## District 2 Public Health

# HIPAA Security Policies And Procedures

# I. Security Policy: General

**Citation: Security Standards: General Rules, 164.306**

**Policy:**

For the purposes of this District 2 Public Health Security Policies and Procedures manual, the District shall be defined as the County Boards of Health and all personnel, facilities, equipment, and programs within Public Health District 2.

The District must ensure the confidentiality, integrity and availability of all ePHI that it creates, receives, maintains or transmits, must protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA regulations.

The District shall use security measures that allow it to reasonably and appropriately implement the standards and specifications required by HIPAA. In deciding which security measures to use, the District shall take into account its size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; the cost of security measures; and the probability and criticality of potential risks to ePHI.

# II. Security Management Policy

**Citation: Security Management Process, 164.308(a)(1)**

**Policy:**

In order to prevent, detect, contain, and correct security violations, the District shall do the following:

A. **Risk Analysis.** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the County Boards of Health;

B. **Risk Management.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the requirements contained in the introductory paragraphs above;

C. **Sanctions**. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the County Boards of Health.

D. **Periodic Review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

All District 2 personnel, including regular, temporary, and contract staff, volunteers, interns, and others participating in the workplace, must comply with the District's HIPAA Privacy Policies and Procedures and HIPAA Security Policies and Procedures.

Networks, systems, and applications that may send, receive, store, or access ePHI must also comply with the HIPAA Privacy Policies and Procedures Manual and the HIPAA Security Policies and Procedures Manual.

The policies and procedures defining these Security Risk Management safeguards will be reviewed and evaluated on a periodic basis to ensure that they maintain their viability and effectiveness. The Security Officer may find the District's policies and/or procedures require adjustment(s). The Security Officer shall make the necessary modifications to the District's policies/procedures by revision or adding addendum(s) to the current policies/procedures, and shall notify all staff members of the change(s) through inter-office memorandum. This shall be done as expeditiously as possible.

# A. Risk Analysis Procedure

On a periodic basis, each and every facility within the District where ePHI is stored or used shall perform a HIPAA Security Rule risk analysis to assess any potential risks and vulnerabilities to the ePHI maintained or used at the facility.

Risk assessments may also be conducted on any entity that has signed a Business Associate Agreement with the District. Risk assessments may be conducted on any information system and/or computer equipment, and any process or procedure by which these systems are administered and/or maintained.

The Security Risk Assessment (Facility Security Audit) will be completed by the District and Local Security Officers, or his/her designees, at a minimum of once per year. The Security Risk Assessment will include a documented review of all relevant losses to data integrity as specified in the HIPAA Privacy and Security rules and regulations. The individual responsible for conducting the Assessment may use the Evaluation Checklist (located in the Forms section of this manual) or any other reasonable protocols approved by the District Security Officer(s), so long as they accurately and thoroughly assess the risks and vulnerabilities of the work unit/work site and any previous findings and remediation actions.

Periodic, random reviews of the work unit's/work site's risk analysis/assessment documents and findings, policies and procedures, and remediation actions may be conducted by the District Security Officer or designee(s).

Employees are expected to cooperate fully with any Risk Analysis being conducted on systems for which they are held accountable and/or use. Employees are further expected to work with the District and/or Local Security Officer in the development of a remediation plan.

All Analyses/Assessments will be reviewed by the Local HIPAA Security Officer, who is responsible for ensuring that the work unit/work site is compliant with the HIPAA Security Rule.

The development and implementation of remediation plans is the joint responsibility of the District and County/Program Security Officers, and the department responsible for the system(s) area being assessed.

# C. Security Sanctions Procedure

The Security Officer may find that one or more staff members either does not understand or refuses to abide by the District's HIPAA Security Policies and Procedures. The Security Officer may deny the employee access to the entire data system temporarily until the employee has been counseled by the Local Security Officer and/or the employee's supervisor.

The sanctions administered will be based on the severity of the violation in addition to other factors. To determine severity, the supervisor may solicit input from the Local and/or District Security Officer, Human Resources, the District Health Director, or other appropriate persons.

**Investigation**

- Once the Security Officer has knowledge of an alleged unauthorized use or disclosure of ePHI, he or she shall immediately begin a thorough investigation of the unauthorized release of ePHI. This may be performed through confidential interviews with staff members, inspection of release logs and/or access logs, and any other method(s) the Security Officer deems appropriate. It may also be necessary for the Security Officer to ask for assistance from another staff member in conducting the investigation; if so, he or she shall ask for assistance from a staff member he or she has concluded is not party to the alleged unauthorized release of ePHI.
- The investigation may find a systemic issue with the District's HIPAA Security Policies and Procedures, or the investigation may find a personnel issue, or both. The Security Officer, upon concluding the investigation, shall implement appropriate changes to policies and/or may make recommendations for personnel actions, and shall do so as expeditiously as possible.
- The Security Officer will ensure that a HIPAA Incident Report is completed to document the incident and that a copy is provided to the employee’s supervisor.
- The Security Officer may make recommendations for personnel actions based on the severity of the incident. The Security Officer may also recommend that the employee(s) no longer have access to PHI/ePHI, based on the severity of the incident or history of incidents.
- In all cases, the Security Officer shall document in writing the unauthorized use(s) or disclosure(s) of PHI/ePHI, the perpetrator(s), and what action(s), if any, were taken as a result of the violation(s).

**Sanctions**

After a thorough investigation by the Security Officer(s), the following sanctions may be applied.

- Accidental or inadvertent violation

  An unintentional violation of security that may be caused by carelessness, lack of knowledge, lack of training, or other human error.

  A) Retraining.

- Failure to follow established privacy and security policies and procedures

  A violation due to poor job performance or lack of performance improvement. Examples of this type of incident include release of ePHI without proper patient authorization; leaving detailed ePHI on an answering machine; failure to report privacy and security violations; improper disposal of ePHI; failure to properly sign off from or lock computer when leaving a work station; failure to properly safeguard password; failure to safeguard portable device from loss or theft; or transmission of ePHI using an unsecured method.

  A) Retraining

  B) Disciplinary Action

  C) Possible loss of access to ePHI

- Deliberate or purposeful violation without harmful intent

  An intentional violation due to curiosity or desire to gain information for personal use. Examples of this type of incident include accessing the information of high profile people or celebrities or accessing or using ePHI without a legitimate need to do so, such as checking the results of a coworker's pregnancy test.

  A) Disciplinary Action, up to and potentially including termination

  B) Loss of access to ePHI

- Willful and malicious violation with harmful intent

  An intentional violation causing patient or organizational harm. Examples of this type of incident include disclosing ePHI to an unauthorized individual or entity for illegal purposes (e.g., identity theft); posting ePHI to social media Web sites; or disclosing a celebrity's ePHI to the media.

  A) Immediate termination

  B) Notification to the appropriate authorities for potential prosecution

In general, the procedures for progressive disciplinary action (Policy #224) shall apply.

## D. Information System Activity Review Procedure

Records of information system activity, such as logs, access reports, and security incident tracking reports, will be regularly monitored and reviewed for and by each site according to the minimum procedures outlined below.

Logs, activity reports, or other mechanisms to document and manage system activity will be reviewed at intervals commensurate with the associated risk of the information system or the ePHI repositories contained on said information system. The interval of the system activity review must not exceed, but may be less than, quarterly for all systems.

Security incidents such as activity exceptions and unauthorized access attempts (such as Intruder Lockout) will be detected, logged, and reported immediately to the appropriate system management, security and privacy officers in accordance with the HIPAA Security Policies and Procedures.

# III. Assigned Security Responsibility Policy and Procedure

**Citation: Assigned Security Responsibility, 164.308(a)(2)**

**Policy:**

The District Information Technology Director will serve as the District HIPAA Security Officer, or may designate an alternate member of the District IT Department to serve as District HIPAA Security Officer. The Security Officer shall be responsible for the development and implementation of the information security policies and procedures required to ensure compliance with HIPAA security regulations.

Each County Board of Health Office Manager is designated as the Local HIPAA Security Officer. In the event that the site in question does not have an Office Manager, or the Office Manager is unable to meet the responsibilities of the position, the Nurse Manager will designate an alternate position to serve as the Local HIPAA Security Officer.

**Procedure**:

The District and Local Security Officers shall carry out the following minimum responsibilities:

- Ensure that the necessary and appropriate HIPAA related policies are implemented to safeguard the integrity, confidentiality, and availability of Electronic Protected Health Information (ePHI) within the covered entity and its business associates.
- Ensure that the necessary infrastructure of personnel, procedures and systems is in place to implement, monitor, audit and review compliance with all HIPAA related policies, and to report incidents and HIPAA security violations.
- Act as a spokesperson and single point of contact for the site in all issues related to HIPAA Security.

The Security Officer designation shall be recorded on the individual's pmf, e-performance document, personnel file, or similarly appropriate location.

The Local Security Officer may name one or more individuals as their backup, and shall record this designation in the individual's pmf, e-performance document, personnel file or similarly appropriate location.

# IV. Workforce Security and Information Access Management Policy

**Citation: Workforce Security, 164.308(a)(3); Information Access Management, 164.308(a)(4)**

**Policy:**

The HIPAA Security Officer must implement policies and procedures to ensure that employees only have such access to ePHI as is appropriate for their duties, and to prevent other employees from obtaining access to ePHI, including the following:

A. **Authorization and Supervision.** Implement procedures for the authorization and supervision of employees who work with ePHI, or in locations where it might be accessed;

B. **Workforce Clearance.** Implement procedures to determine that the access of an employee to ePHI is appropriate;

C. **Termination of Access.** Implement procedures for terminating access to ePHI when the employment of an employee ends.

The HIPAA Security Officer must implement policies and procedures for authorizing access to ePHI that are consistent with HIPAA requirements, including the following:

A. **Access Authorization**. Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, program, process or other means;

B. **Access Establishment and Modification**. Implement policies and procedures that, based upon the CBOH's access authorization policies, establish, document, review and modify a user's right of access to a workstation, program or process.

It is the policy of the District to permit access to ePHI to authorized end-users only, and only to the appropriate level of access required. This policy shall apply to District personnel as well as to vendors or other contractors of the County Boards of Health, if those vendors or other contractors have need to access ePHI.

It is the policy of the District to terminate access to ePHI as quickly as possible for all end-users who are terminated, resign, retire, leave, transfer, or otherwise no longer require access to ePHI based upon their duty(ies) and role(s).

# A/B. Authorization and Access Procedure

1. General:
    a. Access to files or systems containing ePHI is to be granted to authorized personnel only, and only through the use of individual User ID's, which **must** be password protected. No User ID's accessing ePHI are to be shared for any reason.
2. Account Access Protocol
    a. When HR hires, modifies or terminates an employee, the employee information is promptly entered into the *HR Employee Access Request Master.xlsx* Spread sheet and D2ITHelpdesk is notified. This employee information includes:
        i. A code for New, Modified, Terminated or Other Employee,

        "Other" includes volunteers, interns, practicum students, contract employees, and temporary employment agency employees
        ii. First, Middle and Last Name
        iii. Start Date
        iv. Employee ID or Birthdate ( Filled in on start date)
        v. Title
        vi. Supervisor
        vii. Home Base
    b. The D2ITHelpdesk will create tickets for the access creation, modification or termination based on the information listed above. The track-it ticket #'s will be logged into the *HR Employee Access Request Master.xlsx* Spread sheet.
        i. Temporary employees will be given a DPH email address. Interns, practicum students, and contract employees may be issued a DPH email address on a case-by-case basis.
        ii. Email accounts will be requested and noted so in the open ticket.
        iii. An email will be sent to HR and the supervisor listed for the employee with the user credentials at the close of the ticket.
        iv. Email of terminated employees will be disabled.
        v. Email of Modified Employees will have Name or Position/Location changed as per HR data.
        vi. Active Directory accounts will be built for all users with some exceptions (Ex: Hall Co EH Workers using Hall County Gov PC's on Hall Co Gov. Network).
        vii. Active directory special folders and group access will be requested separately by the user's supervisor.

viii. Active directory Modifications and Terminations will be completed as per HR data.

ix. VHN Access is requested as a track-it project with an open-ended date until HR adds the User ID to the *HR Employee Access Request Master.xlsx* Spread sheet and notifies the D2ITHelpdesk. This is not done until the "start date". There will be NO Access Granted to any employee without the Employee ID Number. Temp Employees are classified as *Other* and will be granted access with *Birthdate* for ID Number.

c. VHN Access Modification

i. Employees Changing Positions thru HR will be noted on the *HR Employee Access Request Master.xlsx Spread sheet* as a modified Employee and D2ITHelpdesk will receive notification from HR. Old Access will be removed and New Access will be created as needed.

ii. VHN Access changes needed without HR employee position changes will still be requested by the Supervisor.

d. VHN Termination will be logged as a project and addressed as per data in the *HR Employee Access Request Master.xlsx* Spread sheet.

i. Most Terminations are handled immediately.

ii. All Nurse's VHN Accounts are to be left active for 30 days, but the account password is changed to prevent unauthorized access and so noted and time stamped in the Track-It ticket.

iii. Nurses will be able to close out any orders left unfinished by the terminated Nurse by logging in with their own VHN credentials and completing the unfinished documentation adding the terminated Nurse's Initials and commenting the reason.

iv. D2ITHelpdesk will complete the VHN Termination process after 30days and then the Track-it Ticket can be closed.

3. Supervisors:

a. The employee's supervisor shall determine the employee's appropriate level of access to ePHI based upon the employee's role(s) and duty(ies).

b. Once access has been granted to the employee, this constitutes an authorization by the District for that employee to be given access to ePHI, subject to the limitations documented in Track-IT.

c. Supervisors will maintain an ePHI Systems Access Form for each employee. The form is to be maintained in that employee's local personnel folder, and will transfer with them if they transfer in-district. The employee's current supervisor will note and update all access granted to systems containing ePHI on the form on an on-going basis throughout the employee's tenure with District 2 Public Health.

d. Employee access levels to ePHI will be periodically reviewed by the supervisor to ensure that assignments are still appropriate, based upon current job roles and duties.

e. In the event an employee's systems access, user account, or level of access needs to be modified as a result of a change of assignment or a supervisor's review, a new request will be submitted to IT by the supervisor and tracked and verified by IT following the procedures outlined above.

4. Vendors, Contractors, or Non-Employees:

   a. The District or Local Security Officer may identify individuals or organizations (vendors) who may be authorized to access ePHI.

   b. When adding these individuals or organizations, the Security Officer must take reasonable measures to ensure they understand the confidential nature of ePHI, and that they agree not to disclose ePHI maintained by the County Boards of Health to any other individual or entity.

      i. Reasonable measures include having all vendors, contractors, and other appropriate non-employees sign a Business Associate Agreement. Other measures, such as signing a confidentiality agreement, may also be utilized.

      ii. In addition, the District or Local Security Officer may create procedures to verify the identity of non-employees prior to granting access to ePHI, such as the creation of a unique user ID and password, a requirement for the vendor to present photographic identification, the use of a sign-in sheet, or other procedures as appropriate.

   c. All volunteers, interns, practicum students, contract employees and temporary employment agency employees working under District 2 supervision will be treated as though they were regular employees in terms of HIPAA security policies, and the procedures outlined for access to ePHI will be followed.

## C. Termination Procedure

1. Employees:
    a. In the event that an employee has been terminated, or has resigned, retired, or transferred to another agency, the employee's supervisor must immediately notify the Human Resources/ Personnel Department, following standard District 2 procedures.
    b. Immediately upon the employee exiting employment, the supervisor must fax the ePHI Systems Access Form for that employee to the IT Department. IT will work with district and local staff as needed to ensure that all points of ePHI access noted on the form are terminated as soon as possible for that employee.
2. Vendors, Contractors, or Non-Employees:
    a. The District or Local Security Officer will monitor individuals or organizations (vendors) who were granted to access ePHI. When those vendors no longer need access to ePHI, or the District's or County Boards of Health's association with that vendor is terminated, the Security Officer will work with district and local staff to terminate the vendor's access to ePHI.

# V. Security Awareness and Training Policy

**Citation: Security and Awareness Training, 164.308(a)(5)**

**Policy:**

The District shall carry out a security awareness and training program for all members of its workforce, including management.

Implementation shall include initial awareness training as well as:

A. **Security Reminders.** Provide periodic security updates as needed;

B. **Protection from Malicious Software.** Implement procedures for guarding against, detecting, and reporting malicious software;

   Computer viruses pose a serious threat to the security and integrity of Health Department computer systems, applications and data. While the potential for virus attack on standalone computers is considerable, there is a significantly more dangerous potential for virus attack on our networked computers due to the speed and ease with which viruses can spread across networks. District 2 Public Health has a responsibility to protect its resources against the threat of virus infection. All possible points of virus entry – the Internet, email, personal thumb/data drives, personal computers, gateways, servers – need to be considered and appropriate actions must be taken to counter the risks.

C. **Log-in Monitoring.** Implement procedures for monitoring log-in attempts and reporting discrepancies;

D. **Password Management.** Implement procedures for creating, changing, and safeguarding passwords.

# A. Security Reminders Procedure

## New Employee Awareness Training

As part of the new employee orientation process, all new employees must have HIPAA training. New employees must also review the District's Privacy and Security Policies and Procedures. New employees must sign an acknowledgement that they have trained on the security policies and procedures. This documentation will be placed in the employee's personnel file.

## Current Employee Periodic Awareness Training Updates

All personnel must be notified, with appropriate explanation, of any changes or additions to the existing security policies and procedures

Personnel will be reminded to review the current security policies and procedures on an annual basis.

The Security Officer may deem it necessary to require a review of the security policies and procedures more often than annually, based on incidents.

## Periodic Security Reminders

Periodically, the Security Officer shall send notices to employees regarding security information such as virus alerts, policy reminders, lessons learned from previous incidents and other computer system security topics. These periodic reminders may be in the form of emails, hard copy memorandums, announcements, or any other medium the Security Officer deems appropriate. The reminders shall be issued as often as necessary, but should be regular enough to be effective, preferably monthly.

## B. Protection from Malicious Software Procedure

Approved anti-virus software must be installed on each server and computer in use, and must be kept up-to-date with respect to virus signature files used by the anti-virus software. The District installs Symantec Anti-Virus software on all workstations and servers.

Servers/systems will be maintained behind firewall protection.

Files/software/firmware creating changes to servers/systems by outside contractors involved with the District or County Boards of Health technology systems will be scanned for malware by District IT staff prior to transfer or installation, with the exception of M&M within the constraints specified in their contract.

Servers/systems are to automatically receive virus signature files from the anti-virus software vendor on a regular basis; no less than once per week.

1. The IT Department shall ensure that:
    a. Every workstation has appropriate anti-virus software installed and running.
    b. The anti-virus software preferences are set according to policy.
    c. The virus definition, or pattern, files are kept up to date.
2. The Local Security Officer shall monitor all local workstations for the items above, and ensure that the help desk is called immediately whenever there is any indication that the anti-virus software is not running or is not updating correctly. Indications may include an "out-of-date" error message.
3. The virus definition files are set to update automatically, however, failure can occasionally occur. IT staff shall randomly check the date of the virus definition files to ensure they are up to date, and manually update the files when necessary.

Each actual and suspected virus infection event must be reported to District IT for investigation and remediation. If users believe their computer may be infected with a virus they should contact IT immediately. Suspect emails are not to be forwarded to IT. If a computer is known to be infected by a virus, or shows symptoms that may indicate virus infection, the computer must not be used again until it has been cleared by IT. The IT Department will assist in identifying any widespread viruses. Users will not be blamed when reporting an incident and should be assured that they will receive assistance that is appropriate to the incident and their needs.

If a mission critical server is infected, IT staff will immediately scan, clean/disinfect, and update the latest virus signature files on the server. If repeated attempts to clean the server fail, then the last known good system backup will be restored.

A log of all actual and suspected virus infections must be maintained by the Security Officer on the Virus Report/Log Form.

# D. Password Management Procedure

Passwords are an important aspect of computer security. Employees are responsible for creating, maintaining, and changing their password(s) in order to keep the networks of District 2 Public Health and beyond from being compromised.

Strong Passwords must be used on all Systems, Accounts and Equipment utilized to access ePHI

Strong passwords are those that are difficult to guess or discover through trial and error. Recommended standards for creating strong passwords:

a. Be a minimum of eight (8) characters in length.
b. Contain at least two (2) numeric character (0,1,2,…9).
c. Contain at least four (4) alphanumeric characters, including a mix of uppercase and lowercase.
d. Contain at least two (2) special characters (!,@,#,$,%,^,&,[,]).
e. Be unique (never been used before).
f. Be changed every 30 days.

**Employee's Responsibilities: Passwords and User ID's**

1. All employees must maintain confidentiality of their passwords, and ensure the security of their passwords.
2. Employees shall change passwords frequently, and any time security has been compromised.
3. Employees shall be responsible for all computer transactions that are made with their User ID and password for each network facility they have access to.
4. Employees are responsible for notifying the Security Officer of any suspicious activity regarding the employee's User ID and/or password.

Intruder Lockout will be employed on all ePHI systems, such that the account is locked after multiple, failed login attempts.

# VI. Security Incident Policy

**Citation: Security Incident Procedures, 164.308(a)(6) and 164.400-164.414**

**Policy:**

The District will ensure that suspected and/or known security incidents are reported, investigated, and mitigated to the extent practicable. The Security Officer will also document all security incidents and their outcomes. Any employee who witnesses or has knowledge of a security incident or breach, must immediately report the incident to the site's Security Officer. Failure to report knowledge of a security incident will result in disciplinary action. Any employee who knowingly breaches security will be subject to disciplinary action according to the Security Sanctions Policy.

A Security Incident is an actual, suspected, or attempted loss or disclosure of individually identifiable personal health information within the custody or control of a CBOH or DPH employee. A Security Incident can take place in many different ways: the loss of a disk or laptop computer containing ePHI, a malfunction or unauthorized attempt to enter into an information system on which ePHI is stored, disclosure of ePHI by email or telephone to the wrong person, an unauthorized modification or destruction of data, leaving papers with ePHI in plain sight in a common area, etc.

A Security Incident shall be declared to be a Breach if protected health information was acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

The Security Incident Response Team consists of the local and District HIPAA Privacy Officer and HIPAA Security Officer. If the Security Incident involves ePHI within the custody of a DPH employee, then the DPH Privacy Officer and DPH Information Security Officer will be on the Response Team.

# A. Security Incident Response and Reporting Procedure

Any event that might possibly be a Security Incident shall be reported immediately to the HIPAA Privacy Officer or the HIPAA Security Officer. The Security Incident Response Team shall immediately investigate the event, including personal interviews of any person who might have knowledge of the facts.

**Identification:**

An employee who witnesses, discovers, or otherwise gains knowledge of a security incident must immediately complete a HIPAA Incident Report, found in the Forms section.

The completed HIPAA Incident Report must be submitted to the local Security Officer, unless the Local Security Officer is, or may be, a party to the incident.

1. The completed incident report must also be copied to others as appropriate and identified on the HIPAA Incident Report form.
2. If the local Security Officer is a party to the incident, or is the employee reporting the incident, the completed incident report form must be submitted to the District Security Officer.

**Investigation:**

Upon receipt of a HIPAA Incident Report, the Security Officer (Local or District) will conduct a thorough investigation of the incident reported. The Security Officer may conduct the investigation through confidential interviews, the inspection of related security logs, assistance from Information Technology staff, and/or any other reasonable method(s) the Security Officer deems necessary.

At the onset of the investigation, the Security Officer will notify the manager of the work unit where the incident occurred, that an investigation is underway.

1. The Security Officer might not divulge details of the investigation to the work unit manger, due to confidentiality and to reduce potential problems with the investigation.
2. Upon completion of the investigation, the manager of the work unit will receive complete details about the investigation.

**Incident Documentation**:

The Security Officer will document all information gathered during the investigation, including summaries of interviews conducted, reports received, steps or actions taken during the investigation, outcome(s) of the investigation, and any recommendations for policy or procedure changes.

Upon completion of an investigation, the Security Officer will retain a permanent record of the incident, the investigation, and the outcome(s). The Security Officer will also forward a copy of the complete documentation to the manager of the work unit.

**Determination of a Breach:**

At the conclusion of the investigation, the Response Team shall decide whether there has been a Breach. The incident shall not be considered a Breach in the following circumstances:

1. The acquisition, access, or use of the ePHI was by an employee or business associate in good faith and within the scope of their authority, and there was no further use or disclosure in violation of HIPAA;
2. An inadvertent disclosure of ePHI was made by an employee or business associate authorized to access ePHI to another employee or business associate authorized to access ePHI, and there was no further use or disclosure in violation of HIPAA;
3. The ePHI was disclosed to an unauthorized recipient, but there is a good faith belief that the recipient would not reasonably have been able to retain the ePHI; or
4. A risk assessment of the following factors by the Security Incident Response Team shows that there is a low probability that the ePHI was compromised:
    a. The nature and extent of the ePHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the ePHI or to whom the disclosure was made;
    c. Whether the ePHI was actually acquired or viewed; and
    d. The extent to which the risk to the ePHI has been mitigated.

**Response:**

Regardless of whether or not the Security Incident is deemed to be a Breach, the Security Incident Response Team shall develop and implement a plan to accomplish the following:

1. Ensure that the conditions that made the incident possible are corrected so as to prevent future incidents. This may include recommendations for further training of employees, or changes to office technology, training, policy, or procedures.
2. Identify individuals whose ePHI was or may have been disclosed, and the persons or entities to whom ePHI was or may have been disclosed.
3. Mitigate any possible harm that may have resulted from the incident.
4. Recommendations to the Human Resources Department or District Health Director for disciplinary actions against persons responsible for the incident, if warranted.

**Notifications**:

In the case of a breach of protected health information that is discovered, the District Security 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.

**Timeliness:**

All notifications shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.

1. A breach shall be treated as discovered as of the first day on which the breach is known internally or by a business associate, or should reasonably have been known to have occurred.
2. If a law enforcement official determines that a notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed, with appropriate documentation as specified in 164.412.

**Notice Format:**

Notice to individuals shall be provided promptly and in the following form:

1. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at their last known address, or, if the individual agrees to electronic notice and such notice has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
2. If there is insufficient or out-of-date contact information, and up-to-date contact information can not be obtained, a substitute form of notice reasonably calculated to reach the individual shall be provided.
    a. In the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, notice may be made by
        i. a conspicuous posting for a period of 90 days on the home page of the District 2 website, or
        ii. a conspicuous notice in major print or broadcast media, serving the geographic areas where the affected individuals likely reside.
    b. Such a notice in the media or on the web will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

3. In any case requiring urgency due to the possible imminent misuse of unsecured protected health information, information may also be provided to individuals by telephone or other means, as appropriate.
4. For breaches where the unsecured protected health information of more than 500 residents is reasonably believed to have been accessed, acquired, or disclosed, notice shall be provided to prominent media outlets serving the area.

**Notice Content:**

Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following in plain language:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, or chart number).
3. The steps individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, a web site, or a postal address.

**Breach and Notification Documentation:**

At the conclusion of every investigation, the HIPAA Security Officer shall ensure that a file is prepared and maintained to document the facts of the incident, the basis for the determination that there was or was not a Breach, the response, and proof that all notices required by law were made.

Complete documentation shall include a log of all notifications and details, and copies of all letters or media notices. Documentation shall demonstrate that all notifications were made as required, and shall include evidence demonstrating the necessity of any delay.

Notice shall be provided to the State Agency Security Officer and the HHS Secretary as required regarding any unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals, such notice will be provided immediately. If the breach was with respect to less than 500 individuals, a log will be maintained and submitted annually, no later than February 28 of the following calendar year.

# VII. Contingency Plan Policy

**Citation: Contingency Plan, 164.308(a)(7)**

**Policy:**

Contingency Plan. The HIPAA Security Officer must establish and implement as necessary, policies and procedures for responding to an emergency or other occurrence that damages a system containing ePHI, including the following:

A. Data Backup Plan. Establish and implement procedures for a data back-up plan, to create and maintain retrievable exact copies of ePHI;

B. Disaster Recovery Plan. Establish and implement procedures as needed, for a disaster recovery plan to restore any loss of data;

C. Emergency Mode Operation Plan. Establish and implement procedures as needed, for an emergency mode operation plan, to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

D. Testing and Revision. Implement procedures for periodic testing and revision of contingency plans.

E. Application and Data Criticality Analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components.

District IT shall install operating system patches and fixes as soon as they have been approved. Employees will not intentionally disable updates on workstations.

All servers will be maintained on Uninterruptible Power Supplies (UPS) to allow them to be shut down in a proper manner in the event of a power failure, or on generator, where available.

Each critical function will have alternative operating procedures to ensure continued delivery of services in the event of an interruption caused by disasters, for critical, essential program functions provided by all facilities/systems.

**Data Backup Plan**: District IT and local CBOH staff shall maintain a daily data backup which meets or exceeds the Data Backup Procedure. Designated staff shall be responsible for backup and media storage.

**Disaster Recovery Plan**: In case of disaster, District IT staff will initiate necessary procedures to restore the systems to functional use with the least amount of down-time possible. The most current, valid system backup is to be restored on the server(s) and data validated prior to the server(s) being put back into production mode. As an option, if another like server is available, the latest system backup can be restored to that server, as a backup server, for use until the production server can be returned to service.

**Emergency Mode Operation Plan**: In the event that a facility is unusable for a period of days, operations should relocate to a predetermined site and setup minimal system services to provide essential program functions.

**Testing and Revision Plan**: All contingency plans are to be assessed, tested, and revised on a regular and as-needed basis.

# A. Data Backup Procedure

A full backup of all network servers located at the District Office must be performed at the close of every business day.

1. District Office Servers are backed up to disk via VEEAM Backup and Replication software on server HALL021.
2. All District Office Servers are replicated to the SAN storage unit located in the main server room at the Hall County Health Department.
3. District Office Servers are backed up daily to tape by Backup Exec.

All ePHI located on servers at the individual health departments will be backed up to a secure partition on the main server and a second copy will be replicated to an in-house storage server.

## B. Disaster Recovery Procedure

In the event that an occurrence, whether natural, intentional, or accidental occurs which affects system operations in an information system, the following procedures will be followed:

1. Work with local and district management as needed to determine if law enforcement authorities need to be notified. Any acts of sabotage **must** be reported to law enforcement.
2. Notify management that staff should begin using contingent procedures as identified in Attachment C, Emergency Mode Operation.
3. File a HIPAA Incident Report.
4. If hardware replacement is required, prepare purchase orders, acquire appropriate approvals, and place order with vendors.
5. Secure most recent copy of system backup and system software.
6. If vendor assistance is required:
    a. Contact vendor and make necessary arrangements for vendor support.
    b. Accompany vendor on-site and escort within the facility in compliance with the Facility Access Controls Policy.
7. When systems have been restored, notify management that staff may login and verify accuracy of data.
8. Once data has been verified as complete and accurate, staff may begin backloading data for services provided while system was unavailable, and data for services currently being provided.
9. Document incident causes, mitigation, and all actions taken.
10. Make appropriate recommendations to management for implementation of actions to prevent or reduce the odds for recurrence of the same or similar types of incidents.

Procedures 4 - 7, 9, and 10 are to be performed in collaboration with staff consisting of the Local Security Officer, The District Security Officer, and District OIT Staff.

## C. Emergency Mode Operation Procedure

Computer services and access will be restored based on the priority needs of the situation.

Generator backup will be utilized to power servers in-place wherever possible.

In the event that a health department facility is unusable, central server access will be provided by:

1. relocating staff to another health department location; and/or
2. relocating staff to an alternate site where internet access is available
    a. wire connection is preferable
    b. wireless/tethering access is acceptable

In the event that the district office facility is unusable, central server access will be provided by relocating the main servers to CWSN or another suitable site, not to include the Hall County Health Dept., which shares the AC power grid with the district office.

Servers containing ePHI are to be placed in secure areas of the alternate facility, so that access to them can be limited and monitored.

In the event that a system server is damaged, or client services must be delivered prior to system servers being available through an alternate route or site, staff are to use manual forms and enter the data into the electronic system when server access is again available.

1. Immunization Histories can be accessed on-line using the Immunization Registry.
2. Medicaid eligibility can be verified on-line, or by phone.
3. Required reporting of communicable diseases is reportable through SENDSS, on-line.
4. Hardcopy forms and manual vouchers can be used for WIC clients.
5. Manual processes for all critical services must be maintained at the local level.

# VIII. Evaluation Policy

**Citation: Evaluation, 164.308(a)(8)**

**Policy:**

The HIPAA Security Officer must perform a periodic technical evaluation to ensure that CBOH security policies and procedures meet the requirements of this Policy.

The Security Officer shall periodically review and evaluate the District's security risks and vulnerabilities, and implement appropriate and reasonable protocols to address any risks discovered in the evaluation process using the Evaluation Checklist. See the Risk Analysis and Assessment Policy.

# IX. Business Associate Policy and Procedure

**Citation: Business Associate Contract and Other Arrangements, 164.308(b)**

**Policy:**

The District may permit a business associate to create, receive, maintain, or transmit Electronic Protected Health Information (ePHI) on its behalf **only** if the District obtains satisfactory assurances that the business associate will appropriately safeguard the information. The District is not required to obtain such satisfactory assurances from a business associate that is a subcontractor of a business associate This standard does not apply with respect to the transmission of ePHI to a health care provider concerning the treatment of a patient, or to another agency providing the services when the covered entity is a health plan that is a government program providing public benefits as specified in Section 164.502(e)(1)(ii)(C).

The most current DPH Business Associate Agreement is the approved District Business Associate Agreement.

**Procedures:**

Prior to granting access to ePHI, the Security Officer shall perform the following:

1. Identify current Business Associates contracted by the District who have access to ePHI;
2. Ensure that all contractors or vendors sign the approved Business Associate agreement, if the contractor or vendor will need access to ePHI, or if ePHI will be shared between the County Boards of Health and the contractor/vendor.

The approved Business Associate Agreement may be placed on District 2 or County Boards of Health letterhead, or may be utilized without letterhead.

# X. Facility Access Controls Policy

**Citation: Facility Access Controls, 164.310(a)**

**Policy:**

The HIPAA Security Officer must implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, but ensure that authorized access is allowed, including the following:

A. Contingency Operations: Establish and implement procedures as necessary that allow facility access to support the restoration of lost data under the disaster recovery and emergency mode operations plans in the event of an emergency;

B. Facility Security Plan: Implement policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering, and theft;

C. Access Control and Validation: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and to control access to software programs for testing and revision;

D. Maintenance Records: Implement policies and procedures to document repairs and modifications to the physical components of a facility related to security (e.g., walls, hardware, doors, and locks).It is critical that electronic protected health information (ePHI) maintained on the County Board of Health's computer system(s) be kept secure and confidential. Since ePHI is stored on the application file server, it is equally important that proper measures are taken to secure the application file server, and other components of the electronic information system(s).

In the event of a need to recover or restore data, the facility and required backup media must be available to authorized staff or business partners. Also, emergency mode operations may require the moving of equipment that contains ePHI, and this must be performed in a secure manner so that ePHI is protected from unauthorized access during the move and while at the temporary or contingent location.

## A. Contingency Operations Procedure

Authorized employees will have in their possession, items necessary to enter the primary and backup facilities during non-business hours. Necessary items may include keys, security codes, ID Badges, proxy cards, etc.)

## B. Facility Security Plan Procedure

File servers will be located in secure locations within the facility. Secure location means that fileservers will be housed in a low traffic area, and one or more of the following methods for physically protecting the file server will be utilized:

1. Secure the server to a permanent structure using a cable and lock.
2. Place server in lockable server cabinet.
3. Place server in a room that will be locked when authorized staff are not present.

In addition to one of the above methods, the removal of the server monitor and/or keyboard should also be considered when the server is only secured by cable and lock and either attachment is not required for use.

It is further recommended that:

1. Every building have an alarm system, and that codes be changed at least once every two years.
2. Outside door locks to every building be rekeyed at least once every five years.
3. All server room doors be protected by programmable key access, with access codes changed at least once every two years.
4. Electronic key access be installed and utilized wherever possible and practical.

## C. Access Control and Validation Procedure

Regular access to fileservers will be granted **only** to those employees who provide support and/or administration to the servers.

Staff will escort any non-authorized individual unless other arrangements are made with the Local Security Officer or other designated person. Local HIPAA Officers are responsible for monitoring access to systems by outside contractors involved with the District's data systems. This may include maintaining an access log.

All non-employees must sign Business Associate agreements or the HIPAA training acknowledgement, whichever is appropriate, before accessing files or equipment containing ePHI.

Upon employee termination, all identification badges, facility keys, entry key cards (proxy cards), PDA's, flash/thumb drives, laptops, cell phones, radios, pagers, etc. will be collected on the employee's last day of employment. This will be documented and maintained by the Security Officer, Supervisor, or Human Resources Representative, as appropriate.

## D. Maintenance Records Procedure

The Local Security Officer or other designated person must maintain a log of all structural, and/or system changes that are made to the facility that will affect facility access or security. Such changes would include, but are not limited to, changing door locks, changing alarm system/security system codes, addition of doors or windows, addition of walls or partitions, removal of walls or partitions, installation of a new security/alarm system, etc.

# XI. Workstation Use Policy

**Citation: Workstation Use, 164.310(b)**

**Policy:**

The HIPAA Security Officer must implement policies and procedures that specify the proper functions to be performed, the way in which these functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI.

All computers and computer related equipment are property of the County Boards of Health, District and/or the State.

Computers and networks are provided for employees who are affiliated with the District for the purpose of conducting Health Department business in support of the vision, mission and goals of Public Health. This includes, but is not limited to, computers, network access, printers, mobile telephones/radios, smartphones, tablets, etc. This same technology increases the risks of actions, deliberate or not, that are harmful in various ways, including: 1) interference with the rights of others, 2) violation of the law, 3) interference with the mission of the District, or 4) endangering the integrity of the District's information systems or network.

All users have a responsibility to use District computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer resources, the Internet, or Protected Health Information may result in disciplinary action, including possible termination, and civil and/or criminal liability.

The District IT Department is responsible for the day-to-day operations and administration of all networks and peripherals. District IT has the right to utilize software that makes it possible to identify, track, and block access to Internet sites deemed inappropriate for the workplace. Internet activity on work resources (computers, laptops, etc.) is logged.

# A. Workstation Use Procedures

**Employee Responsibilities:**

1. Know and abide by all District policies related to Information Technology, including security and confidentiality of business records.
2. Operate the equipment in a manner complying with all applicable District policies.

**Intended Use of Equipment:**

1. The use of equipment in political campaigns is forbidden.
2. Equipment may not be used in connection with compensated outside work or for the benefit of organizations not related to the District. State law restricts the use of equipment purchased using tax dollars for personal gain or benefit.
3. Computer users must obey all laws against private use of state property, divulging confidential patient records, copyright infringement, fraud, slander, libel, harassment, and obscenity.
4. Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone lines.
5. Pyramid schemes and chain letters that ask for money or anything else of value are illegal.
6. Employees shall power off their computers at the end of the workday. A computer is considered off when the lights on the unit are off.
7. Employees shall logout when leaving their workstations.
8. Employees are prohibited from installing software regardless of the source (even if sent by the state office) without prior approval from the IT Director. Approval can be acquired via email or through the IT Help Desk.
9. Employees are prohibited from allowing anyone that is not an authorized end user from using any work computer equipment or peripherals.
10. Employees are responsible for maintaining backups of critical documents on DVDs or other storage media.
11. Employees may not add hardware or reconfigure any portion of the system without written approval from the IT Director.
12. Employees may store only limited personal files, of any type, on county / state owned computers. Personal files include, but not limited to, personal documents, photographs, videos, music files, etc. All personal files must be virus scanned.

13. Employees are responsible for reporting suspected criminal or administrative misconduct regarding misuse of District technical resources to their Supervisor, Human Resource Representative, or the Security Officer.
14. Employees are prohibited from making personal long distance and international phone calls from office phones. The office manager or other designated person will monitor phone bills for inappropriate usage. Repeat offenses may result in disciplinary action. Employees making unauthorized personal long distance calls will be required to pay the cost of the call, or the cost of the call minutes at the current per minute rate, depending on the type of phone system and bill. Failure to pay for unauthorized personal long distance charges may result in that amount being deducted from other payments or reimbursements to be made to the employee.

**Internet Usage:**

1. Internet access is for District business and may not be used for purposes that would violate any District policy, or Federal, State, or Local Law.
2. Personnel may use the Internet, including social media, for occasional personal use, so long as the time spent is minimal and does not interfere with the work activities of the person or the work unit as determined by the person's supervisor, and to the extent that it does not violate any District policy, or Federal, State, or Local Law.
3. Personnel may not illegally copy material protected under copyright law or make that material available to others for copying. Users may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of their supervisor or the IT Department.
4. Personnel may not use the District's Internet connection to download entertainment software, screen savers, etc.
5. Personnel may not access, post, send, upload, or store, material that is sexually suggestive, obscene, pornographic, fraudulent, offensive, harassing, intimidating, defamatory, abusive, discriminatory, threatening, or otherwise inappropriate, unless a legitimate work-related reason exists to do so. Personnel receiving such materials should notify their supervisor immediately.
6. The Internet is commonly used by the online criminal community to deliver malware, and to carry out schemes designed to damage property or steal information. All personnel are expected to use good judgment in deciding which sites to access and/or links to follow while at work, so as to protect the District's assets.
7. Personnel are not to click on Web pop-ups that promise to clean your computer or install needed patches.
8. Participating in chat rooms without a legitimate work-related reason to do so, or utilizing unapproved instant messaging is prohibited.

9. Inappropriate use, including excessive personal use, of the Internet may result in loss of Internet access privileges and/or other disciplinary action, up to and including termination.

Excessive use of the Internet is prohibited**.** Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Each office has a predetermined size/speed of circuit known as bandwidth to run their processes. Compare the bandwidth to a garden hose. When the hose is filled with water nothing else can get through. When the circuit is filled with data activity nothing else can get through, or it slows the data flow to almost nothing. It is important that employees utilize the existing circuit in the best interest of our business needs.

Listening to music from the Internet is strictly prohibited. Viewing Streaming video or audio files on the Internet without a legitimate business reason to do so is strictly prohibited.

Excessive use of the Internet may result in loss of Internet access privileges and/or other disciplinary action, up to and including termination.

**Electronic Mail (email):**

1. While email is intended for official purposes, incidental and occasional personal use of the state email system is authorized. Users must exercise common sense and good judgment in the use of this resource.
2. Email should adhere to the same standards of conduct as any other form of mail. Respect others by avoiding distasteful, inflammatory, harassing or otherwise unacceptable comments.
3. Personnel are responsible for all activity involving their work email account. Email accounts must be kept secure. Under the Georgia Open Records Act, information which is stored on work computer systems, including email, are open to inspection by members of the public.
4. The Electronic Communications Privacy Act (18 USC 2701-2709) and other wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.
5. All Protected Health Information (ePHI) sent by email must be encrypted. *Consider de-identifying all ePHI before sending email.*

6. Never open email attachments from outsiders, or use media storage devices from non public health sources.
7. Do not open email from unknown sources. Right click on the envelope and click on "Delete."

**ePHI on Phones or other Mobile Devices:**

ePHI is not to be sent via text message or instant message, except under the following conditions:

1. Any staff member texting ePHI must be on record with the District Security Officer.
2. The patient or client must have a current, signed Consent to Text ePHI on file, giving their permission to communicate ePHI with them in this manner.
3. ePHI sent via text must be limited to the least amount necessary.
    a. Use text messages only for simple, quick check-ins with little or no ePHI included.
    b. Ask to discuss situations involving ePHI via phone. (For example, text: Can I call you to talk about it? Are you free to talk now? etc., then follow up with a call.)
4. If ePHI must be sent by text, first send a message stating: "I am about to send personal health information. Is that okay?" Do not send the ePHI until or unless the patient responds affirmatively.
5. Do not take any photo or image of a patient or client without first obtaining their approval. Take photos only in locations that provide the patient or client with adequate privacy.
6. Do not send photos of patients, clients, or body parts by text message.
    a. Photos taken with a cell phone must be immediately transferred to a work laptop or computer via a cable connection and sent by encrypted e-mail.
        i. All copies of photos on cell phones must be deleted as soon as they are transferred.
    b. Photos taken using a tablet or other mobile device must be treated as though they were taken using a cell phone.
    c. All unencrypted copies of photos on laptops or computers must be deleted as soon as they are sent or encrypted.
7. Cell phones must not be visible to others. Cell phones and mobile devices must be protected from viewing just as are computers and laptops.
8. All text messages containing ePHI must be documented on a contact log or in the patient's record. The IT Department may supply a text logging app, should a suitable one be identified.

9. All text messages containing ePHI must be deleted within 24 hours of the message time and date.
10. Instant messaging through Facebook or other means may only be used to make contact with a patient or client. No ePHI is to be transmitted via these insecure modes of messaging.
11. No personal phone or mobile device may be used to text, transmit, or store ePHI. Only District issued phones or mobile devices may be used for texting ePHI.

# XII. Workstation Security Policy

**Citation: Workstation Use, 164.310(c)**

**Policy:**

The HIPAA Security Officer must implement physical safeguards for all workstations that access ePHI, to restrict access by unauthorized users.

This policy is intended to protect the data on our network; protect the State's data system from breaches through our system; ensure that we meet HIPAA requirements; and ensure that our network operates efficiently for performing the business of the County Boards of Health. All terms such as computer, network, PC, system, or workstation, in this or any other HIPAA Security Policy or Procedure, must be interpreted to be inclusive of all computer equipment and any other device that may be used to create, store, receive, transmit, and/or process information.

The data system is the responsibility of the appointing authority for the County Boards of Health personnel, i.e. the District Health Director. This responsibility is delegated to the District's Information Technology Director (IT Director) and/or HIPAA Security Officer for the day-to-day administration of all computer equipment, software, access, and security controls. The IT Director, Supervisors, and Employees are responsible for implementing and following the intent of this policy.

# A. Workstation Security Procedure

**Employee's Responsibilities: General**

All employees must comply with the following policies and procedures:

1. Know and abide by all policies and procedures dealing with security and confidentiality of public health records.
2. Anyone utilizing a computer/workstation with access to ePHI must lock the computer or log off the ePHI system whenever leaving the computer/workstation, such that ePHI is inaccessible.
3. All access devices (modems, wireless/cell phone hotspots, wireless network cards, etc.) must be approved and configured by District IT prior to installation and use.
4. Employees are responsible for ensuring that all ePHI stored on hard drives (computers, laptops, etc.) or external drives is encrypted.
    a. Storing/maintaining files that contain ePHI on the hard drive of the local workstation is not recommended.
    b. Files containing ePHI should be stored on the individual's network drive, if available. This drive will be designated as the drive with your User ID in the drive name. This drive is secure and is backed up daily.
    c. Files containing ePHI are not to be stored in a "shared" network directory, or folder, unless all other employees who have access to the shared directory or folder are authorized to have access to the ePHI contained in the file(s).
    d. It is sometimes necessary to temporarily store files containing ePHI on the hard drive of the local workstation, so that the file can be transmitted or transferred. In such cases, the file **must** be deleted from the hard drive of the local workstation after it has been transmitted. It is the responsibility of the employee who transmitted/ transferred the file to delete the file when they have completed their task.
    e. Storing/maintaining files that contain ePHI on a flash/thumb drive is not recommended. ePHI on a flash/thumb drive must be encrypted, and may only be stored on a drive that is password protected.
    f. Contact District IT for assistance with encryption, identifying local and network drives, and for questions regarding access to an individual or shared network directory/folder.

**Mobile Devices:**

1. Mobile devices include but are not limited to cell phones, smart phones, hot spot devices, tablets, and laptops.
2. All mobile devices issued by the District will have some form of tracking and/or security software installed by IT. Different devices may have unique tracking and/or security software and configurations. (See the listing of the current District IT required and supported security software in the appendix.)
3. Each device issued by the District will be assigned to a user and checked out for use. Each device will be logged. Users must sign the District's Acceptable Use and Acknowledgement form. The user is responsible for any and all hardware and/or software received, as well as for securing any ePHI or other sensitive data stored on or passing through the mobile device.
4. All District issued laptops will be issued with a standard configuration, matched to the user's department or position. Additional hardware, software, or configurations must be approved by the IT Department, and the user's supervisor may be requested to provide approval as well. Laptops must have a BIOS password. Laptops must have the District security client, current malware protection, and remote access for the IT Dept. installed.
5. All District issued smart phones and tablets will be issued with a standard configuration. Smart phones and tablets must have the District required security software, which allows App monitoring, location tracking and remote wiping of the smart phone or tablet in case of loss or theft. Additional security related features may be added later with OS and security software updates. These updates may include but are not limited to phone password requirements, application controls, and restrictions. All smart phones and tablets must have at minimum some form of access control at the main screen that locks after specified amount of time. The access control may consist of 4 digits or more PIN, screen pattern, and/or biometric.
6. All District issued hotspot devices will be configured by the IT Department. Configuration will be secured by a password. SSID with key will be configured and must be used while accessing the internet via the hotspot.
7. Third party software and apps must be approved by the user's supervisor and by the IT Department prior to installation on a District issued mobile device. Installation by the IT Department may be required depending on the device or software configuration.
8. VPN access is restricted to District issued devices and must be approved by the user's supervisor and the IT Department.
9. Clinical data system(s) access is restricted to District issued devices.
10. No personal phone or mobile device may be used to text, transmit, or store ePHI. Only District issued phones or mobile devices may be used for texting ePHI.

# XIII. Device and Media Controls Policy

**Citation: Device and Media Controls, 164.310(d)**

**Policy:**

It is imperative that we protect the confidentiality, integrity, and availability of our client's ePHI. In order to accomplish this, controls over hardware and media, which store ePHI, must be in place.

The HIPAA Security Officer must implement policies and procedures for the receipt and removal of hardware and electronic media containing ePHI into and out of a facility, as well as the movement of these items within a facility, including the following:

A. Disposal. Implement policies and procedures to address the final disposition of ePHI, and the hardware or electronic media that stores it;

B. Re-Use of Media. Implement procedures for removal of ePHI from electronic media prior to the media being made available for re-use.

C. Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible for such movements;

D. Data Back-up and Storage. Create a retrievable, exact copy of ePHI, when needed, before moving equipment.

## A. Disposal Procedure

USB or other removable disks that will no longer be used must be returned to IT to be physically destroyed.

Floppy or other removable magnetic disks must be destroyed by removing the magnetic media from its casing and cutting the magnetic media.

Magnetic tape must be destroyed by removing the media from the tape hub and cutting the media.

Hard disk drives must be removed from computers and physically destroyed.

Compact disks, dvds, and other optical media must be destroyed by breaking the disk.

## B. Media Reuse Procedure

Mobile, or portable media, such as cd's, flash (thumb) drives, etc. that is to be re-used within the organization must be formatted before it can be re-used.

Hard drives in computers that are to be reused within the organization must be processed by appropriately reformatting or reimaging prior to transfer for re-use.

## C. Accountability Procedure

Personnel receiving District cell phones, smart phones, tablets, or other mobile devices, or receiving reimbursement for the use of personal devices must sign the District's Acceptable Use and Acknowledgement form. The Security Officer shall maintain this document for all users.

Devices that are reused and/or transferred within the organization must be turned in to IT and logged to indicate the source and destination of the transfer, the date of the transfer, and the person who actually transferred the device.

## D. Data Back-up and Storage Procedure

All servers containing ePHI must be backed up daily. See the backup schedule found in the Data Backup Procedure under the Contingency Plan Policy.

All files containing ePHI, or data critical to the function of the work unit, must be backed up daily.

# XIV. Access Control Policy and Procedure

**Citation: Audit Controls, 164.312(a)**

**Policy:**

The HIPAA Security Officer must implement technical policies and procedures for information systems that maintain ePHI, which allow access only by those persons or software programs that have access rights, including the following:

A. Unique User ID. Assign a unique name or number for tracking and identifying user identity;

B. Emergency Access Procedure. Establish and implement procedures as needed to obtain necessary ePHI during an emergency.

C. Automatic Log-off. Implement procedures to terminate an electronic session after a certain period of inactivity;

D. Encryption. Implement a mechanism to encrypt and decrypt ePHI.

**Procedure:**

Unique User ID.

The IT Department will assign a unique user ID and password for VHN.

The IT Department will assign an Active Directory username and password for employees needing to store ePHI on a server.

Emergency Access.

The IT Department staff will have access to all staff and shared files on server drives in order to provide access in an emergency.

IT staff will work with M&M to ensure access to VHN data in emergency situations not covered elsewhere in this policy and procedures manual.

Automatic Log-off.

VHN is set to auto-log off users after 30 minutes of inactivity.

Encryption.

VHN is not encrypted while “at rest” on the server, but is encrypted during transport between the server and the workstations.

For staff and shared files on server drives, data partitions are set up which encrypt automatically.

For files on local computers or laptops, 7-Zip is to be used for encryption until built-in encryption becomes available.

# XV. Audit Controls Policy and Procedure

**Citation: Audit Controls, 164.312(b)**

**Policy:**

The HIPAA Security Officer must implement hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

It is critical that patient and client ePHI be maintained in a secure manner. In order to verify this, system access audits will be performed a minimum of once each fiscal year. The audit will include, but is not limited to, verifying that system access is allowed to current, authorized staff and business associates only. System access logs that are available in the operating system should be turned on and reviewed on a regular basis. The Security Officer, designated staff, or appropriate vendor will investigate intrusion attempts or other unusual activity to determine the level of access and develop a method of prevention.

**Procedure:**

A system access audit will be performed a minimum of once each year to verify that access is limited to current staff and authorized personnel only. Current users will be verified against a list of current active employees from Personnel.

An activity audit will be performed a minimum of once per year to ensure that ePHI has not been accessed, altered, or destroyed in an unauthorized manner.

If the capability exists, a log of attempted unauthorized system intrusions will be maintained. This log will cover the period of one year.

In the event of an intrusion attempt, or other unusual activity, the Security Officer or other designated staff will:

1. Determine the access method
2. Determine the level of system access
3. Determine User ID and password used
4. Determine which applications, data, or records were accessed, if any
5. Report findings to the appropriate persons
6. Define, recommend, and implement solutions to deter future successful system intrusions that use the same method of access

# XVI. Integrity Policy and Procedure

**Citation: Audit Controls, 164.312(c)**

**Policy:**

The HIPAA Security Officer must implement policies and procedures to protect ePHI from improper alteration or destruction, and to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

**Procedure:**

1. Identify all District programs that maintain ePHI.
2. Conduct a risk assessment.
3. Assist Program Directors' in developing a program specific policy.
4. Program policies will be reviewed yearly with the HIPAA Security Officer.

# XVII. Person or Entity Authentication Policy and Procedure

**Citation: Audit Controls, 164.312(d)**

**Policy:**

The HIPAA Security Officer must implement procedures to verify that a person or entity seeking to access ePHI is the one claimed.

**Procedure:**

1. For District employees:
    a. Employees must state in writing what information is needed and for what period of time.
    b. The employee's supervisor must provide IT with written approval.
2. Business associates must maintain a valid BA with the District that is reviewed at least yearly. Business associates must comply with all state and federal laws.

# XVIII. Transmission Security Policy and Procedure

**Citation: Audit Controls, 164.312(e)**

**Policy:**

The HIPAA Security Officer must implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network, including the following:

A. Integrity Controls. Implement security measures to ensure that electronically transmitted ePHI is not improperly modified during transmission;

B. Encryption. Implement a mechanism to encrypt ePHI whenever deemed appropriate.

**Procedure:**

A. Integrity Controls

All transmission of ePHI within DPH will be sent via the state's encrypted network. This includes, but is not limited to, email and any attachments; connections to the state lab, CareWare, WIC sites, etc.

B. Encryption

All transmission of ePHI outside DPH must be encrypted using 7-Zip. *(Employees may use their OneDrive account to temporarily allow access to Business Associates.)*

# XIX. Documentation Policy

**Citation: Documentation, 164.316(b)**

**Policy:**

The HIPAA Security Officer shall maintain the policies and procedures implemented to comply with the Security Rule in written format. The documentation must be reviewed periodically and updated as needed due to environmental or operational changes affecting the security of ePHI. Procedures followed in the event of a security incident and the outcome must also be documented. The documentation must be kept for six years from the date of its creation or the date when it was last in effect, whichever is later.

Each Security Officer (District and Local) shall maintain a written copy of the HIPAA Security policies and procedures. An electronic copy will suffice as written form. The HIPAA Security manual is not to be posted on the Web/Internet.

Each Security Officer (District and Local) shall maintain complete written records of any assessment, incident, action, or activity that is required to be documented by this manual or by the HIPAA Security Rule. An electronic copy will suffice as written form. If signatures are required, a scanned copy may be kept. The District Security Office shall maintain such records for all sites. The Local Security Officer shall maintain records for all sites he/she is responsible for.

# A. Documentation Procedure

**Time limit:**

All documentation required by this manual or by the HIPAA Security Rule shall be retained for a period of six (6) years from the date of its creation, the date it was last in effect, or the time as outlined by the Georgia Common Records or Health Services Record Retention Policies, whichever is the later date.

**Availability:**

All documentation required by this manual or by the HIPAA Security Rule shall be made available to those persons responsible for implementing the procedures or updates to procedures, and/or to those responsible for taking action(s) to which the documentation pertains.

**Updates:**

It may become necessary to update policies and procedures contained in this manual. It may also be necessary to add policies and procedures in order to comply with the HIPAA Security Rule or subsequent federal or state law. The need for updates or additions may become necessary as a result of:

1. Periodic review of the policies and procedures,
2. Response to a reported incident,
3. Response to an environmental or procedural change to business operations,
4. Response to a vulnerability identified during a periodic assessment,
5. Recognition of a vulnerability by a member of the workforce or the public,
6. Other means.

In the event that the need for an update to the policies and procedures is recognized, the following procedure should be followed:

1. The District Security Officer will perform the necessary research to develop the terms of the update.
2. The District Security Officer will make a formal recommendation for the update to the District Management Team. Any necessary modifications will be negotiated at this time.
3. If approved, the update will be incorporated into the HIPAA Security Manual and distributed to all sites.

# Glossary

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Computer Equipment:
Includes a full range of data handling equipment such as servers, workstations, PCs, terminals, thin clients, laptops, netbooks, tablets, i-pads, PDAs, smart phones, blackberries, and peripherals such as flash/thumb drives, external hard drives, printers, and scanners. The definition expands as technology advances to include all new forms of related data handling equipment.

Day: Business day.

Documents:
Document files include, but are not limited to, the following types of files: Word Processing (.doc, docx .rtf, .txt, .pub); Portable Document Format (.pdf); Spreadsheets (.wk1, .xls); Powerpoints (.ppt)

ePHI: Electronic Protected Health Information: Protected Health Information that is transmitted by electronic media or maintained in electronic format or on electronic media.

HIPAA: Health Insurance Portability and Accountability Act

IT: District 2 Public Health Information Technology Department.

PHI: Protected Health Information: Health information pertaining to an identifiable patient, which is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and which relates to the past, present, or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient, and that identifies the patient, or for which there is a reasonable basis to believe the information can be linked to the patient, and which is transmitted, recorded or maintained in any form or medium.

Programs: Programs include, but are not limited to, the following types of files: Batch (.bat); Command (.com); Executable (.exe); and Macros.

Unsecured ePHI:
Protected health information that is not secured through the use of a technology or methodology specified by the HHS Secretary. In the absence of such guidance,

unsecured ePHI is protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals, where such technology standard is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

User ID: User Identification, also called a User Login.

Year: Fiscal year.

# District 2 Public Health

# HIPAA Security Policies And Procedures

**Adopted: 09/16/10**
**Revised: 07/22/13**
**Revised:** 0**3/12/14**
**Revised: 01/01/16**

Dr. David N. Westfall, M.D., M.P.H., C.P.E.
District Health Director

Date

# Security Forms and Addenda

Facility/Access Log

Evaluation/Audit Checklist

HIPAA Incident Report

Breach Notification Log

Virus Report/Log Form

ePHI Systems Access Form

Consent to Text Personal Health Information

Mobile Device Acceptable Use and Acknowledgement

Required and Supported Security Software

**FACILITY / ACCESS LOG**

| Date | Structural Change* | or | Contractor** | System Accessed | Time In/Out |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

* Structural, and/or system changes that are made to the facility that will affect access or security, including changing door locks, changing alarm system/security system codes, addition of doors or windows, addition of walls or partitions, removal of walls or partitions, installation of a new security/alarm system, etc.

** Outside contractors involved with the District's or County Boards of Health's data systems, when they access those systems.

# EVALUATION / AUDIT CHECKLIST

**Date:**_____ **Sufficient = S** **Needs Improvement = NI**

| **A. Security Management Process** | **S** | **NI** | **Comments** |
|---|---|---|---|
| 1) Risk assessment completed within fiscal year | | | |
| 2) Documented review of all relevant losses to data integrity completed | | | |
| 3) Security measures implemented for all risks identified | | | |
| 4) Sanctions policy implemented appropriately and documented for all security incidents | | | |
| 5) Logs, activity reports, or other system management mechanisms reviewed quarterly | | | |
| 6) Security Officer assignment is current | | | |
| **B. Workforce Security/Information Access Management** | | | |
| 1) Authorization procedures for user access to ePHI followed by all supervisors and documented in Track-IT | | | |
| 2) ePHI Systems Access Forms on record and up-to-date for all users | | | |
| 3) Procedure to terminate access to ePHI followed and documented for all separated employees | | | |
| **C. Security Awareness/Training** | | | |
| 1) Routine periodic security updates disseminated to all staff by security officer | | | |
| 2) Security awareness training as part of new employee orientation documented for all new employees | | | |
| 3) Periodic updates to security awareness training documented for all employees. | | | |
| **D. Security Incident Procedures** | | | |
| 1) Incident report form filled out and submitted by staff to SO for all security incidents. | | | |
| 2) All security incidents thoroughly investigated and documented | | | |
| 3) Outcome of all security incident investigations documented | | | |
| 4) In the event of a breach, all notification requirements complied with and documented | | | |
| **E. Contingency Plan** | | | |
| 1) All servers containing ePHI backed up daily and backup clearly labeled and stored in secure location | | | |
| 2) All virus attacks logged, and steps implemented to prevent reoccurrence | | | |
| 3) UPS/generator systems maintained in good working order | | | |
| 4) Virus quarantine log shows no unreported viruses | | | |
| 5) Any disaster recovery incidents documented properly | | | |

# EVALUATION / AUDIT CHECKLIST - PAGE 2

**Date:**_____ **Sufficient = S** **Needs Improvement = NI**

| **F. Business Associate Contracts** | **S** | **NI** | **Comments** |
|---|---|---|---|
| 1) Business Associates having access to ePHI have all been identified and signed current version of the BA agreement | | | |
| **G. Facility Access Controls** | | | |
| 1) Only authorized employees have access to keys and security codes to enter primary and backup facilities during non-business hours | | | |
| 2) Security maintained on all servers and server locations | | | |
| 3) Non-authorized persons are escorted by staff unless other, appropriate arrangements are made with facility SO | | | |
| 4) ID badges, keys, entry key cards, etc. are collected on last day of employment from separated employees, and are documented | | | |
| 5) Log maintained of all systems access by non-authorized persons and structural changes to facility affecting access | | | |
| **H. Workstation Use/Security** | | | |
| 1) Employees power off computers at close of business day | | | |
| 2) Employees log off all ePHI systems or lock workstation when leaving their workstation for an extended period of time | | | |
| 3) No software is installed on workstation without IT authorization | | | |
| 4) No hardware, including modems, is connected to workstation without IT authorization | | | |
| 5) No ePHI is stored on workstations or shared network directories/folders without IT authorization | | | |
| 6) No ePHI is transmitted via e-mail except by IT authorized methods | | | |
| 7) All passwords are maintained in a confidential manner | | | |
| 8) No family members or other unauthorized persons are allowed to use computers | | | |
| **I. Device and Media Controls** | | | |
| 1) All optical and magnetic storage media is stored, transferred, and disposed of properly | | | |
| 2) A fully documented log of transferred devices is maintained | | | |
| **J. Audit Controls** | | | |
| 1) A log of attempted unauthorized system intrusions is maintained, if the capability exists | | | |
| 2) For all successful intrusions, solutions were implemented to deter future intrusions using the same method of access | | | |

# HIPAA INCIDENT REPORT

As required by the Health Insurance Portability and Accountability Act (HIPAA), the following documentation is submitted regarding a possible violation of one or more HIPAA Privacy or Security Regulations.

Type of Incident: ☐ Privacy ☐ Security ☐ Both ☐ Unsure

Date of Incident: _____ Date of Report: _____

Form Completed By:
Name: _____ County/Program of Employment: _____
Worksite: _____
Title: _____ Phone: _____ Fax: _____

Email Address: _____ Signature: _____

Incident Details:

| | |
|---|---|
| Date of Discovery: | |
| Location(s) affected or involved: | |
| Person(s) affected or involved; Include witnesses: | |
| Description of Incident: (Provide detailed description below, attach additional documentation if necessary.) | |
| | |

| This section to be completed by Local or District Privacy or Security Officer! |
|---|
| Investigation Notes: (Describe investigation including any interviews conducted and/or any actions taken.) |
| |
| Mitigation/Follow-Up: (Describe actions taken to mitigate damages and prevent recurrence of incident.) |
| |

Date Incident Closed: _____ Closed By: _____
Signature: _____

Employee Signature: _____
I have been informed of my involvement in this incident and understand the consequences of such involvement, as well as consequences of any future incidents of the same nature.

**BREACH NOTIFICATION LOG**

Date of Breach:_____

Brief Description of Breach, including location and means:

| |
|---|
| |

Persons Affected / Notified*:

| **Name** | **Address** | **Date Notified** | **Method** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

* Attach example copies of all letter(s), media releases, web-site postings, etc., utilized.

BREACH NOTIFICATION LOG - PAGE _____

Date of Breach:_____

| **Name** | **Address** | **Date Notified** | **Method** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**VIRUS REPORT/LOG FORM**

| Date of Virus: | System: (PC, Laptop) | System Location: | System User: | Virus Information: (Name, Description, Etc) | Date Reported to District IT: | IT Resolution: |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**EHPI Systems Access Form**

Employee Name:_____ Empl. ID#_____

Place a checkmark by each system to which the employee has a login. As access to additional systems is granted, add new checkmarks. For systems not listed, please notify IT, and write them in as "Other". If employee access to a system is officially removed, please record the date removed on the form in the field marked “Data Access Ended”. (Note that “access ended” does not mean the employee stopped using a system, but rather that their login was removed, so that they CAN'T use the system.)

| Access | System | Login ID | Date Access Ended |
|---|---|---|---|
| ☐ | Outlook | | |
| ☐ | VHN (M&M) | | |
| ☐ | Garrison DHD | | |
| ☐ | GRITS | | |
| ☐ | Care 360 (Quest) | | |
| ☐ | MLab (State Lab) | | |
| ☐ | Covansys | | |
| ☐ | GWIS | | |
| ☐ | GWISnet | | |
| ☐ | SENDSS | | |
| ☐ | CareWare | | |
| ☐ | BreasTest & More Access Database | | |
| ☐ | BBH Access Database | | |
| ☐ | Indigent Care Spreadsheet | | |
| ☐ | Drug Room Computer | | |
| ☐ | CWSN Server | | |
| ☐ | CWSN Oracle Database | | |
| ☐ | CWSN Referral Tracking Access Database | | |
| ☐ | CompuMedic Scheduler | | |
| ☐ | CMS Kids Access Database | | |
| ☐ | Babies Can't Wait Access Database | | |
| ☐ | RBB Access Database | | |
| ☐ | Children 1st Access Database | | |
| ☐ | District Hall4 Server - private and shared drives* | | |

(*This is where you log onto your computer, not as district2, but as yourself, e.g. mmouse.)

| Access | System | Login ID | Date Access Ended |
|---|---|---|---|
| | Billing | | |
| ☐ | Medicaid (mmis.georgia.gov) | | |
| ☐ | Amerigroup (amerigroupcorp.com) | | |
| ☐ | Wellcare (georgia.wellcare.com) | | |
| ☐ | Peach State (pshpgeorgia.com) | | |
| ☐ | DentaQuest (dentaquestgov.com) | | |
| ☐ | Scion (sciondental.com) | | |
| ☐ | EDI (edidirect.acs-inc.com) | | |
| ☐ | eDispense (edispense.com) | | |
| ☐ | United Healthcare (unitedhealthcareonline.com) | | |
| ☐ | Cigna (cignaforhcp.cigna.com) | | |
| ☐ | PaySpan Health (payspanhealth.com) | | |
| ☐ | Medicare dial-in | | |
| | Other | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |
| ☐ | | | |

All _____

Public Health
Prevent. Promote. Protect.

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

# Consent to Text Personal Health Information

Date:_____

District 2 Public Health [**PROGRAM**] would like to contact you by text to discuss your personal health information and/or health related issues. The specific health information sent will be limited to the extent possible. However, it is important to note that information sent by cell phone or text is NOT secure. **Your personal health information sent or received by this means could be viewed or accessed by others.** By agreeing to communicate via text, you agree to accept any unintentional disclosure of your protected health information sent or received by this means.

Also note that you may incur a cost (on your cell phone) if you receive a text message from District 2 Public Health [**PROGRAM**].

**Option 1 - YES**:

I _____ would like to communicate about my personal health and/or health related issues with District 2 Public Health [**PROGRAM**] by text message. I understand that information sent by cell phone or text is not secure, and I agree to accept the risk and any unintentional disclosure of my personal health information communicated by this means. I understand that by selecting this option, I will be responsible for any costs assessed by my wireless carrier that are associated with receiving messages. I must inform District 2 Public Health [**PROGRAM**] of any changes to my cell phone number or any cancellation of cell phone service.

My cell phone number is _____

District 2 Public Health [**PROGRAM**] may continue to send and receive my personal health information by text until I contact their office to discontinue this service.

**Option 2 - NO**:

I _____ do not want to communicate about my personal health and/or health related issues with District 2 Public Health [**PROGRAM**] by text message. I understand that by selecting this option, I may still receive phone calls, letters, or other forms of communication based on any other consents I have given.

**Signature:** _____

Public Health | District 2
Gainesville, GA

# Mobile Device Acceptable Use and Acknowledgement Form

Name: _____ Date: _____

Job Title: _____ Department: _____

Description of Mobile Device: _____ Mobile Phone Number Assigned: _____

Serial #: _____ MAC Address: _____

Accessories: _____ Wireless MAC Address: _____

***I certify that:***

- I have read and agree to abide by the current District 2 HIPAA Security Manual, paying particular attention to the Workstation Use and Security Policies and Procedures.
- I understand that I am responsible for any and all data breaches or loss of ePHI should I not strictly adhere to the current District 2 HIPAA Security Policies and Procedures.
- I understand I must complete this acceptance agreement form in order to receive a District 2 mobile or electronic messaging device.
- I understand the IT Department will manage and monitor the device. Modification and/or removal of any tracking or monitoring software is forbidden.
- I understand that the IT Department must approve software and apps prior to installation.
- I understand that I must return the equipment to the IT Department upon demand, and must notify the IT Department immediately upon damage or loss of the device.
- I understand that equipment must be returned to the IT Department upon termination of employment.

_____ _____
Employee's Signature Date

_____ _____
Receipt of Equipment Date

_____ _____
Dispensing Technician Date

Additional Accessories:

# Required and Supported Security Software

The following software is required to be installed on District 2 owned computers.

Required:

- Symantec Endpoint Protection
- Malwarebytes Anti-Malware from www.malwarebytes.org
- CCleaner by Piriform
- 7 Zip
- Flash
- Shockwave
- Java is to be kept up-to-date with the Security Tab set to High.
  Websites can be added to the Java Exception Site List only when that site is required for an employee to complete their assigned work.

Supported by IT as needed:

- Spybot Search and Destroy
- RKill (root kits)
- SuperAntiSpyware

Mobile Security Apps:

All cell phones and tablets are required to have a Google license purchased each year by the requesting department. (Cost is approximately $50.00 per year.)

Devices are managed through the District's Google d2ph.org domain.

- Google Device Policy
- Android Lost
- Norton Mobile Security

Mobile App Courtesy Install:

- Ready Georgia