained from someone other than a health care provider, and

2. Obtained under the promise of confidentiality, and
3. The inspection and copying would likely reveal the source of the information.

Exceptions- Reviewable Exceptions

(If you deny access you must have an appeal process in place to review the denial.)

Endanger the Life- a licensed health care professional determined the inspection and copying was reasonably likely to endanger the life or physical safety of the patient or another person. Under this reason for denial, you may not deny access on the basis of the sensitivity of the health information or the potential for causing emotional or psychological harm.

Serious Harm- the information requested makes reference to someone other than the patient (and other than a health care provider) and a licensed health care professional determined the inspection and copying was reasonably likely to cause substantial harm to the other person.

Personal Representative- the request was made by the patient's personal representative, and a licensed health care professional determined the inspection and copying was reasonably likely to cause substantial harm to the patient, his or her personal representative, or another person.

PROCEDURES

Simple Request: (a verbal request that can be answered simply, if they have permission, by asking limited information)

1. Identify them by asking them:

    A) Who they are? - ask to see their driver's license, employment I.D., or other picture identification.
    B) What information they are requesting?
    C) Why do they need this information?

2. Check the medical record to see if there is an authorization to release this information.

3. Check the Notice of Health Information Practices Acknowledgement to see if this person is listed as a personal representative.

4. If authorized, release information and record on Disclosure of Protected Health Information Log

5. If not, explain to the requestor that we are not permitted to disclose this information without authorization from the patient. Ask them to complete the papers described under Complex Request.

Complex Request:

1. Receive the request from the personal representative.

2. Instruct the personal representative to complete the 1st and 2nd pages of "Personal Representative's Request for Access to Protected Health Information", (Attachment C) sign it, and return the completed form to you.

3. Process the request by completing the top part of the 3rd page of the form.

4. If access is allowed, in full, notify the personal representative of your decision by sending them a letter (see example labeled Attachment D)

5. Allow access by:

   A) If personal representative requests to review the patient's PHI, arrange for a mutually convenient time and place for the personal representative to inspect the protected health, or obtain a copy.

   B) If information is maintained electronically, you may print a copy of the information and allow the personal representative to view the printout on-site. You may discuss the request with the personal representative as necessary to facilitate the timely provision of access.

   C) If the personal representative requests an explanation or summary of the information provided, and agree in advance to associated fees, you may charge a reasonable fee, to be set by District 2 Public Health, for preparing the explanation or summary as well.

   D) If the personal representative requests a copy of the information, you must do so, and you may charge up to a maximum of $20 for research and retrieval, $7.50 for each record certified, $.75 per page for the first 20 pages of the patient's record which are copied, $.65 per page for pages 21 through 100; and $.50 for each page copied in excess of 100 pages (See OCGA § 31-33-3).

   E) If the patient requests that you mail a copy of the information, you must do so, and you may charge the actual cost of postage for mailing PHI.

Complete Section 1 of Attachment C and record the disclosure on the Disclosure of Protected Health Information Log.

6. If Access is allowed, in part, notify the personal representative of your decision by sending them a letter (see example labeled Attachment E). Then go back to step 5 to process request. Complete Section 2 of Attachment C. If access is denied, notify the personal representative of your decision by sending them a letter (see example labeled Attachment E). Complete Section 3 of Attachment C.

7. If the personal representative requests a review of the decision, arrange for the reviewing official to review the decision within 30 days following the request for the review and record their response in the Section 2 or 3 of Attachment C. Notify the personal representative of the reviewing official's decision (see example labeled Attachment F).

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
REQUESTS FOR PHI BY OTHER THAN PATIENTS, THEIR TREATMENT PROVIDERS, OR THEIR PERSONAL REPRESENTATIVE

PURPOSE

To protect and insure confidentiality of our patient's protected health information.

GENERAL POLICY

It is the policy of the District 2 Public Health that the identity and authorization of all persons requesting protected health information are confirmed prior to release of any information.

PROCEDURES

You can only provide protected health information to the patient or to another treatment provider. You are not permitted to disclose any protected health information to anyone else, unless you have written authorization from the patient or unless the disclosure is required by law. This includes spouses, children, friends, attorneys, or other "representative" of the patient. You may receive a request for a patient's protected health information from someone other than the patient, their personal representative, or their treatment provider. When you receive such a request, you must follow these steps before revealing ANY protected health information. No matter how insistent the requestor, you CANNOT disclose any information about the patient before completing these steps.

In person: If someone, other than the patient, their personal representative, or their treatment provider comes in to the office and makes a request for a patient's protected health information, you must first verify the identity of the individual.

Simple Request: (a verbal request that can be answered simply, if they have permission, by asking limited information)

1. Identify them by asking them:

    A) Who they are? - ask to see their driver's license, employment I.D., or other picture identification

    B) What information they are requesting?

    C) Why do they need this information?

2. Check the medical record to see if there is an authorization to release this information

3. Check the Notice of Health Information Practices Acknowledgement to see if this person is listed as a personal representative.

4. If authorized, release information and record on Disclosure of Protected Health Information Log (Attachment G).

5. If not, explain to the requestor that we are not permitted to disclose this information without

authorization from the patient. Ask them to complete the papers described under Complex Request.

If the requestor is unhappy, refer him or her to the Privacy Officer, who will explain why the health department is limited in what we can reveal about our patients.

Complex Request: (a verbal request that requires more detailed examination for authorization to release protected health information.)

1. Identify them by asking for their driver's license, employment I.D. badge, or other picture identification.

2. Make a copy of the identification.

3. Ask the requestor to fill out and sign the Requests for PHI by Other than Patients, Their Treatment Provider, or Their Personal Representative form (see Attachment H).

4. Take the completed form, the copy of the picture identification, and present them to the Privacy Officer for his or her approval.

5. You should then enter the request on the Disclosure of Health Information log (see Attachment G).

If the requestor is a public official, you must verify the identity of the individual making the request by examining an official letter from the agency or department where the individual is employed (or represents), a government identification badge, or similar proof of official status. The individual must also present to you written evidence of the agency's legal authority to obtain the information.

If the requestor is an attorney and the information is to be used in a legal proceeding, you must ask for and copy an official judicial subpoena or other official court document supporting the attorney's legal authority to request the patient's information. This must be approved by Dr. Westfall before patient information can be released.

Upon verification of the individual's identity and completion of the Requests for PHI by Other Than Patients, Their Treatment Provider, or Their Personal Representative form, the Privacy Officer must approve or deny the request. After approval and entering the request in the logbook, you may then disclose the information to the requestor. If denied, complete the "Denial of Request for PHI by Other Than Patients, Their Treatment Provider, or Their Personal Representative" form (see Attachment I) and give a copy to the requestor.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
AMENDING A PATIENT'S MEDICAL RECORD

PURPOSE

To provide guidelines for responding to a patient's request to amend their medical record.

GENERAL POLICY

The HIPAA Privacy Rule gives individuals the right to request an amendment to their protected health information as long as the health department maintains the information.

PROCEDURES

Patients who believe information in their health records is incomplete or incorrect may request an amendment or correction to the information. The employee should follow the steps outlined below when a patient makes such a request.

That patient may approach the author of the entry (the treating provider), point out the error, and ask the author to correct it. Alternatively, the patient can contact the Privacy Officer to ask for a correction to his/her medical information.

For "simple" corrections, such as name, address, age, and other non-medical information, the author can correct the entry or add a progress not to clarify content. For more "complicated' corrections, the Privacy Officer should be contacted, and he or she will assist the patient in completing the health record correction/amendment form. If the entry author is unsure as to whether the correction should be considered "simple" or "complicated", he or she should contact the Privacy Officer for assistance.

Upon completion of the form, the Privacy Officer will give a copy of the form to the patient, place a copy in the patient's health record immediately, and route the original form with the record to the author. If the author chooses to add a comment to the amendment/correction form, a copy of the form will be routed to the patient with the author's comments. In those instances, the original correction/amendment with the author's signature will replace the copy previously placed in the patient's record.

Timely Action

Once a health record correction/amendment form has been received, you must respond to the request within 60 days. If you are unable to meet the deadline, you may extend the deadline up to 30 days. However, if you choose to extend the deadline, you must inform the patient in writing, within the initial 60-day period, of the reason for the delay and the date you will complete your action on the request. The deadline can only be extended once per request for amendment.

Accepting the Amendment

If, after reviewing the request for amendment, the author and/or Privacy Officer accept the request, the following steps must be completed within the time period:

1. Notify the patient, in writing, that you have accepted his/her request for amendment.

2. Copies of the correction/amendment form will be furnished to those individuals or organizations the patient deems necessary and documents on the correction/amendment form. Copies of the correction/amendment form will also be furnished to the facility's business associates or others who have the information subject to the amendment and that may have relied on or might rely on that information to the detriment of the patient.

3. The author should make an entry at the site of the information that is being corrected or amended indicating, 'See correction/amendment." The correction/amendment form will be attached to the incorrect or amended entry.

Whenever a copy of the corrected/amended entry is disclosed, a copy of the correction/amendment form will accompany the disclosed entry.

Denying the Amendment

If you deny a request for correction/amendment, you must notify the patient in writing. This written denial must include the basis for the denial, how the patient may file a written statement disagreeing with the denial, and how the patient may make a complaint to the Privacy Officer or HHS. This written denial must also state that if the patient chooses not to file a statement of disagreement, he/she may request that you include the original request for amendment and your denial of the request with any future disclosures of the PHI that is the subject of the request for amendment.

Also, the patient is permitted to submit a written statement disagreeing with the denial and the basis of the disagreement. This statement is limited to 250 words. If the patient submits a statement, you may prepare a written rebuttal to the patient's statement of disagreement. If you do prepare a rebuttal, you must provide a copy to the patient.

If the patient submits a written statement of disagreement, an entry should be made at the site of the disputed information indicating "See Denied Amendment". The following information should be attached to the entry:

- The patient's request for amendment
- Your denial of the request
- The patient's statement of disagreement (if any)
- The written rebuttal to the patient's statement of disagreement (if any)

If the patient submits a written statement of disagreement, then all of the appended information, or an accurate summary of it must be included with each subsequent disclosure of the PHI to which the disagreement relates.

If the patient does not submit a written statement of disagreement you must include the appended information ONLY if the patient requests that you do so.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
BUSINESS ASSOCIATES

PURPOSE

To assure every effort is made to adhere to the Health Insurance Portability and Accountability Act of 1996.

GENERAL POLICY

Under current federal regulations, District 2 Public Health is required to ensure all individuals and organizations who have been deemed "Business Associates" as that term is defined in the federal regulations follow our policies and procedures on protecting our patient's health information. This includes both current Business Associates (BAs) as well as future Bas. The Privacy Officer shall make the final determination as to 1) Whether the organization with which the health department has a relationship is a BA within the meaning of the federal regulations, and 2) Whether the health department has received adequate written assurances that the other entity will abide by our privacy and security policies.

PROCEDURES

Step One: Determining District 2 Public Health's Business Associates

The federal regulations define a BA as an entity that performs certain services "for" (County) Board of Health, or an entity that acts "on behalf of "District 2 Public Health as long as the services involve the use or disclosure of our patient's protected health information. Some examples of a BA are:

- Legal
- Actuarial
- Accounting
- Consulting
- Management
- Administrative accreditation
- Data aggregation
- Financial services

If any entity performs the above- mentioned services "on behalf of" District 2 Public Health AND the entity will use or disclose protected health information, they are deemed a Business Associate and therefore require the appropriate safeguards in any agreement.

Some entities may be obvious Business Associates; others however may require more investigation. The Privacy Officer may need to review each entity's agreement with the health department as well as how the other entity interacts with District 2 Public Health. Upon reasonable investigation the Privacy Officer will determine whether there is a need for the BA safeguards as specified in the federal regulations and will document his/her decision, which will be kept on file as an attachment to the current agreement or contract.

Step Two: Establishing Safeguards

Once a BA has been established the Privacy Officer will use the BA Checklist survey to analyze whether adequate assurances are in place. The Business Associate is not required to use our privacy policies and may submit their privacy policies to the Privacy Officer for his/her review. The Privacy Officer may then accept the Bas policies without any additions may submit to the BA additions to provide for additional safeguards or may reject the BA's policies altogether.

However, in NO event shall District 2 Public Health agree to any relationship or sign any contract with a Business Associate prior to the Privacy Officer's documented verification of adequate privacy and security safeguards.

Current Business Associates

For current Business Associates the Privacy Officer should contact the BA and inform them that under federal regulations, District 2 Public Health must attach an addendum to the current contract between the two organizations. This addendum will add to the current agreement the necessary language so the BA and District 2 Public Health will comply with federal regulations. The Privacy Officer should contact the BA as soon as practicable and should send the addendum to the BA for their approval along with a copy of District 2 Public Health's current privacy policies.

Potential Business Associates

When District 2 Public Health begins a new relationship with another organization that involves the use or disclosure of protected health information, the other organization should be deemed a BA. The Privacy Officer must include in the agreement between the health department and the other organization language that stipulates the other organization must abide by District 2 Public Health's privacy policies and procedures.

DISTRICT 2 PUBLIC HEALTH
FILE SERVER SECURITY

PURPOSE

To provide guidelines for securing and protecting file servers that have Protected Health Information (PHI) stored on them.

GENERAL POLICY

It is critical that our clients' PHI be kept secure and confidential in accordance with District 2 Public Health's Policy on Confidentiality. Since PHI is stored on the application file server it is equally important that proper measures are taken to secure the application file server.

PROCEDURES

The following District 2 Public Health HIPAA Security Policies must be adhered to:

- Contingency Plan Policy, including:
  - Attachment A – Date Backup
  - Attachment B – Virus/Anti-Virus Policy
- Facility Access Control Policy

SANCTIONS

Violations of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
THE DESTRUCTION OF PROTECTED HEALTH INFORMATION

PURPOSE

To provide a guideline for destroying Protected Health Information (PHI) in a way that protects the client's confidentiality in accordance with the HIPAA Privacy Rule.

GENERAL POLICY

To protect and insure the clients' PHI remains secure and confidential after records are destroyed.

PROCEDURES

Protected health information should be destroyed in accordance with state approved records retention schedules (OCGA § 50-18-102). This information must be destroyed so that it cannot be read, interpreted or reconstructed. Further guidelines on records destruction can be found in DHR Operating Procedure No. IX, dated September 23, 1993. (See also DCH and DHR agency specific schedules maintained by the Georgia Secretary of State).

- Records are to be destroyed according to schedule referenced above if the schedule permits destruction.
- Records not specified in the schedule referenced above should be destroyed whenever they are deemed of no further use.

Methods of Destruction

- Paper records must be shredded or burned.
- Microfilm records must be burned or destroyed by use of a chemical solution.
- Email and attachments should be deleted, and the "Trash" must be emptied.
- Electronic media that has stored PHI must be destroyed according to the procedures outlined in District 2 Public Health's HIPAA Security, Device and Media Controls Policy.

SANCITONS

Violations of this policy may result in disciplinary action up to and including termination of employment.

DISTRICT 2 PUBLIC HEALTH
NOTIFICATION IN THE CASE OF A BREACH

PURPOSE

To ensure compliance with the Improved Privacy Provisions and Security Provisions contained within the Privacy section of the HITECH Act with regard to notification in the case of a breach.

GENERAL POLICY

In the case of a breach of protected health information that is discovered either internally or by a business associate the District Privacy Officer shall work with District and Local management to ensure that each affected individual is notified. Affected individuals are those whose unsecured protected health information has been or is reasonably believed to have been accessed, acquired or disclosed as a result of such breach.

PROCEDURES

The notification in the case of a Breach Policy contained in the District 2 Public Health HIPAA Security Policies must be adhered to.

SANCTIONS

Violation of this policy may result in disciplinary action up to and including termination of employment.