

## **Data System Usage and Security**

### **References:**

Confidentiality of Personal Information -Policy 1401  
Disciplinary Actions, Including Adverse Actions -Policies 1601A & 1601B  
Standards of Conduct -Policy 1201  
U.S. Copyright Law -Title 17, U.S. Code  
Federal Electronic Communications Privacy Act (ECPA) 19 U.S.C.-2510  
Preventing Workplace Violence -Policy 110  
Health Insurance Portability & Accountability Act –Public Law 104.191, 164.302-318

### **General Provisions:**

Computer information systems and the network are an integral part of business at the NWGA Health District and the County Boards of Health that make up the district. They are an important resource to provide timely, efficient and cost effective data and communication services.

Computers and networks are provided for employees who are affiliated with the county boards of health and the district office for the efficient exchange of information and the completion of assigned responsibilities consistent with the agency's statutory purposes. The use of these systems and the network by any employee will be consistent with this policy.

### **Purpose:**

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. The use of the words "**network**" and "**system**" refer to all computers, software, terminals, modems, e-mail, Internet, and any other computer related components, software or functions.

### **I. Administration:**

The data system is the responsibility of the appointing authority for the County Boards of Health personnel. This responsibility may be delegated to the District's Information Technology Director/HIPAA Security Officer (IT Director) 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. Employee's Responsibility:**

## **General**

1. Know and abide by all County Board of Health policies dealing with security and confidentiality of business records.
2. Initiating and/or transmitting any content that is offensive, harassing, or fraudulent is prohibited.
3. Know and abide by all applicable policies for network and computer usage.
4. Employees must not transmit copyrighted materials inappropriately as this is a violation of the U.S. Copyright Law -Title 17, U.S. Code.
5. Employees shall power off their computer at the close of business each day and when leaving their workstation for an extended period unless approved by the IT Director/HIPAA Security Officer. A computer is considered off when all the lights on the system unit are off. All modems attached to live systems must be powered off when not in use.
6. Employees shall not install any software regardless of the source without authorization from the IT Director/HIPAA Security Officer. Authorization can be obtained via email.
7. Employees are prohibited from allowing family members from using any of the County Board of Health's computer equipment. This includes laptop computers that may be carried home for official use by the employee.
8. Employees are responsible for maintaining copies of critical documents on the server and workstation for backup purposes.
9. Employees may not add hardware or reconfigure any portion of the data system without approval of the IT Director/HIPAA Security Officer.

## **Internet**

1. Internet access is for Public Health business and may not be used for purposes that would violate any policy of the County Board of Health.
2. Employees may use the Internet for occasional personal use to the extent that it does not interfere with work, or violate any other policy.
3. Non-business use of: animations; webcasts; chat rooms; listening to music or radio stations through the Internet; and the use of unauthorized Instant messengers are prohibited.
4. Excessive or inappropriate use or random web browsing unrelated to the business of

Public Health may result in loss of Internet access and other disciplinary action.

5. Data transfers containing EPHI (Electronic Protected Health Information) via the Internet will use encryption as soon as encryption becomes practical for each application.

### **Passwords and user IDs**

1. All employees must maintain confidentiality of personal passwords. Passwords and user IDs shall not be shared with others or recorded in conspicuous places unless authorized through the District's IT Director/HIPAA Security Officer. Authorization can be obtained via email.
2. Employees shall change passwords as required by individual systems and will change passwords immediately if it is suspected that others may know them.
3. Employees shall be responsible for all computer transactions that are made with his/her User ID and password for each network facility they have access to.
4. Passwords will be a minimum of 8 characters long, contain 2 numbers and mixed case characters.
5. To ensure the integrity of database audit trails, users accessing EPHI will not be allowed to have multiple simultaneous logins by default. Those whose job functions indicate the need for multiple connections may be granted such so long as the local or District HIPAA Security Officer Designates:
  - Which people are authorized for access via multiple connections
  - Which computers to be used for multiple connections.
  - What the multiple connections are to be used for - lab, Immunizations, portal etc.
  - Users must log out of M&M, HOST, HN2 or any other client database on these machines when they walk away under penalty of HIPAA security sanctions.
  - Employees remain fully accountable for transactions made with their user ID.
  - These computers will be limited to the necessary, documented functions designated above. 164.312
6. Logins shall not be shared.
7. Any system that has an automatic logoff function available will have it implemented. Idle time will be no more than 5 minutes. 164.312
8. Windows screen saver logoff functions will be implemented for users who do not access shared databases. 164.312

### **Email**

1. While e-mail is intended for official purposes, incidental and occasional personal use of

the GroupWise e-mail system is authorized. Short personal messages to individuals or to small groups are acceptable as long as no policy is violated. However, e-mail users must exercise common sense, good judgment, and propriety in the use of this resource.

2. E-mail sent to large groups of users is not authorized for personal reasons such as selling, conducting personal business or chain letters or for business reasons without supervisor's approval.
3. Email containing animated greetings or Internet links to animated greetings or other animations is prohibited.
4. Users who receive email containing prohibited content must advise the sender that they do not want to receive such email.
5. Using unauthorized private e-mail from a work location is prohibited.

**B. Supervisor's Responsibility:**

1. Supervisors are responsible for ensuring employees within their unit comply with this and all other applicable policies and rules.
2. Supervisors are responsible for reviewing with new employees the County Board of Health's Data System Usage Policy and have them sign the agreement documenting that they have reviewed the policy if the IT Director/HIPAA Security Officer was unable to do it on the employees first day. The agreement sheet(s) or a copy must be sent back to the IT Director as soon as possible.
3. Supervisors must monitor access frequency by contractors involved with the district's or county board of health's data system by maintaining an activity log. Information maintained should describe who, the purpose of the access, what was done and date of access. (Examples are DHR/IT, ABC Accounting, Teletask and M&M.)
4. Supervisor must initiate prompt, effective counseling with employees who violate this or any other applicable policies.
5. Initiate appropriate actions consistent with personnel policies when employees repeatedly violate this or any other applicable Policies. Disciplinary action may result in the loss of System Access or dismissal from employment.
6. Monitor the system at his/her unit to ensure computers and modems are shut off at night. Supervisors are responsible for making arrangements with outside contractors such as M&M if modems must be left on during non-business hours for installing upgrades etc.
7. Report all virus-warning messages immediately to the District IT Director, and remove the unit from service at the discretion of the IT Director.

8. Include in every employee's PMF a requirement to comply with all network usage and security policies.
9. Provide prompt feedback to the IT Director/HIPAA Security Officer when violations by employees are presented to them.

**C. Information Systems Unit Responsibility:**

1. Maintain security of the system with regard to HIPAA, intruder protection, virus protection, password security and administration and backups of client data.
2. Administer the system including user administration, network applications, printers, business continuity contingency planning.
3. Approve and install any software requested by a supervisor that:
  - Has a legitimate business purpose
  - Does not compromise system security or performance
  - Is consistent with long-term data system strategy
  - Has a documented strategy complying with security, billing, reporting requirements etc as appropriate
  - Is legal
  - Software or system changes described as "Required" must be accompanied by supporting documentation from the entity imposing the requirement.
4. Repairs, maintenance and installation of servers, computers, printers and any other system hardware or software components that are not covered by external contracts.
5. Provide software support and hardware support to users, or direct them to other support as needed.
6. Apply all meaningful patches, updates and upgrades.
7. Advance our applied technologies where opportunities exist in an efficient and cost effective manner, consistent with long-term objectives.
8. Develop and maintain written standards and procedures necessary to ensure compliance with appropriate and intended use of the system.
9. Provide appropriate authorization, access, support, and guidance to assist employees in fulfilling their data system needs and obligations.
10. Review this and any other applicable system use and security policies with every new employee and existing employees when appropriate.

## D. Responsibilities of Local and District HIPAA Security Officers

164.308(a)(2) Assigned security responsibilities Required

The Appointing Authority is required to designate a HIPAA Security Officer. At this time that person is the Director of Information Technology. The District HIPAA Security Officer will ask local management to nominate Local Assistant HIPAA Security Officers. The District HIPAA Security Officer may approve or decline these nominees based on the nominee's technical knowledge and skills.

It is the responsibility of the District HIPAA Security Officer to develop, implement and enforce policies to ensure compliance with HIPAA Security.

It is the responsibility of Local HIPAA Security Officers to ensure compliance at their locations consistent with this policy. They will be granted some privileges for the purpose of local user and printer administration, software updates and other tasks in cooperation with District OIT.

164.308(a)(1)(C) Sanctions Policy Required

All provisions in the Data System Usage and Security Policy are there to address specific risks and vulnerabilities to the system. Therefore, any violation of any section of the policy constitutes a risk to the data system.

The District and Local Security Officers will maintain a log of all violations.

Violations resulting in disclosure of, damage to, or loss of EPHI are obviously more severe, and must be addressed more aggressively. In either case, denying the offender access to the system will mitigate the threat. Once the immediate threat is removed, the sanctions schedule below will be applied. Access to the system will be restored or denied according to the sanctions schedule. This policy will be enforced uniformly.

Offense	EPHI Disclosed	No EPHI Disclosed
First	Verbal reprimand with note to the District HIPAA Security Officer	Verbal reprimand with note to the District HIPAA Security Officer
Second	Written reprimand	Written reprimand
Third	Up to two week suspension without pay	Up to one week suspension of system privileges
Fourth	Dismissal from employment	Permanent suspension of system privileges

164.308(a)(3) Workforce Security

Procedures must be followed to ensure that all employees requiring access to EPHI have it at the appropriate level, and those who's job function does not require access to EPHI do not have it. This section applies to everyone including supervisors, seasonal, temporary, contract and part time employees.

164.308(a)(3)(A) Authorization and/or supervision Addressable

Prior to being granted access to EPHI, all employees must attend orientation, which includes a detailed review of the Data System Usage and Security Policy. The employee must sign the agreement page of the policy, and be given a copy of the policy.

164.308(a)(3)(B) Workforce Clearance Procedure Addressable

Each supervisor must complete an EPHI access Clearance form for any employee requiring access to EPHI. It is the supervisor's responsibility to ensure that the employee is an appropriate person to have access to various EPHI.

164.308(a)(3)(C) Termination Procedure Addressable

As soon as it is known an employee is leaving, the employee's supervisor and Personnel must notify the District HIPAA Security Officer via email. All access to any portion of the data system will be revoked as soon as any person is no longer actively employed. The supervisor is responsible for getting any IDs, keys, cards or other means of access from employees upon termination. Any access codes or passwords known to departing employees that are used by others must be changed at that time.

164.308(a)(4) Information Access Management

Implement policies and procedures to limit employee's access to EPHI to what is required for their role.

164.308(a)(4)(A) Isolating clearinghouse functions Required Not Applicable

164.308(a)(4)(B) Access Authorization Required

Prior to creating a user account or to granting an employee access to EPHI, the Security Officer must have a signed Data System Usage and Security Policy acknowledgement form and an EPHI Access Clearance form from the employee's supervisor.

164.308(a)(4)(C) Access establishment and modification procedures Required

When a user's level of access requires modification either to add or remove access, a new EPHI Access Clearance form must be submitted to the Security Officer.

164.308(a)(5) Security awareness and training

164.308(a)(5)(A)

New employees - See existing policy

Security Reviews – The Security officer will provide a formal security session annually at each site.

Special Reminders - Whenever unique current risks become known, special memos, reminders and updates will be emailed to every user.

164.308(a)(6) Security Incident Procedures – Required

Any employee who witnesses, discovers, or otherwise gains knowledge of a security incident, must complete a Security Incident Report form and submit the form to the local Security Officer. If the local Security Officer is party to the incident, or is the employee reporting the incident, (s)he will

submit the report to the District HIPAA Security Officer. The District HIPAA Security Officer will verify the complaint and take whatever action is necessary to mitigate the breach pending a full investigation and remediation.

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

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

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 the completion of an investigation, the District HIPAA Security Officer will maintain a permanent record of the incident, the investigation, and the outcome. The Security Officer will also forward a copy of the complete documentation to Personnel or others as appropriate.

#### Business Associate Policy 164.308(b)(1)

To ensure that all new and/or previously established Business Associate contracts and Agreements are developed and/or modified appropriately to accommodate the requirements as stated under the Security Rule, Section 164.308(b).

#### **Policy:**

The County Board of Health may permit a business associate to create, receive, maintain, or transmit Electronic Protected Health Information (EPHI) on its behalf only if the County Board of Health obtains satisfactory assurances that the business associate will appropriately safeguard the information. 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).

#### **Procedures:**

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

- Identify current Business Associates hired by the covered entity who have access to electronic protected health information;
- As appropriate, prepare an addendum for existing Business Associate contracts and Agreements requiring the Business Associate to implement administrative safeguards to protect the confidentiality, integrity, and availability of electronic protected health information as addressed in the Security Rule. Obtain signatures from Business Associates assuring they will abide and safeguard the information.

- Modify existing Business Associate Contracts and Agreements to address the Security Rule and implement with new Business Associates as appropriate.

## **Business Associate Agreement Attachment A**

The following text will be included in all data system related contracts.

Business Associate Agreements to comply with the HIPAA Security Rule:

The Business Associate understands the importance of the security of a patient's "electronic protected health information" ("EPHI") and agrees to protect that right to the extent necessary under this Agreement and under current federal and state law. For purposes of this Agreement, "electronic protected health information" is any data or other information as defined by the Department of Health and Human Services in the Code of Federal Regulations, Title 45, CFR Subpart A, Sec. 160.103

As required by the HIPAA regulations, the Business Associate shall make the following assurances to the Provider:

- The Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any patient's "electronic protected health information" ("EPHI") that the Business Associate creates, receives, maintains, or transmits on behalf of the Provider.
- The Business Associate shall ensure that any agent to whom it provides EPHI, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect such EPHA.
- The Business Associate shall report to the District HIPAA Security Officer any security incident of which it becomes aware.
- The Provider may immediately terminate this Agreement if it determines that the Business Associate has violated a material term of this Agreement.

### 164.310 Physical Safeguards

To provide facility access guidelines for the purpose of data restoration under the disaster recovery plan and in emergency mode operations in order to comply with HIPAA Security Rule section 164.310.

### **Policy:**

It is critical that Electronic Protected Health Information (EPHI) maintained on the County Board of Health's computer system be kept secure and confidential in accordance with the Public Health Policy of Confidentiality. Since EPHI is stored on the application file server, it is equally that proper measures are taken to secure the application file server.

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 patient information is protected from unauthorized access.

### **Procedures:**

Facility access for authorized staff:

Authorized employees will have items necessary to enter the primary and backup facility during non-business hours in their possession (keys, security codes, etc.)

The County Board of Health staff will escort any non-authorized individual unless other arrangements are made with the facility Security Officer or other designated person. A log of all such access will be maintained by the Security Officer or other designated person.

All non-County Board of Health individuals must sign Business Partner Agreements or Confidential Statements, whichever is appropriate, before accessing files or equipment containing EPHI.

Upon employee termination, all identification badges, facility keys, entry key cards, etc. will be collected on the last day of employment. This will be documented and maintained by the facility Security Officer or other designated person.

If electronic keypad access is utilized, individual unique access codes must be used for facility access if possible. Codes known to those no longer authorized must be changed.

The Security Officer or other designated person must maintain a log of all structural changes which occur on the facility that will affect access, such as door locks, security hardware, doors, walls, etc.

1.

## **II. E-mail**

All system users within the District Office/County Board of Health have access to GroupWise for business related e-mail. GroupWise is the only generally authorized e-mail platform in this organization. Under limited circumstances and with prior approval from the District's IT Director, certain users may receive authorization to access other e-mail systems providing they can demonstrate a business need, and adequate security can be assured.

### **A. Confidentiality/Privacy:**

1. While the e-mail system is designed to be secure, i.e., it employs encryption technology on all messages traffic; users are not guaranteed absolute privacy of their e-mail.
2. Supervisors, under rare emergency conditions, will be granted access to a users e-mail account. Submission of a signed written request with approval from the appointing

authority is required prior to being granted access.

## **B. Security:**

1. Authority to access other employee's e-mail communication shall only be accomplished by GroupWise proxy.
2. All employees, including system administrators and supervisors are expressly prohibited from violating the security of the e-mail system.
3. All e-mail users are required to have and use an eight-character e-mail password in addition to a network password, as well as any system that allows passwords to be used.
4. Client data may not be stored on systems where passwords are not required or are ineffective.
5. Passwords should be periodically changed.

## **C. Email containing Protected Health Information and HIPAA**

### **PURPOSE**

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

### **GENERAL POLICY**

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

### **PROCEDURES**

#### **PHI in E-Mail**

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

## **Example Confidentiality Statement**

“This message and any included attachments are from the [County] Board of Health and are intended only for the addressee(s). The information contained herein may include privileged or otherwise confidential information. Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited. If you receive this message in error or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by email. Thank you.”

## **Receiving PHI in E-Mail in Error**

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

## **D. Monitoring**

1. All messages created, sent, or retrieved over the Internet are the properties of the County Board of Health, and are public records. The appointing authority reserves the right to access the contents of any messages sent over its facilities to monitor system usage. All communications, including text and images, can be disclosed to citizens, law enforcement, courts, lawyers, etc. if appropriate procedures are followed for gaining access to specific information. Therefore, one should not put anything into e-mail messages that an employee would not want to see on the front page of the newspaper or be required to explain in a court of law.
2. Any e-mail system in use at a work location is government property. Therefore, periodic, monitoring by individual supervisors or the IT Director/HIPAA Security Officer for appropriateness of content may be authorized by the appointing authority.

## **IV. Computer Viruses**

Computer viruses are programs designed to make unauthorized changes to programs and data , and are much easier to prevent than to cure. Viruses can cause destruction of any or all Public Health data. Therefore, employees should protect against computer viruses by:

1. Using only data and programs that have been approved by the IT Director.
2. Utilizing District approved anti-virus software.
3. Using good judgment when accessing web sites.

4. Report all virus-warning messages immediately to their supervisor and the District IT Director.
5. When a user's computer is chronically and repeatedly infected, that user may be denied access to the Internet, email, or the entire data system.

## **V. DESTRUCTION OF PROTECTED HEALTH INFORMATION**

### **PURPOSE**

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

### **GENERAL POLICY**

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

### **PROCEDURES**

Protected health information should be destroyed in accordance with state approved records retention schedules (OCGA § 50-18-102). This information must be destroyed so that they cannot be read, interpreted or reconstructed. Further guidelines on records destruction can be found in DHR Operating Procedure No. IX, dated September 23, 1993.

Records are to be destroyed according to schedule referenced above if the schedule permits destruction.

Records not specified in the schedule referenced above should be destroyed whenever they are deemed of no further use.

### **Methods of Destruction**

Paper records must be shredded or burned.

Microfilm records must be burned or destroyed by use of a chemical solution.

Email and attachments should be deleted and the "Trash" must be emptied.

Electronic media that has stored PHI must be destroyed if it is no longer being utilized. Types of magnetic media and appropriate destruction methods are:

Floppy or other removable magnetic disks – destroy by removing magnetic media from its casing and cutting the magnetic media.

Magnetic tape – destroy by removing media from the tape hub and cutting the media

Hard disk drives – remove unused hard disk drives from computers and destroy the drive

Compact Disks – destroy by breaking the disk

Or delivered to the District Office of Information Technology for destruction.

## **VI. FILE SERVER SECURITY**

## **PURPOSE**

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

## **GENERAL POLICY**

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

## **PROCEDURES**

Physical Protection – Select low traffic area and one or more of the following methods for protecting the file server.

Secure the server to a permanent structure using a cable and lock

Place server in lockable server cabinet

Place server in a room that will be locked when authorized staff are not present

Backup Media – If the local Privacy Officer determines a need for backup to local media, they must designate staff to be responsible for backup and media storage. Store backup media in locked fireproof safe. Rotate one copy to secure off site location. Backup media should be placed in a locked container for transport and storage. Otherwise, PHI will be backed up to the District off-site backup system.

Firewall – Installation of firewall protection for the application file server is mandatory for servers with routable Internet addresses.

## **VII. FAXING PROTECTED HEALTH INFORMATION**

### **PURPOSE**

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

### **GENERAL POLICY**

Adherence to Public Health Policy of Confidentiality is expected with the use of facsimile when transmitting patient health information. Properly completed and signed authorizations must be obtained to release patient information unless specifically specified through State Public Health Law or regulations for internal public health use. An authorization transmitted via fax machine is acceptable, with verification for signature. In medical emergencies, the information may be

released without authorization when the provider or business associate requesting the information is required by law to treat the individual or when there are substantial communication barriers or threats to the health of the public. Health Departments may fax medical records using a notice of confidentiality on the agency letterhead. When using faxed duplicates instead of the original medical record, destroy the copied material once the use is completed. Fax users must be instructed on the proper procedures for handling of confidential information. It is recommended that specific patient healthcare information be faxed only when the data are to be used for patient care. HIPAA provisions allow facsimile of data for treatment, payment and healthcare operations without an authorization. Use of the fax for these reasons should only occur when the original document or mail-delivered photocopies will not serve the purpose. Fax machines must be located in a secure area that is protected from public view and available only to those employees legitimately entitled to access protected health data.

## **PROCEDURES**

### **For Transmitting PHI**

Use a cover letter for each fax transmission and retain it in correspondence. Verify by telephone when possible the availability of the receiver and log the fax transaction. Notify recipients of any misdirected or returned fax and file a HIPAA Privacy Rule incident report.

When the faxed information is to be included in a medical record, it must be clearly legible, complete, accurate and dated with appropriate signatures as indicated.

Faxed data must include:

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

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

### **For Receiving and Handling of Fax**

- Remove any incoming material

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

### **Examples of Confidentiality Statements**

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

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

“This facsimile may contain confidential or privileged information and is intended only for the recipient named above. Receipt of this transmission by any person other than the intended recipient does not constitute permission to examine, copy or distribute the accompanying material. If you receive this facsimile in error, please notify us by telephone and return the original facsimile to us by mail.”

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

164.308(a)(7) Contingency Plan

## Disaster Operation

In addition to the procedures for recovery of the data system, each site and each program is responsible for maintaining paper forms and documents to allow for operation for up to one week under any circumstances.

## Tape Systems

Two complete tape backups will be done on each server at installation and again when significant software updates are done. One tape will be stored at the site, and the other at District IT.

## General Fault Tolerant Approach

The data system configuration throughout the district consists of a multi-layered approach to facilitate disaster recovery in a variety of scenarios. If all elements of the data system are configured properly, failures within the district will have minimal impact, and be quickly recoverable through multiple techniques regardless of where in the system the failure occurs.

## Distributed server-based resources

Applications in the district are installed on multiple low-cost servers. An example is a county where HOST or another primary database is on one server, and GroupWise is on a different server. This would allow a portion of the Health Department's software to function even though some applications could not in the event of a single server total failure.

A single server failure would not cause the location to lose all functionality. Other backup schemes will capture enough critical data to restore the lost functionality on the remaining server, or a temporary server.

## Recovery and Continuity

In the event of a single total server failure, District IT will reinstall applications to a functional server at the site. If no functional server exists at the site, District IT will provide equipment that will act as a temporary local server. Data from the related applications will be restored from local backups. If no local backup exists data will be restored from district off-site backups if such data exists on the off-site backup system.

In the event that all servers at a site are lost, District IT will install applications on temporary servers. The related data will be restored from local or offsite backups if such backup data exists.

Temporary workstations can be setup from surplus computers or borrowed from the District or other counties.

## Mirrored drives or RAID 5 arrays on all servers

All servers purchased since April of 1999 came equipped with at least 2 identical disks. The servers with 2 drives are configured to use drive mirroring. Mirroring provides fault tolerance in that if one of the mirrored disks fails, Novell will take that disk offline and use the other as a single disk configuration. Recovery is automatic when the failed disk is

replaced.

## Recovery and Continuity

A failure in this scenario will involve only enough downtime to actually change the disk and reboot the server. This repair can be scheduled.

## Critical data off site backups

Our most critical county client data, environmental data and selected user directories are backed up automatically on a schedule to a server at the district. Select district data is backed up nightly to a server in building 510/512.

This data will be used to rebuild applications and restore functionality after a total server failure or disaster. It will keep many copies of this data for cases where latent virus infestations have occurred.

The total disk capacity in the district for all computers is currently somewhere in the neighborhood of 15 terabytes. There is no tape or disk system capable of backing up this much data.

## Virus Protection

We use a three layered virus protection system. All servers capable of running DHR supplied AV software are running it. These servers update the virus definitions daily. All workstations capable of running DHR supplied AV software are running it. Workstation virus definitions are updated daily. The GroupWise system has a virus filter.

In the event of latent, undetected virus infestation we would look to our offsite backups to find an uninfected past backup.

## Recovery and Continuity

Virus infestations can propagate in many ways from a variety of circumstances. Indeed no solid, every case scenario can be accurately defined. The BCP must then focus on likely scenarios, but remain flexible for unexpected events.

In most cases, a local computer can be cleaned of viruses. In an event where the virus has spread to a server, the server should be taken offline by removing the network connection. District IT staff will attempt to isolate the virus and clean the server. If the virus infests a site, the entire site may need to be isolated and cleaned including all servers and workstations.

Viruses can spread from LAN to LAN, site to site through a variety of channels. The most likely sources are via chain email, email attachments containing executables or infected macros. Viruses can propagate to any attached network drives. It is therefore imperative that users from one location do not map to drives at another location. For a rapidly spreading, destructive virus, no action could be fast enough to contain it to a single site. There are no such users in the district except District IT for administration

purposes.

### **VIII Summary of Responsibilities**

1. Each employee is responsible for ensuring that their use of any element of the data system complies with this and all other applicable policies and rules.
2. Each supervisor is responsible for ensuring that employees within their area of responsibility comply with this and all other applicable policies and rules, and to focus any corrective action solely on the violator's failure to meet the minimum acceptable standard for access to the system.
3. The IT Director is required to ensure that the all users, supervisors and IT staff comply with their responsibilities under this and all applicable rules and policies, and to act quickly to ensure system integrity is maintained when these rules are violated.

