

# Northwest Georgia Health District

## Data System Procedures

Software/Equipment purchasing procedure.....	2
Computer Equipment/Software Request.....	3
New/Obsolete User Procedure.....	4
Approved Software List.....	5
Specifically non-approved software .....	5
Taking care of your work files.....	6
Violations of Data System Usage Policy .....	8
Change Requests.....	9
Process for implementing HOST billing and code changes .....	10
Viruses, Intruders and other Security Issues.....	11
Unknown Computer technicians.....	11
Power off at night – unless otherwise authorized.....	11
Service requests .....	12
Report, Database and WEB Development.....	14
Report Request.....	15
Database Development Procedure .....	16
Web Development .....	18

## Software/Equipment purchasing procedure

Responsibilities of the District Information Technology Director regarding purchases:

1. Ensure that our technology dollars are spent wisely.
2. Ensure that hardware and software purchases are compatible with existing and future hardware and software, and are likely to remain so.
3. Ensure that no hardware or software purchased or used is likely to compromise network security or performance, or presents unnecessary risk to security or network performance.

At the time of this writing, the standard computer is a generic Pentium IV, 1 Gigabyte of RAM, 80 Gigabytes of disk storage, stereo sound, CD/DVD reader/writer, AGP video with a minimum resolution of 1024 x 768 at 16 million colors and a 17-inch monitor. It will come with the current version of Microsoft Office Professional installed. For locations where space is restricted, we are using 15" LCD panels.

Our standard laptop is a Gateway Pentium 4 with 512 Megabytes of RAM, 20 Gigabyte disk, CDRW, AGP video and stereo sound. It is equipped with a modem and network adapter. It comes with the current version of Microsoft Office Professional.

These machines are more than adequate for every user and every application in use in the district, as well as those likely to be deployed during the life of the computer. As technology and prices change, our standard computer model and installed software will change to keep pace.

Requests for equipment other than that described above will require additional rationale. Such rationale should be provided for each non-standard component. For example, if a computer were requested with Word Perfect in place of, or in addition to Microsoft Office, an explanation as to why it is *needed* to conduct the business of Public Health would be appropriate. Requests for hardware components such as CD writers and large monitors must include a business rationale as well.

You may want to discuss non-standard items with the Information Technology Director prior to submitting the request. Non-standard requests without adequate rationale will be denied. In no case can a new computer be acquired without a Computer Equipment Request Form having been submitted to the district procurement specialist.

A copy of the form is on the next page. You can also acquire a soft copy in MS Word format from Dave Hoitt 706-295-6788.

**Send the completed form via email to Pat Collins.**

## Computer Equipment/Software Request

This form can be copied and pasted into a GroupWise message.

Date:

County:

Requestor:

Equipment/Software description:

Rationale. If requesting non-standard or specific, equipment or software provide a rationale for each non-standard item.

Estimate of cost:

Supervisor:

Date approved:

Comments:

## New/Obsolete User Procedure

### New

Because of the large volume of sensitive data stored and processed on the Public Health data system, the scale of the system, connectivity to other systems, and the risks from hackers, viruses and vandals, a Data System Usage Policy has been developed for all system users in the Northwest Georgia Health District. This policy covers all computers in the district, and applies to all system users regardless of position or employment status.

On a new employee's first day of work, they will be at the district office to fill out required paperwork. At that time, they will be directed to meet briefly with the District Information Technology Director to discuss and sign the Data System Usage Policy.

If this does not occur at that time, they must read the policy, fill out the acknowledgment form and forward it to the Information Technology Director before they can be granted access to any part of the data system.

A copy of the Data System Usage Policy and the acknowledgment form can be acquired from Dave Hoitt 706-295-6788.

### Obsolete users

Personnel will notify the Information Technology Director via email or hardcopy immediately.

## Approved Software List

Any software normally used to conduct Health Department business is approved. This list represents several programs known to be in use. Other software can be added to this list by notifying Dave Hoitt at 706-295-6788.

- M&M
- CHAT
- HOST
- ECHO
- Quickbooks
- Any **existing** Word Perfect Suite component
- Any Microsoft Office component **Except Outlook**
- Any Windows version that came installed or was installed by District IT
- GroupWise (only approved email)
- Netscape if required by other approved software
- Mosby's
- R&R Report Writer
- Crystal Reports
- ARMIS
- PC Anywhere
- Closeup
- Salary Planning Tool
- PM Tools
- STD MIS
- Adobe

### Specifically non-approved software

- Any Internet-enabled software not required for the business of Public Health
- Any unlicensed software
- Any shareware, freeware or other downloaded software without explicit approval from the Information Technology Director.
- Any software not on the Approved Software list without explicit approval of the Information Technology Director.
- Microsoft Outlook and any other non-GroupWise email client software.
- Real Player and other Internet-enabled software except for official business.
- Games

## Taking care of your work files

Hardly anyone who has used a computer for any length of time has never lost a file. Somehow, it always seems to be an important file, or something that you have put a great deal of work into. Early mankind, after spending months chiseling out a few words on stone tablet would occasionally be dismayed when, with last little chip, the tablet would crumble. Early scribes would no doubt from time to time make a critical typo on the last line of a long text written in ink on parchment or papyrus. I say this only to point out that the problem is not new, it only presents itself in a different form today.

While these primitive systems offered no way of making a secure backup, or recovering from such disasters, modern systems do. That is not to say that anyone can avoid an occasional lost file, but unlike our primitive ancestors, we can take actions to minimize the impact of these disasters when they do happen. We still need to give it some thought, and we still need to be diligent, but we do have options that were not available 30 years ago.

There are two procedures I will describe here: backup to server, and version backup.

### **Backup to server**

Almost every user in the district has access to a network of some type. For most folks, their network disk area is called H:. H:, on our systems isn't really a physical disk, such as something you can hold in your hand. It is a reasonably secure area on a disk, on a server, reserved for use for each individual user. Each person on a network sees a drive H:, but one person's drive H: is not the same as any other's drive H:. They are unique areas on the servers. What you see on drive H: depends on who logged into Novell on the workstation you are using. By the same token, if an individual logs in on a different workstation, their drive H: is still their same drive H: as on any other workstation. It appears to move with the user.

The great thing with these network drives is that you can use them just like drive C: on the workstation. They will perform a bit slower, because the data has to be moved over the network, and the server is doing many things. This often makes them unsuitable to use as a "working" disk. On the other hand, they work great as a backup disk.

To use your H: drive to backup files, you can copy and paste them from where ever they are on your C: drive, to your H: drive. You can even have folders (directories) on your H: drive to keep things in order. You can also use File, Save As, to save copies of files to your H: drive. What these accomplish is, if your workstations crashes, the disk fails, a power glitch renders your C: drive unreadable, you can get your backup off of H: after the computer is repaired.

One word of caution, the disks in modern workstations are large. In many locations the workstations have larger disks than the servers. It is possible to fill and thereby disable a server by loading an H: drive with unimportant files. So use it, but be careful not to abuse it. When files become obsolete, they should be deleted from H: drive.

## Version Backup

For typical small documents, version backup isn't generally indicated, as they seldom fail and are easy to recreate. Large or complex files, may sometimes, for lack of a better word, self-destruct. Often, this doesn't become apparent until the next time the file is needed. This tends to happen in direct relation to the deadline at which it is needed, and the difficulty one would encounter recreating it. So the most likely time to lose a critical file of size, would be the morning it is needed, after the time it would be possible to redo it.

The version backup scenario can substantially mitigate your losses in the event of such an untimely disaster. Let's say you are working on a document that will take 3 weeks to complete. We'll call it "Book A", and we are starting it on a Monday. When you are ready to put it away for the night, you would select File, Save As, from the menu. Name it "Mon Book A". On Tuesday, save your work as "Tues Book A", etc. What this does for you is this, if on Wednesday you come in and "Tues Book A" has somehow become unusable overnight, you can revert to "Mon Book A" and only lose a single day of work, rather than the whole document. Massive and complex documents may warrant more frequent version saves as major changes are made.

Combine the two techniques

This is the safest way to go for major documents. Multiple versions, stored on multiple computers is as good as it gets. While it isn't effortless, it is the quickest and most reliable way you can safeguard your important works-in-progress.

Last item... Where you save files on your C: drive is important. All windows computers have a "My Documents" folder. You can create folders within "My Documents" to organize your files however you like. This provides a standard location where IT folks will look for salvageable files in the event a repair is done, or if the computer is replaced. This translates to: It is the safe place to keep your work. The only other standard salvageable location is your GroupWise archive, which is located in C:\archive. Files stored in other places on your C: drive may not be recovered in the event of repairs or replacement, as we will not know they are there, and may not be able to find them.

## Violations of Data System Usage Policy

There are essentially 3 areas where compliance with the District 1 Data System Policy is critical. Security considerations include physical security, back-ups, virus protection, passwords etc. The second critical area is related to things that can impact network performance. The third is compliance with State and Federal laws. Many matters related to each are enumerated explicitly in the Data System Usage Policy. Due to constant changes in technologies, software and the Internet, many issues of security and performance simply cannot be foreseen, and therefore policy related to these cannot be etched in stone. Often, decisions regarding new issues will need to be made immediately. Such matters should be addressed to the Information Technology Director.

District IT is charged with maintaining our networks to be as secure and efficient as possible. Therefore, guidelines may change quickly, even instantly. This section deals with how policy (new or existing) violations will be addressed.

In cases where users are observed to be in violation of the District Data System Usage policy, the infraction will be brought to the attention of the user. If the matter can be resolved at that level, it will be considered so at that time, and no further action will be necessary. In the event of a user being in violation and refusing to resolve the issue, the violation will be reported to the Information Technology Director, who will then discuss it with the appropriate director.

## Change Requests

This form can be copied and pasted into a GroupWise message.

Often, users and supervisors as well as technical people will make, or desire to make, changes to system hardware and software. From time to time, unexpected consequences occur as a result of failing to consider the total impact of the change. It is essential that IT be aware of desired changes to system hardware and software components so that related functions can be considered to the fullest extent possible, and technical people can plan to be available if needed. The consequences are not always apparent in the planning phase.

To minimize unintended problems, a change request should be submitted to the Information Technology Director. Print or edit this page, answer the questions as completely as possible, and forward it.

Date: \_\_\_\_

Description of the change, addition, removal, relocation:

What functions is the equipment/software used to perform now?

What functions do you see being impacted if this change is implemented?

Is continued functionality dependent on other systems not yet in place?

When does this need to be done?

## Process for implementing HOST billing and code changes

1. Carolyn Terry will forward the request and all relevant documentation to the
2. IT Director.
3. IT will update the master tables as required to implement the changes.
4. IT will use the network FTP facilities to install the updated tables on county systems.
5. Carolyn will be available for additional information and provide contact information as needed.

## Viruses, Intruders and other Security Issues

Virus incidents are becoming more common within our data system. How they are spread and how much damage they do are up to the creators of the viruses. Whether or not we create an environment that is susceptible to them is up to us. Our connectivity, through the state's network has several layers of security designed to protect our data from viruses and hackers. If we use the system properly, and stay away from behavior conducive to virus acquisition, we can expect to minimize the frequency and severity of these attacks.

If, on the other hand, we check our personal email accounts from work, download Internet freeware programs, and fail to protect the confidentiality of our passwords, we can reasonably expect to suffer catastrophic data loss or compromise at some point. Safe usage of the data system cannot, therefore, be considered optional.

In the event of a virus warning appearing on your screen, you should stop what you are doing and call IT. Consider the computer to be unusable until IT has authorized it to be brought back online.

Sometimes, an active virus will be accompanied by sustained activity on your system (flashing lights on the tower etc) in addition to a virus-warning message. In these cases, power the system off immediately and call IT.

### ***Unknown Computer technicians***

District IT as well as site supervisors should be aware of any computer maintenance going on at any location in the district. If a person wants to service any part of the data system, and you don't know them or weren't expecting them, call IT immediately before allowing them to proceed. Any legitimate computer system technician will have an ID. If they refuse to wait and insist on getting at the computer equipment, call 911.

### ***Power off at night – unless otherwise authorized***

Failure to power off computers at night produces the following effects:

1. Wastes energy.
2. Provides a means for unauthorized people to get to our data system, using your user ID.
3. Increases the likelihood of software errors the longer it stays on.
4. Unless authorized by the Information Technology Director, it is a violation of our Data System Usage Policy.
5. Serves no purpose.

## Service requests

Our data system has grown exponentially over the last few years. As it has grown, the demand for repairs and software fixes has grown accordingly. Blending large behind-the-scene projects with routine IT business presents a growing challenge. District IT is always looking for ways to improve the efficiency and effectiveness of our maintenance functions, which will result in greater satisfaction of system users.

The Office of Information Technology has installed a system to ensure that priorities are handled, and non-priorities don't get lost or forgotten. The system has been operation for some time. Each location and department has been provided with a user ID and password for entering IT requests.

Routine service requests must be submitted using the Ayanova system.

Emergencies can be reported by phone or email, but should be followed up with an entry in the system.



## Report, Database and WEB Development

This section will provide guidance as to how to proceed with development of a database or report to ensure the greatest chance for success.

Many departments, from time to time, will seek to create reports, extract data from an existing database, or create a new database from scratch. While it is the position of the Northwest Georgia Health District, IT Department, that employees should strive to enhance their computer skills, often, experience is the difference between a successful project and a costly, embarrassing failure. Generally speaking, when IT projects fail, it is due to failure to appreciate and allow for all of the factors that will influence the project as it develops and beyond. The best of intentions and lots of hard work can be laid to waste for what may seem to be insignificant or irrelevant at the outset of the project.

The considerations that go into database development are beyond the sight of most general and even advanced system users. Which data engine to use? How should the data fields be designated for size and data type? How can data integrity and security be assured? What are the system-wide implications? What do you eventually want to get out of it? These and many other considerations should be given the utmost attention up front, or they will surely come back to haunt the unwary. This is the realm of data professionals.

Reports from an existing database, on the other hand, contain an entirely different set of risks. Carelessly generated reports can provide very misleading data. The focus here must always be on accuracy based on the data as entered into the system. No report, regardless of how well written can analyze data that has not been captured.

In either case, detail and accuracy up front are the keys. The forms on the next pages should help to get a report or database project off to a good start.

## ***Report Request***

What existing database will this report be drawn from?

Key people:

Name	Phone	email	Location
------	-------	-------	----------

Sponsor: \_\_\_\_\_

Go to person: \_\_\_\_\_

Technical manager: \_\_\_\_\_

Programmer: \_\_\_\_\_

When is it needed?

- Using any method, create a mockup of what is wanted. What do you want the report to look like? What do you want on it?
- All information on the report should have the source identified. What fields in the database will be used for this report?
- All fields on the report that require calculations should have the formula for the field clearly defined. If a field is to have, for example, a list of services for a specified period of time, describe how you would do this if you were doing it manually.
- Use as many sheets as necessary.

## ***Database Development Procedure***

Database development can be quite involved. Many costly projects either duplicate existing datasets, or fail outright due to inadequate preparation. Frequently, the actual outputs needed are obtainable from existing datasets. It is the intention of this document to provide a standard process for all database development projects throughout the district.

Prior to discussing data needs with outside contractors, a clear set of goals and needs should be documented and submitted to the Information Technology Director. Bringing a contractor in prior to discussions with and approval from the Information Technology Director results in a scenario where the IT Director is forced to argue the merits of an outside contractor's proposal with internal personnel. Technical contracts can be very ambiguous, and technical contractors frequently mislead non-technical negotiators. This path will most likely result in an unsatisfactory outcome, as it undermines the integrity of the management team and presents an inconsistent picture of authority. It is the responsibility of the Information Technology Director to deal with external technology contractors in all cases. It is the responsibility of people initiating IT projects to adequately document and present them to the IT Director, not outside contractors.

While it is easy to make a list of data elements one wants to collect, often non-technical people will overlook critical details, or fail to consider the larger picture of the data system, HIPAA considerations and GTA guidelines. Many database projects duplicate data that is already available. When this occurs, duplicate entry is always the result. Reporting will become fragmented and unreliable, as entries are double counted or not counted at all. Every effort should be made to use an existing database prior to initiating development of a new one. In defining a database project, it is therefore critical that the focus be placed on what you want to get out of it, rather than what you want to put into it.

Technology projects managed by non-technical people fail at an extraordinary rate. Projects managed by Northwest Georgia Health District IT succeed at an extraordinary rate. As stewards of the Public Health system and data, we have an obligation to do the best we can.

Gather as much of the information on this form as possible. Submit this form and copies of all supporting documents to the Information Technology Director as a single package. This information will be used to define the project in technical terms, so that a good decision can be made whether to develop it internally or seek an outside contractor.

In no case should an outside contractor be contacted prior to completion of this process. Doing so may eliminate the contractor of choice.

Project Name: \_\_\_\_\_

Please provide as much of this information as possible prior to contacting the Information Technology Director. This information is what is needed to provide the best opportunity for success. Provide documentation.

Key people:

Name	Phone	email	Location
------	-------	-------	----------

Sponsoring manager: \_\_\_\_\_

Go to person: \_\_\_\_\_

Technical manager: \_\_\_\_\_

Programmer: \_\_\_\_\_

1. Attach all documentation on this project. Include notes, samples, mock-ups etc.
2. Does the funding source have any requirements for reporting, timelines, security, database type, hardware or operating system? Provide supporting documentation for each.
3. Where will it be deployed, and how many users at each site? Health Departments, schools, Environmental sites, DFACS? Will it require multiple simultaneous users?
4. What are the expected outputs? Ensure detailed mockups or originals of input screens, desired reports, certificates etc are attached.
5. What specific data elements need to be captured to make these outputs possible?
6. Determine which input fields can be validated, and what are the acceptable values. List all. Gender, Race, DOB, CPT codes, ICD9 codes etc.
7. Is this database to be merged with other any other existing Public Health databases, and do we already collect some or all of this data?

## ***Web Development***

Web developers, like any technical people, vary widely in both skill and sincerity. It is not the concern of a contractor to determine if a project will or will not work in an existing data system, if the project is feasible, or even if it is a good concept. Contractors complete work based on a description of what they are to do by the individual they are negotiating with.

That in mind, it again behooves this organization to use internal resources for web development where possible, and use the Information Technology Director to negotiate contracts with experienced professional developers when external talent is required.

Web development projects, like any technology project, require significant knowledge and skill to ensure success within budget. Web contractors can use a variety of techniques to get contracts that strongly favor them. An example is a contract that provides for X number of hours at a specified rate per hour. This only obligates the contractor to work on, but not complete a project. Typically, when the funds run out, the contractor must be paid additional money to finish it, as he has completed his obligation under the time and material contract. These seldom include any reference to what constitutes a finished product, and are generally unsuccessful as a result. The customer then has to provide additional funding to the contractor to get the job completed.

As with any technical project, the first step is to document clearly and completely what the project will look like, what it will do and how it will do it, as well as any other considerations prior to involving outside contractors. In short, define the finished product before hiring someone to make it.

All web projects should be well documented by the requestor, and approved by the Information Technology Director prior to contacting external contractors. The Information Technology Director should select contractors based on their demonstrated ability to complete the project.

Describe the project and available resources in detail: