COUNTY OF MONMOUTH

NEW EMPLOYEE ORIENTATION

HIPPA / HITECH PRIVACY & SECURITY AND COMPUTER TECHNOLOGY MANUAL

08-2019

Table of Contents

The Purpose of This Manual

The purpose of this manual is to ensure that each employee of Monmouth County (hereinafter referred to as "County") is aware of his or her responsibilities with respect to information privacy and information security. This manual will discuss HIPAA, the HITECH Act of 2009, and computer related issues and tasks. As an employee of the County, you have been trusted with the County's confidential information. With this trust comes the responsibility and obligation to ensure that the information and computing facilities are used only for their intended business purposes as they are the exclusive property of the County.

The County handles sensitive and confidential information on a daily basis. This responsibility is great. This manual will explain what you need to know to be an active participant in the County's information privacy and security program.

Objectives

This manual implements the following objectives:

1. Introduce you to information privacy and security concepts.
2. Provide guidelines on how you can implement information security measures.
3. Provide education and guidelines to comply with current HIPAA / HITECH rules and regulations.
4. Emphasize the importance of employee awareness in protecting information.
5. Provide you with information about computer technology.
6. Make people aware of their responsibilities.

Employee Expectations

The expectations set forth in this manual regard all individuals working for the County. The guidelines make all employees accountable for actions relevant to technology. All employees should:

1. Communicate properly with the appropriate Help Desk in order to obtain computer assistance. ITS Help Desk number is 732-431-7039
2. Ensure the protection of proprietary, confidential, privileged, or otherwise sensitive data that may be processed in any manner by the County and/or any agent for the County.
3. Do not share your confidential county Password with anyone.
4. Maintain security and access of networked data by utilizing the password protection feature of the Windows operating system.
5. Secure email from unauthorized access.
6. Protect the confidentiality and integrity of the files and programs from unauthorized users.
7. Implement professional procedures when using email and sending information.
8. Understand with clarity that all files, email, hardware, software, computer network access and usage are considered public record.
9. Report any unusual activity to the appropriate Help Desk, as a preventive security measure.

Statement of Consequences

Noncompliance with the County policies may constitute a legal risk to the County, an organizational risk to the County in terms of potential harm to employees or citizen security, or a security risk to the County's network operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the County network could lead to liability on the part of the County as well as the individuals responsible for obtaining it. You are accountable for all your computer related activity, and therefore, you are subject to any disciplinary action from the County should you intentionally violate any of the policies and procedures contained in this manual.

HI PAA Frequently Asked Questions

What does the word "HIPAA" stand for?

"HIPAA" stands for the "Health Insurance P01iability and Accountability Act". It's the LAW!

What is HIPAA all about?

The Health Insurance P01iability and Accountability Act of 1996 (HIPAA) is a multifaceted piece of legislation covering three areas:

1. Insurance portability.
2. Fraud enforcement (accountability).
3. Administrative simplification (reduction in health care costs).

Under HIPAA Administrative Simplification, rules have been established requiring a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy and security of protected health information (PHI).

The United States Department of Health and Human Services (HHS) does not prescribe the particular measures that covered entities must take to meet this standard. The HHS commentary states that the nature of the required policies and procedures will vary with the size of the covered entity and the type of activities that the covered entity undertakes. The regulations apply to both electronic and paper information.

What is HIPAA Administrative Simplification?

HIPAA administrative simplification helps to attain uniformity and simplification in health care transactions and will:

1. Reduce costs of administrative overhead.
2. Establish Unique Provider Identifiers.
3. Establish National Uniform Identifiers.
4. Simplify communications between payers/providers.
5. Establish protections for the privacy and security of individual health information.

Who is covered by HIPAA?

1. Health providers who submit/receive electronic transactions (e.g. eligibility, claims, and payments).
2. Health plans and clearinghouses are "covered entities" and must comply with the HIPAA regulation.
3. Any entity that uses or discloses health data on behalf of a "covered entity" will sign a "business associate" agreement which will require them to comply with the HIPAA regulation.

What is protected by HIPAA?

HTPAA protects an individual's identifiable health information. Here is a list of information identifiers:

1. Names.
2. Addresses.
3. Employers.
4. Relatives' names.
5. Dates of birth.
6. Telephone and fax numbers.
7. Email addresses.
8. Social Security numbers.
9. Medical record numbers.
10. Member or account numbers.
11. Certificate numbers.
12. Voiceprints.
13. Fingerprints.
14. Photos.
15. Codes.
16. Any other characteristics which may identify the individual (e.g. occupation).

What lead to the passage of the HIPAA law?

Reactions to following sorts of abuses, as well as a general concern about health privacy, led to the passage of HIPAA. Here are a number of examples:

1. Long Island, NY - Emergency Department workforce members copied medical record charts of accident victims and provided the copies to lawyers, acupuncturists, chiropractors, etc. They were paid up to $5000 per delivery.

2. New York City, NY - A Congresswoman was up for re-election to office. The night before the election, a NYC newspaper published a story stating that she was receiving treatment in a Behavioural Health Clinic. She lost the election.

3. Jacksonville, FL - A woman brought her teenage (age 13) daughter to work at the hospital, and left her unattended at a logged in computer. The girl looked up patient phone numbers, and phoned to tell them that they'd tested positive for HIV. One patient attempted suicide.

4. Rapid City, ID - A medical student took home copies of patients' psychiatric records to work on a research project. When finished, he disposed of the material in the dumpster of a fast food restaurant (where they were found and given to a newspaper reporter).

5. Miami, FL - Several hundred hospital workers browsed through the records of a famous patient that had recently come to the facility, even though few of them were actually involved in the case.

6. Minneapolis, MN - A university health facility sent emails to transplant recipients that revealed the names of hundreds of donors to whom confidentiality had been promised.

7. Tampa, FL - A county health department worker copied lists of HIV patients, distributed the information to his friends and sent the information to a local newspaper.

8. Missoula, MT - A hospital posted the psychiatric records of dozens of children on its public web site, where they remained for weeks until discovered by a newspaper reporter.

What is Information Privacy?

Privacy refers to the *disclosure* of information about an individual while security refers to the *protection* of information, facilities, or other assets. Often people think of privacy and security in the same context, that is, if you secure the information you are also protecting its privacy. But it is important to understand that simply disclosing information to a person who is not authorized to receive it is a violation of State and Federal law as well as the County policy and may lead to adverse action.

Information comes in many forms:

1. Computer screen displays.
2. Computer printouts.
3. Word processing documents.
4. Spreadsheets.
5. Graphics and drawings.
6. Presentations.
7. Letters, memos and rep01is.
8. Email and schedules.
9. Internet and Intranet.
10. Personal computer hard disks and records.
11. Diskettes and CDs.
12. Microfilm and microfiche.
13. Fax documents.
14. Conversations both on and off the phone.
15. Voice mail messages.

What is Information Security?

Information security refers to the controls that protect information assets from unauthorized access, destruction modification and disclosure. It is a part of your job whenever you work with information to ensure that information is secure. Examples of sensitive or co nfidential information are personnel files, client records, addresses and home telephone numbers of the County personnel.

Here are a few things you can do to keep information more secure:

1. Back up information or store documents on your file server to insure against loss.
2. Lock up diskettes, tapes, or other media when leaving the area.
3. Lock doors where appropriate.
4. Lock file cabinets that contain sensitive or confidential information.
5. HIPAA legislation requires that all unattended workstations be logged off.
6. Make sure that your computer has current virus protection activated.
7. Keep diskettes and other computer data storage devices away from magnets, computer tops and other somces ofelectrical energy.

Isn't HIPAA more than just privacy and security of data?

Yes! HIPAA is more than just privacy and security of data:

1. Title I of HIPAA deals with health care access, health care p01iability, and health care renewability. The intention is to protect health insurance coverage for workers and their families when they change orlose their jobs.
2. Title II of the law, also known as "Administrative Simplification", deals with preventing health care fraud and abuse.
3. "Administrative Simplification" requires the United States Department of Health and Human Services (HHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients.

HIPAA is designed to improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for specified administrative and financial transactions; and to protect the security and confidentiality of electronic health information.

What is Protected Health Information (also known as "PHI")?

Protected health information (PHI) is individually identifiable information that is:

1. Transmitted by electronic media.
2. Maintained in any electronic media.
3. Transmitted or maintained in any other form (including oral or wTitten PHI).

What are the differences between privacy, confidentiality, and security?

1. Privacy is the individual's *right* to keep certain information to him or herself, with the understanding that the information will only be used or disclosed with his or her perm1ss1on.

2. Confidentiality is the *practice* of permitting only certain authorized individuals to access information, with the understanding that they will disclose it only to other authorized individuals.
3. Security is a safeguard to protect confidentiality.

Why are privacy and confidentiality important?

Individuals' expectations of privacy and confidentiality are central to any provider facility (e.g. hospital, physician practice, lab, nursing home, pharmacy, service provider, etc.) that has access to individually identifiable information (also known as protected health information (PHI)). Under HIPAA, the hope is that educated individuals will be able to trust their providers and the facilities in which they work. To build trust, HTPAA calls on covered entities to learn the rules for privacy and confidentiality and then live by them.

Privacy and Confidentiality refer to an individual's right to control access and disclosure of his / her protected, identifiable health information. Under HIPAA, this means that information provided by the individual to health care providers and notes and observations about the individual's health will not be used for purposes other than treatment, payment, or health care operations. These principles allow individuals to feel comfortable sharing information with their providers. Privacy and confidentiality are essential to good individual care.

Haven't privacy and confidentiality always been required?

Health care facilities have always upheld strict privacy and confidentiality policies. Unless you're new to health care, this idea will be familiar to you. But there are changes. The United States government has begun to strengthen the laws protecting privacy and confidentiality in response to what's been happening with private medical information getting into the wrong hands. As cases of health information being misused increase, Congress has taken action to make health care providers do more to protect health information privacy and confidentiality. With the enactment of the Health Insurance Portability and Accountability Act of 1996, (HIPAA), the idea that individuals have the right to privacy and confidentiality became more than just an ethical obligation of physicians and health care facilities. It became the law.

What are the top 5 privacy questions and answers?

Here are the most common questions we are asked about HIPAA Privacy:

Q. How do I know when information is considered private?
A. Did you learn it through your job? If yes, then it is considered private.

Q. How do I handle an individual asking for access to their record?
A. Individuals have a right of access. Route requests to your manager / supervisor.

Q. How do I handle an individual's request to change their medical record?
A. Individuals have the right to amend or correct their record. Requests will be investigated. Route requests to your manager.

Q. How do I handle a family member or close friend asking about a patient?
A. You can provide them with directory information, including their name, location, and condition in general terms.

Q. How do I handle another member of the workforce inquiring into a patient's condition or treatment?
A. Determine if it is necessary to their position and if it is related to treatment.

What are examples of prudent privacy practices?

Prudent privacy practices are day to day activities that you can take to prevent unauthorized access to protected health information (PHI). In addition, employees who work in the County Care Centers should abide by their facilities' Notice of Privacy Practices. You can ask your supervisor for a copy.

Examples of prudent privacy practices:

1. Shred or destroy all hardcopy PHI when it is no longer needed.
2. Fax machines, printers and copiers should be located in secured locations, away from public access.
3. Avoid talking about patients and/or clients in public areas.
4. Keep PHI away from public view / access.
5. Secure PHI in all locations.
6. Manage passwords.
7. Angle computer screens away from public view.
8. Remember individuals' right to privacy during treatments.

Why should I be concerned about information security?

The information that you routinely use may require protection. Whether you work with paper records, on a computer, or spend most of your day on the phone, you are an integral part of the County's information security program. Information security is not an option or choice; it is a legal requirement. Information security is embedded in the law and is found in regulatory requirements. It is your responsibility to adequately protect the County's information from misuse, alteration, or destruction. We have an obligation to provide services to county residents, to protect our employees and those under our care. It is essential that every single employee be a part of the information security program.

What are the general requirements for securing Protected Health Information (PHI)?

The HIPAA Security Rule requires the County to secure electronic protected health information (ePHI) that the County creates, receives, maintains and/ or transmits. To generally comply with HIPAA Security, the County must:

1. Ensure confidentiality of PHI. Only authorized people should view protected health information.
2. Ensure integrity of PHI (the information is what it is supposed to be - it hasn't been changed).

3. Ensure availability of PHI (the right people can see it when needed).
4. Protect against reasonably anticipated threats or hazards to the security or integrity of information.
5. Protect against reasonably anticipated uses and disclosures not permitted by privacy rules.
6. Ensure compliance by workforce.

What are threats to PHI?

Protected health information (PHI) can be exposed to threats via unauthorized or inappropriate:

1. Access - An example is a hacker gaining access to ePHI.
2. Possession - An example is a stolen laptop containing ePHI.
3. Disclosure - An example is when a workforce member discloses PHI to someone who is not authorized to know.
4. Modification - An example is when someone changes ePHI in an unauthorized manner.
5. Destruction ... both accidental and intentional - An example is a flood in the data center.

What are the sources of threats to PHI?

Threats to PHI can be from internal, environmental and external sources, including:

1. Employees and Volunteers.
    a. Unintentional - acting in good faith.
    b. Intentional - disgruntled or unhappy staff.
2. Environment.
    a. Equipment failure.
    b. Fire, flood, hurricane, vandalism.
    c. Software errors.
3. Outsiders.
    a. Ex-employees.
    b. Hackers, "social engineers".
    c. Visitors.

The HIPAA Security Rule is not black and white - what does that mean?

The HIPAA Security rule applies to many different kinds of organizations. Organizations can differ in size, complexity, available resources, etc. Because organizations are not all alike, the HIPAA Security rule is not black and white; there is no standard list of what each organization has to do to comply with HIPAA. Each organization must do a "risk analysis" and make business decisions as to what is "reasonable" to do to reduce their risk to the security of ePHI. Therefore, HIPAA Security is:

1. *Scalable and Flexible* - Can take into account:
    a. Size.
    b. Complexity.
    c. Capabilities.
    d. Technical infrastructure.
    e. Cost of procedures to comply.

f. Potential security risks.

2. *Technologically Neutral* - Explains what needs to be done, not how.
3. *Comprehensive* - Not just technical aspects, but behavioral as well.
4. *Addressable* - If an implementation specification is addressable, a covered entity can:
    a. Implement a solution, if reasonable and appropriate to reduce risk of security vulnerability.
    b. Not implement it if there is a low likelihood for risk of security vulnerability.

What are the HIPAA Security Standards?

HIPAA has organized the security requirements into 3 standards. They are administrative, physical and technical. The next three questions cover the three HIPAA security standards.

What are the Administrative Security Standards?

The administrative aspect of the security standards incorporates the following:

1. Security Management:
    a. Risk analysis - need to determine the likelihood and impact of each threat?
    b. Risk management - need to determine what can be done to reduce the likelihood and / or the impact.
2. Assigned Responsibility (an organization must have an "Information Security Officer" (TSO)).
3. Workforce Security:
    a. Termination procedures - need to eliminate access to systems and facilities as of the date of separation.
    b. Clearance procedures - An example is the need to background checks before hiring new employees.
4. Information Access Management - need to manage access to ePHI.
5. Isolating Clearinghouse - not applicable.
6. Access Authorization - need to have a process to authorize access to ePHI.
7. Security Awareness and Training - need to train the workforce on your HIPAA Security policies and procedures.
8. Security Incident Procedures - need to quickly respond to security incidents.
9. Contingency Planning - need to have a plan of action to respond to a disaster such as a flood in the data center.
10. Evaluation - need to review and update HIPAA Security policies and processes on a periodic basis.
11. Business Associate Contracts - need to have agreements with third parties who gain access to your protected health information (PHI).

What are the Physical Security Standards?

The building you work in may require safeguards to protect data and information. The following controls may be required:

1. Facility Access Controls - need to control access to buildings and sections of buildings where PHI exists.

    a. Contingency operations - need to control access to facilities during an emergency / disaster.
2. Facility Security Plan.
    a. Access control - same as above.
    b. Maintenance records - need to keep records of changes to buildings in order to determine the impact to the security of PHI.
3. Workstation Use - An example is the need to position workstation monitors away from public view.
4. Workstation Security - An example is the need to keep laptops in a secured location when not in use.
5. Device and Media Controls - An example is the need to protect information that is stored on pen drives and CD's.

What are the Technical Security Standards?

Computer databases may contain PHI (protected health information). The following technical security controls can reduce the risk of unauthorized access.

1. Database Access Control:
    a. Unique User name - each user must be uniquely identified.
    b. Emergency Access - need to determine who can have access to ePHI during an emergency.
    c. Automatic Logoff - software applications should have an automatic logoff when not in use.
    d. Encryption and Decryption - An example is the need to encrypt information stored on a laptop in order to protect it in the event it is stolen.
2. Audit Controls - need to be able to audit who accessed ePHI.
3. Data Integrity - need to protect the integrity of ePHI from unauthorized change or from threats that could damage it.
4. Person or Entity Authentication - As an example, each user must have a unique password in order to access a system that contains ePHI.
5. Transmission Security - need to protect ePHI that is transmitted to an open network such as the internet.

Isn't security inconvenient?

Some people believe that secmity results in umeasonable controls and that these controls are inconvenient, ineffective, and counterproductive. The reality is that controls and security standards are designed to protect all of us. Appropriate controls and cost-effective safeguards make sure that each person is accountable for his or her actions. Controls protect the honest employee from unwarranted accusations or suspicion.

Without accountability, we could all be equally suspect if and when something destructive occurs. Errors or omissions most often cause inaccuracies, lost, or damaged information. With security in place, controls often make it possible to avoid mistakes and omissions, and when they do occur, to identify potential problem areas and limit the extent of damage that mistakes can cause. Security is in place to protect you as well as the information and information systems with which you work.

What could really happen?

Even if you aren't responsible for confidential data, information is an asset that must be properly managed and protected. The loss of information can cost time, money and even lives. Incorrect information can lead to all kinds of serious trouble. Here are a few of the things that could happen as a result of poor information security:

1. *Loss or Destruction ql lnjc)rmation.* It can be difficult, time consuming, and costly to re-create data. In some cases, lost information is impossible to recreate.
2. *Unauthorized Access to lf?formation.* The County's information systems have not only client data, but personal information about employees, such as addresses, telephone numbers and identification numbers.
3. *inaccuracies in if?formation.* The vast majority of information maintained by the County is generated by various County agencies and must be accurate for the County system to function properly. Inaccuracies in information are a serious matter. Inaccuracies can cause delays in legal proceedings, mishandling of information, inappropriate legal actions, mishandling of monies, or other actions that have an adverse effect on the County.

How can I protect information in my work area?

We tend to become lax about protecting the information in our work area because we have authorized access to it. We become desensitized to the importance of the information we work with because we see it all the time. It is essential that we be alert to the sensitivity of information and aware of those who may want it. It is your responsibility to prevent unauthorized access to the County's information assets by visitors, service personnel, employees, or anyone else to whom access has not been granted.

There are additional ways that information can be accessed. Please be aware of the following:

1. Never share your User names or passwords with anyone other than your supervisor or authorized Monmouth County Information Services (MCITS) personnel.
2. Clear your desk at the end of the day.
3. Dispose of confidential and sensitive documents properly; do not just throw it in the garbage. (If you are not sure of the proper method to shred confidential and sensitive documents, please ask your supervisor.)
4. Never discuss confidential information in public areas or with individuals who do not have a need to lmow.
5. Log-off your computer when you leave.
6. Report unesc011ed unauthorized people to your supervisor.
7. Do things to protect information, such as:
    a. Back up your data regularly to diskette or store your data on your file server.
    b. Lock up sensitive documents and diskettes.
    c. Protect diskettes and CDs by storing them in a safe and secure environment.
    d. Keep diskettes away from magnetic fields (e.g. telephones, workstations, radios, microwaves, coffeepots, etc.).
    e. Avoid using diskettes and CDs as coasters if you ever want to retrieve data from them in the future.
    f. Label all diskettes, confidential and sensitive documents appropriately.

g. Keep food and liquids away from workstations, printers, documents, diskettes and CDs.
h. Contact MCITS if your anti-virus software is not up to date.
1. lfyou useemail and/or the Internet at work, be careful about opening attachments and downloading information.

Privacy of information is very important. Use caution when disclosing information m the presence of any individual currently not working in your unit.

How should I handle questions regarding client information?

Depending on your job, you may come into contact with a number of non-County people, for example consultants and contractors or County employees who are not authorized to receive the information for which they are asking. How you handle requests for information depends largely upon who asks the questions. Here are some suggestions:

1. Verify the identity of the individual asking the questions.
2. Refer any requests from the news media (rep011ers) to your department head.
3. Do not respond to surveys or questionnaires which are not County issued or authorized.
4. Requests for employee information such as lists with home addresses or phone numbers should be referred to your supervisor.
5. Remember to follow the County's policy on requests for information made under the Open Public Records Act.

What about phone calls (including IP phones and County issued cell phones)?

When providing information over the phone, it is important to establish the identity of the caller, whether that person has a need to know, and if the caller is authorized to receive the requested information. If you have any doubts as to the identity of the individual or his/her right to have the requested information, talk to your supervisor. Do not give information to a person who is not authorized to receive it. Do not provide unnecessary information. Here are some general points to keep in mind:

1. Verify the identity of the caller. If in doubt, say that you will have to call them back, and then verify the authenticity with your supervisor.
2. Verify their need to know with your supervisor.
3. Verify that they are authorized to receive the information.
4. Do not provide unnecessary information, for example, opinions or speculation.
5. Be aware of who is in the area that could overhear the conversation.
6. Do not divulge departmental employee information such as lists with home addresses or phone numbers.
7. If you receive a request for this type of information, take the name and telephone number of the individual and notify your supervisor.
8. Never give out a password over the telephone unless requested by a known MCITS technician or your supervisor.
9. Do not forward your telephone to a number with which you are unfamiliar.
10. Do not mention names of other employees or use County terminology unless you are sure of the identity of the caller and their need to know.

11. Do not send documents, plans, schedules, or any other document unless you are sure that the recipient is authorized to receive them.
12. Talk to your supervisor if you have any doubts about the caller.

How should I dispose of sensitive or confidential information?

Confidential and sensitive information are defined as information maintained by County agencies that is exempt from disclosure under the provisions of the New Jersey Public Records Act (Government Code) or other applicable state or federal laws; and sensitive information is information maintained by County agencies that requires special precautions to protect it from unauthorized modification or deletion. Some suggested methods for disposing of confidential and sensitive material. *Check with your manager or supervisor to co71:fzrm which process to use:*

1. Use a paper shredder.
2. Dispose of diskettes by taking the magnetic media out of the protective plastic case and cutting it in half.
3. Reformat diskettes prior to giving them to another person. Do not use the quick format option. If the diskette was used to store confidential information, rewrite the entire content of the diskette before reformatting, or destroy it. *Again, check ·with your manager or supervisorto confirm which process to use.*

Are cell phones safe?

Cell phones are not at all like the phones we use in our offices. "Land line' phones, such as those in our office, are in a controlled environment - our offices and cubicles. Cell phones can be used anywhere and everywhere, including public places. We use them in grocery stores, airports, parks and while shopping. We feel that we must answer the phone, regardless of where we are and who may be nearby, even if it is a stranger. Our cell phone conversations are much more public than the same conversation conducted using the office phone.

The older cell phones use "analog" technology, and communications with such devices is conducted much like that used with two-way radios. Anybody can listen in on these conversations if they have a radio tuned to the same frequency your phone is using. Newer phones use "digital" technology, and they allow more privacy. The signal is converted to digital format while it is in transit from one phone to another, and those who want to listen in must have special equipment to do so. Even so, your side of the conversation is audible to anybody within earshot. Here are a few suggestions for how you could improve the privacy, safety and security of using cell phones:

1. Be mindful of where you are and who is within earshot when using your cell phone. Move to a less-public place if appropriate.
2. Do not provide or discuss sensitive or confidential information on a cell phone.
3. Use care when driving. Remember, safety always comes first. Be mindful of local municipal and state laws. For example, it is illegal in the state of New Jersey to use a hand held cell phone while driving.
4. Be courteous to those around you. Turn the ringer off on your phone when in "quiet" places such as restaurants, churches, theatres, meetings and training sessions.
5. If you must talk on your phone in such places, step outside first.

Should I be concerned about phone fraud?

Telephone or toll fraud is one of the fastest growing information security issues today with over $4 billion in loss per year. Losses due to unauthorized access to telephones nationwide exceed $100 million a year. Phone card theft and the transferring of phone numbers or calls are common methods of phone fraud. A popular voice mail scam is to change an outgoing voice mail message to say "Yes operator, I will take that call," or "I will accept those charges". Be aware of anyone near you when using a phone card. Your phone card number and pin can be stolen by somebody looking over your shoulder as you dial. Lastly, it is extremely important that you protect your voice mail password and privileges. Here are some tips to help you protect the County's voice mail system:

1. Voice mail passwords should be a minimum of three characters in length.
2. Do not use your phone number in your voice mail password.
3. Do not use repeated or consecutive numbers in your voice mail password.
4. Follow the password tips provided in "How can I protect my password?" in this manual.
5. Do not give your password to anyone.
6. Remember, telephone service personnel do not need your password to maintain your system.
7. When using a phone card, shield the keypad to dissuade those who would steal your card number (sometimes this is referred to as "shoulder surfing").

How can my system access be protected when I'm using a workstation?

Use these simple precautions:

1. Log-off when you leave your immediate work area.
2. You could also lock the screen by hitting CTRL ALT DEL keys and select LOCK COMPUTER.
3. Do not leave an unattended session.
4. If the workstation has a mechanical lock, use it when you are away from the workstation, and protect the key from use by others.
5. If you see an unattended workstation or somebody in your work area that you do not know using a workstation, notify your supervisor.
6. If sensitive information is displayed on the screen, be sure that no one else can see it.

Protect your password! Do not share it with anyone else except known County Information Services technician(s) or your Supervisor. If someone else can successfully log on to the system with your User name and password combination, all activity will be attributed to your User name, in other words, *You.*

What must I do when I use my computer when away from the office?

Workstations may be stolen or damaged when they are removed from the office. If you take your computer home or your job requires that you travel, remember these important points:

1. Obtain approval from your manager or supervisor to use County owned equipment away from the office.
2. The computer should be password protected and your password safeguarded!

3. Use care in handling the equipment.
4. Do not leave equipment visible in your parked car.
5. Do not leave equipment in your car overnight - take it with you!
6. In public facilities, do not leave equipment unattended, even if "just for a moment."
7. Put away reports and other papers that you are not using.
8. Make backup copies of your information and leave them at the office. Protect the information from disclosure, damage, or destruction.
9. Protect sensitive/confidential information from casual observation by others.
10. Properly discard unneeded reports and other papers that contain sensitive or confidential information at the office, not in the trash can.

Can I bring my home computer to the office?

It is not recommended since the County does not assume liability for personal property brought to the job site.

Can I make copies of County-owned software to use on my home computer?

Unless the software license specifically allows its use on multiple systems and Information Services has approved it, you cannot make copies of County owned software. Some software companies allow the user to make one copy for use at home. The intent being that when one copy is being used-the other isn't. Misuse of the County owned software can expose you and the County to potential lawsuits for violation of U.S. Copyright law. When the County buys proprietary software, it purchases a license to use it on a specified number of workstations. Making and using copies not authorized under the license agreement is a violation of copyright law.

Can I make a copy of software that I wrote?

County policy prohibits employees from "using County time, facilities, equipment, or supplies for personal gain or advantage." Any software developed on County time, using County equipment, facilities, or supplies, is subject to a claim of County ownership.

What steps can I take to reduce the exposure to a computer virus?

There are simple steps you can take to avoid the frustration, cost, and loss of work caused by computer viruses:

1. Store your files on your file server or back up to disks, CDs or memory key which are securely stored.
2. Restrict use to authorized people, reputable software, and verified clean (e.g., virus-scanned) diskettes or CDs.
3. Use only software purchased through MCITS.
4. "Shareware" and "freeware" are prime entry point for system viruses. *Do not* use or install these types of software without prior permission from MCITS.
5. Exercise caution when receiving and / or using demonstration diskettes because they are major sources of computer viruses.
6. When downloading a file, download it onto a diskette first.

What if I see or bear information I do not need?

There will be occasions when you will have access to confidential information that you do not need for yow- work. For example, if an individual is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. This is confidential information about an individual; do not communicate it to anyone else.

You may also see individual information on marker boards throughout the facility. These are usually posted where the public cannot see them. In the course of providing individual care, you may work in areas where they are visible. You must keep this information confidential. Do not use it in any way, and do not disclose it to anyone, including coworkers, other individuals, or anyone else who may ask.

ln the comse of doing your job, you may also find that individuals speak to you about their condition. While there's nothing wrong with this, you must remember that they trust you to keep what they tell you confidential. Do not pass it on.

It's important that individuals understand how they can protect their own health information, and how their providers protect their information. Because of this, the HIPAA rule also requires health care providers to post notices telling individuals how their information will usually be used. This Notice of Privacy Practices tells individuals about the provider's privacy policies and practices, how the provider will use their information, and tells them that they have the right to access their own records and request additions or amendments to them. You will also see these information notices posted in places where individuals can see them. If individuals have questions about how the facility uses information, they can be directed to these posted notices, or tothe facility's privacy officer for more questions.

HIPPA requires providers to make a "good faith effort" m obtaining individuals' written acknowledgement that they received a copy of this notice.

What happens if a HIPAA policy is violated?

Breaking HIPAA's privacy or security rules can mean either a civil or criminal sanction. Civil penalties are usually fines. These are the result or "inadvertent violations," not necessarily resulting in personal gain. These penalties can result in fines of up to $100 for each violation of a requirement. For instance, if the health facility released 100 individual records, it could be fined $100 for each record, for a total of $10,000. $25,000 is the annual limit for violating each identical requirement.

Have you ever looked up a neighbor's medical history out of curiosity? Under HIPAA this could subject your facility to a civil sanction and a fine. In some specific cases, even "inadvertent violations" can result in criminal sanctions.

Criminal penalties for "wrongful disclosure" can include not only large fines, but also jail time. The criminal penalties increase as the seriousness of the offense increases. ln other words, selling individual information is more serious than accidentally letting it be released, and can result in more serious penalties. These penalties can be as high as fines of $250,000, or prison sentences of up to 10 years. Examples of wrongful disclosure:

1. Knowingly releasing individual information can result in a one-year jail sentence and $50,000 fine.
2. Gaining access to health information under false pretenses can result in a five-year jail sentence and a $100,000 fine.
3. Releasing individual information with harmful intent or selling the information can lead to a 10-year jail sentence and a $250,000 fine.

For instance, criminal penalties for "egregious violations" could result from the sale of a celebrity's medical record information to a tabloid newspaper or the sale of health information to marketing or pharmaceutical companies for personal profit. Your facility is committed to protecting individual privacy and confidentiality. When you fail to protect individual information and individual records by not following your facility's privacy policy, it can have an impact on your ability to do your job, on your status with your facility, and even on your license to practice. You should carefully review your facility's privacy policy to be clear about its requirements

Can the County workforce receive sanctions for violating HIPAA policy?

All violations of HIPAA Policies or Procedures are subject to disciplinary action. The specific disciplinary action that will be taken depends upon the nature of the violation and impact of the violation on Monmouth Counties Information assets and related facilities. Such disciplinary action may include dismissal and / or criminal prosecution depending on the severity of the infraction.

Summary of the County HIPAA Privacy Policies and Procedures

This section provides you with outlined information about the County HIPAA Privacy policies and procedures. These policies are managed by the County Privacy Officer (the phone number for the County Privacy Officer is on page 50 - "County Resources"). You can ask your supervisor for a copy of one or more of the County HIPAA privacy policies at any time.

HIPAA authorization requirements

In some cases the County must obtain a patient authorization for the use and disclosure of their health information. The requirements for authorization include:

1. Authorization is required for the use and disclosure of health information for business-related purposes.
2. Authorization must be in writing- the Patient voluntarily agrees to let you use the information only for a particular request or need.
3. Authorization is required to disclose psychotherapy notes.

Minimum Necessary Standard

Reasonable effort must be made to disclose or use only the minimum necessary amount of protected health information (PHI) in order to do the job.

Rights of the Individual regarding HIPAA disclosure

Individuals are guaranteed specific rights under HIPAA, including:

1. Where practical, receiving a "Notice of Privacy Practices" outlining how one's health information may be used or disclosed.
2. Obtaining a copy of one's full health record.
3. Correcting - or at least noting disagreement - if the health record appears to be in error.
4. Knowing the persons and facilities to whom one's health information has been disclosed.
5. Asking for extra protection of confidential communications of sensitive data.
6. Assurance that the facility follows appropriate privacy and security practices.
7. Complaining to the covered entity's Privacy and Security Officers - or directly to DHHS Office of Civil Rights - if one believes HIPAA rights have been violated.

The County's responsibilities

Here is the list of the County responsibilities in order to comply with HIPAA Privacy:

1. Give each patient, where practical, the HIPAA notice that outlines their privacy rights.
2. Post the HIPAA notice in the facility and make copies available.
3. The HIPAA notice must describe planned uses and disclos ures, including the "basic" ones for treatment, payment and health care operations.
4. Written acknowledgment of HIPAA notice must be obtained, where practical.
5. Provide an opportunity for individuals to discuss any privacy concerns.
6. Inform patients about their rights, including what to do if they feel their rights have been violated.
7. Implement a process to handle problems and complaints.
8. Get authorization for certain additional kinds of uses and disclosures, beyond those for treatment, payment or basic health care operations.
9. Develop reasonable HIPAA privacy and security policies.
10. Provide HIPAA policy training to all members of the workforce according to their job responsibilities.
11. Get assurances from any business associates that handle PHI on the covered entity's behalf.

Obligations of all health care providers

Here is the list of obligations of all Health Care Providers:

1. Use or disclose protected health information (PHI) for treatment, payment and operations, or otherwise when authorized bythe patient.
2. The County workforce must limit use and disclosure of PHI to the "minimum necessary" according to their job responsibility.
3. Exercise reasonable caution to protect all PHI under their control.
4. Understand and follow the facility's privacy and security policies.
5. Attempt to remedy any privacy problems - or report them to the Privacy Officer or DHHS Office of Civil Rights.
6. HIPAA prohibits covered entities from retaliating or discriminating against staff who file a complaint.

Disclosure of Protected Health Information

Disclosure is defined as the release, transfer, access, or divulging of PHI to an outside person or entity. Disclosures can occur without patient permission for the following reasons:

1. Public health (rep011ing of diseases and conditions).
2. Reporting child abuse, neglect, domestic violence.
3. Law enforcement investigations.
4. Judicial or administrative proceedings.
5. Averting a serious, immediate threat to public safety.
6. National security purposes.

Psychotherapy notes and privacy

Not all protected health information (PHI) 1s treated the same under the pnvacy rule. Psychotherapy notes have much stronger protections. Personal notes of the treating psychotherapist can be damaging if they fall into the wrong hands; they're also of little or no use to those absent from therapy sessions.

Under HIPAA, the general category of treatment, payment, and health care operations isn't adequate for psychotherapy notes. Instead, the law requires authorization from the individual in order for these notes to be shared, even for treatment purposes.

The HIPAA final privacy rule defines psychotherapy notes as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session staii and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

The Minimum Necessary Standard of information disclosure

Providers must make a reasonable eff011 to disclose or use only the minimum necessary amount of protected health information (PHI) in order to do their jobs. However, they can disclose information requested by other health care providers if the information is vital for treatment. Consider the following questions when determining minimum necessai·y information that can be disclosed or withheld:

1. How much information are you planning to use or disclose?
2. By using the information, will the number of people who are likely to have access to that information increase?
3. How important is it that I use/disclose this information?
4. What's the likelihood that further uses or disclosures could occur?
5. Where information is being disclosed (location), and in what form (email, conversation, fax)?
6. Making minimum necessary determinations is a balancing act. Providers must weigh the need to protect individuals' privacy against their reasonable ability to limit the information that is disclosed, and deliver quality care.

7. There is no minimum necessary requirement when it comes to treatment.

Maintaining records

When individual information 1s m your possession, you are responsible for keeping it safeguarded. Do not leave it in an unattended area. This includes public buildings, provider locations, and areas with heavy pedestrian traffic.

When you are finished using paper individual information, return it to its appropriate location, e.g., the medical records department or to a file at a nursing station. When you are done accessing electronic information, log off the system. Do not leave the information visible on an unattended computer monitor. Protect your password! Do not share it with anyone else except known County Information Services technician(s) or your supervisor. If someone else can successfully log on to the system with your User name and password combination, all activity will be attributed to your User name, in other words, you.

When discarding hardcopy protected health information (PHI), make sure the information is shredded, and, preferably, locked in a secure bin. Leaving hardcopy PHI intact in a wastebasket can lead to a privacy breach. What if the wastebasket is knocked over and the information is not placed back along with the rest of the contents? What if the paper information falls off a recycle truck and blows down the street?

Summary of Key County HIPAA Security Policies and Procedures

This section provides you with outlined information about the County HIPAA Security policies and procedures. These policies are managed by the County Information Security Officer (the phone number of the County Information Security Oflicer is on page 50 - "County Resources"). You can ask your supervisor for a copy of one or more of the County HIPAA security policies at any time.

Email Policy

Email is an instantaneous form of communication. Email is a part of many agencies and departments within the County. While it is expedient in nature, there are many guidelines and rules that should always be respected. Employees will follow the protocol set forth in this manual.

Email usage

Please keep the following list in mind when using County email:

1. Email is designed to facilitate business communications.
2. Email is to be used for the employee's job-related duties and responsibilities.
3. Personal use must be limited so that it does not impede worker productivity.
4. Email must not be used in a way that may be disruptive, offensive to others or harmful to morale.
5. Your emails can be disclosed to law enforcement and government agencies.
6. Management has the right to audit your emails. All messages are the property of the County and part of the public record. Email sent or received at work is not private.

Employers may legally read your email and make use of it. Additionally, all email addresses provided to employees of the County are property of the County.

7. Email created, sent, or received in conjunction with the transaction of official business is public record in accordance with New Jersey's Freedom of Information Act (FOIA) and Public Records Act (PRA). Employees will cooperate with any investigation regarding email associated with the County.

Email prohibited usage

Certain activities are prohibited with regard to use of email and communication systems. The list below provides a framework for activities that fall into the category of unacceptable use. This list is not exhaustive and the County has the right to decide any activity is inappropriate at its discretion:

1. *Do not email ePHI (electronic protected health information).*
2. Using email and communication systems for effecting security breaches or disruptions of network communication.
3. Engaging in any activity that is illegal under local, state, federal or international law.
4. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner.
5. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
6. Use of email system for unauthorized solicitation of funds, political messages, gambling, commercial, or illegal activities.
7. Transmission of information to individuals inside or outside the County without a legitimate business need for the information.
8. Use of email addresses for marketing purposes without explicit authorization from the target recipient.
9. Forwarding of email from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the County without the express authorization of counsel.
10. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.
11. Obtaining access to the files or communications of others with no substantial business purpose and beyond the individual's "need to know".
12. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.
13. Sending external transmission of confidential information via email and communication systems, including email attachments without proper authorization, authentication and encryption.
14. Excessive personal use and/or unethical use of the County's email and communication systems.
15. Opening, responding to, or forwarding email messages from any unknown source.
16. Displaying or transmitting sexually explicit images, messages, games, cartoons or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, marital status, veteran status, age, disability or religious or political beliefs. Email is subject to County policy and procedures

governing sexual harassment and discrimination. Sending or forwarding offensive material violates this policy as well as the business use policy.

17. Using email and communication systems to solicit others for commercial ventures, religious or political causes, outside organizations not approved of by the County, or in any other non-job-related situations.
18. Circumventing user authentication or physical security controls to access email and communication systems.
19. Copying, transmitting or providing information about email and communication systems to any individual without proper authorization.

This list is not considered all-inclusive or collectively exhaustive. Further questions regarding appropriate use of email should be directed to the employee's supervisor or the County Information Security Officer.

Email passes through the Internet from computer to computer. As the message moves between workstations, and is relayed from server to server, it is potentially visible to others. Use discretion before sending confidential or extremely personal information via email.

Remember that there is always the possibility that a recipient of your email message will forward your message on to others. Always write email messages in a professional manner. All forwarded messages, regardless of the nature, may be forwarded to an employee who may find it offensive or harassing.

Unless you have made prior arrangements with the sender, you should never double-click (or open) an email attachment, even when recognizing the sender. There are executable attachments that have file extensions such as .com, .exe, .vbs or .bat. that may be harmful to your computer. These file extensions do not necessarily pose a threat if the sources are verified and safe. Opening an attachment from an unfamiliar and/or unverified source creates a vulnerability to the entire County network.

Email attachments aren't the only way to receive infected files. Simply receiving an email and selecting the message header may inadvertently launch a virus. This can be prevented by removing the **Reading** Pane from the layout in Outlook **2007.**

Turn off the **Reading Pane** in Outlook **2007:**

1. Open Outlook.
2. Select **View** on the menu bar.
3. Click **Reading Pane.**
4. **Select the OFF from the available options.**

There is always the potential of someone impersonating your log on and password to gain malicious entry into the network. If you are logged into your PC, anyone may be able to access your information. Possible security threats and massive problems could be created. Imagine if a destructive and/or offensive email is sent to your supervisor or department head with your name,

or your account used for illegal purposes. To prevent this, always log off or select LOCK COMPUTER when you step away from your PC.

Internet and Intranet Policy

Internet and Intranet access is provided to County employees for the purpose of conducting official County business to reduce costs or as a means to provide more accurate and complete information to County constituents. Once an outbound connection is established, all Internet access activity is electronically monitored on a continuous basis.

Internet and Intranet usage

Please keep the following list in mind when using the Internet and/or the County Intranet:

1. Access to the Internet / Intranet is intended to facilitate business activities.
2. Internet / Intranet communications are not confidential - the County can and will monitor activity.

Internet and Intranet prohibited usage

The following activities are considered inappropriate with regard to use of the Internet and County Intranet. The list below is by no means exhaustive, but provides representative activities that fall into the category of unacceptable use:

1. Engaging in any activity that is illegal under local, state, federal or international law while utilizing the Internet/Intranet.
2. Using the Internet and/or County Intranet for effecting security breaches or disruptions of network communication.
3. Use of the Internet/Intranet that interferes with County workforce member productivity and responsibilities.
4. Excessive personal use (per individual's management staff) and/or unethical use of the Intemet/Intranet.
5. Use of the Internet/Intranet that is disruptive to productivity, offensive or disruptive to others or harmful to morale.
6. Using the Internet to display, obtain, access or transmit sexually explicit images, offensive messages, games, cruioons or anything that may be construed as hmassment or dispmagement of others based on their race, national origin, sex, sexual orientation, marital status, veteran status, age, disability or religious or political beliefs.
7. Soliciting others for commercial ventures, religious or political causes, outside organizations not approved of by County, or other non-job-related functions.
8. Copying, retrieving, modifying or forwarding copyrighted materials, except as permitted by the copyright owner or as a single copy for reference use only.
9. Downloading unauthorized softwme fromthe Internet.
10. Transmitting data and/or information to others with regard to entity identification, practices or County proprietary information unless authorized to do so by executive management at the County.
11. Transmitting data and/or information to others with regard to entity identification, practices or County proprietary information without employment of acceptable, formally documented encryption methods.

12. Creating, sharing, copying, distributing or selling County Internet or Intranet applications for personal gain.

    Note: Employees or other users of the email/Internet systems in violation of local, state, national or international laws may be prosecuted.

Media Controls Policy

The County uses various media to store, disseminate, and share information. Media is considered complementary equipment or devices that work in conjunction with computer technology. Common types of media include CD's, DVD's, media cards, diskettes, pen drives and other portable devices for information storage. Here are key points contained in the Media Controls Policy:

1. Governs the receipt and removal of media (pen drives, diskettes, CD's, tapes, etc.) into and out of a County facility.
2. States that access to media containing ePHI shall be controlled by the media owner and can only be shared with an authorized individual or Entity/User.
3. States that disposal of ePHI stored on media requires the data to be completely overwritten, erased, and destroyed by MCITS or designee.
4. Identifies unacceptable use of media including:
    a. Creating, distributing, possessing, transporting or disposing of County media containing ePHI without authorization by your department head.
    b. Utilizing County ePHI stored on media in an illegal way under local, state, federal or international law.
    c. Unauthorized access, manipulation or transpo1i of media containing ePHI into and out of a County facility.

Password Policy

Passwords allow you to authenticate yourself to a computer system or network. Please keep the following list in mind regarding your password(s) to the County network /systems:

1. Passwords must be at least 6 characters.
2. Choose passwords that cannot be easily guessed but can be easily remembered ("TmBl w2Rt" = This may be one way to remember").
3. Passwords should be changed every 90 days.
4. Do not write your password down - someone may find it.
5. Do not reveal your network / application password to anyone.
6. Do not reveal any password in an email message.
7. Do not talk about your password in front of others.
8. Do not attempt to guess another user's password.
9. The County will periodically run "password cracking" tests to reveal weak passwords.
10. Users who forget their password will be required to have their supervisor contact MCITS or designee to have it reset.
11. The Personnel department will notify MCITS or designee when a workforce member is terminated so their password can be removed immediately.

Passwords may be easily guessed by an intruder to your computer unless precautions are taken. It is advisable not to write your passwords anywhere, but if you do, keep the passwords in a location that is not easily accessed. Do not keep them beneath your keyboard, or taped to your monitor.

Never save passwords in scripts or log on procedures as these could be used by anyone who has access to your PC. For example, you should not check any boxes that ask you to remember the password for future use. Enter a password every time you log on.

Be certain that you are really logging into your system. Just because a log on prompt appears and asks you for your password does not mean you should enter it. Some trojan horses and viruses are log on scripts which capture your User Name and Password and report them back to the hacker. If you believe that additional log on scripts appear on your computer, report your observation to the MCITS Help Desk as soon as possible, and stop using your computer.

Do not leave a computer logged on and walk away from it. This can lead to the possibility breach of security or privacy. Lock your computer when you are away from it for a short period of time, e.g., during lunch or break time. Log off your computer at the end of your work day. Both of these actions prevent others from accessing your computer without your knowledge.

Do not let others have access to your computer or to your files on the network without approval from your supervisor.

Portable Device Security Policy

Portable devices such as laptops, personal digital assistants (pda's), etc. are more vulnerable to loss to theft. Therefore, extra care must be taken to protect them. Here are key points to remember regarding the use of p01iable devices:

1. Use of portable devices to store ePHI is to be limited in scope and secured from theft, loss, or unauthorized access.
2. Use must be approved by MCITS or designee and ePHT stored on a portable device must beencrypted.
3. Portable devices must be boot password protected.
4. Portable devices are subject to the same procedures defined in the HTPAA Workstation Security policy including screensavers, logoff: power off: discarding, replacing, securing and anti-virus / anti-spy ware software.
5. Protected health information (PHI) no longer needed on portable devices must be deleted immediately, including when a portable device is retired or transferred out of the department. Also see the HIPAA media controls policy.
6. Portable devices shall be, where practical, secured with locking devices and kept in a secure location when not inuse.
7. Data backups and recovery are the responsibility of the user.
8. MCITS or designee can audit a portable device at any time.

Sanction Policy

The County workforce has been and will continue to be educated on HIPAA policies and procedures and are, therefore, subject to sanctions for violations. Here are key points to remember regarding the County Sanction policy:

1. The County workforce is expected to follow established policies and procedures regarding the privacy and security of protected health information (PHI).
2. Workforce members who violate policy will be subject to sanctions up to an including termination.
3. Policy violations may result in written warning, suspension or termination.

Workstation Security Policy

Workstations store and display ePHI and steps must be taken to protect ePHI from unauthorized access. Here are key points to remember regarding the County Workstation Security Policy:

1. Requires County workforce to maintain a secure work area in order to eliminate or minimize the possibility of unauthorized access to ePHI:
    a. Workstations shall be positioned / shielded from public view.
    b. Printers, fax machines and copiers shall be located in areas that are not accessible to the public.
    c. All workstations must be logged off / turned off when not in use.
    d. All offices with access to hardcopy PHI and / or ePHI must be locked when unmanned.
2. Portable devices containing ePHI should not be left unattended (e.g. in your car, etc.).
3. Any theft must be immediately reported to the Information Security Officer and a security incident report must be completed.
4. MCITS or designee will conduct random periodic audits and document workstation security vulnerabilities for mitigation.
5. MCITS or designee will maintain an inventory of all hardware and software.

Other County HIPAA Security Policy Outlines

The County HIPAA security policies included in this section define technical and administrative controls that are managed by MCITS and the Information Security Officer (ISO). Numbered outlines of the key points of each policy are provided in this section. Please note that you can ask your supervisor for a copy of one or more of these policies at any time.

Audit Controls

The County is required to audit access to systems that contain ePHI. Here are the key points contained in the County HIPAA Security Audit Controls policy. MCITS will:

1. Deploy technical audit controls.
2. Record and examine system activity.
3. Look for potential and actual violations (security incidents).
4. Respond to security violations and weaknesses.

Authorization Controls

The County is required to authorize access to systems that contain electronic health information (ePHI). Here are the key points contained in the County HIPAA Security Authorization Controls policy:

1. Defines the process for granting access to ePHI (electronic PHI).
2. Access to ePHI requires direct management approval.
3. The objective is to reduce the possibility / vulnerability for ePHI to be altered or destroyed in an unauthorized manner.
4. Requires the County workforce to sign a confidentiality statement.
5. Authorization will be revoked if you are terminated or suspected of misuse or abuse of access.
6. Authorization may be revoked if there is a change in software application or job function.

Breach Notification

The County is required to respond to a breach of information that contains electronic health information (ePHI). This policy includes federal guidance on breach response and notification requirements depending on the scope of the breach. This policy and procedures must be followed in conjunction with the County's Incident Response and Reporting policy and procedure.

Configuration Management

The County is required to manage the configuration of hardware and software systems in order to reduce security risks to ePHI. Here are the key points contained in the County HIPAA Security Configuration Management policy:

1. The intent is to create and manage system (hardware and software) integrity in order to minimize security exposures.
2. All hardware and software implementation must be reviewed and approved by MCITS or designee.
3. Requires MCITS to centrally manage technical controls such as virus protection, spy ware, email filtering, etc.
4. All County security plans, tests, and protection of hardware and software must be documented, updated and readily accessible.

Data Integrity Controls

The County is required to protect the integrity of ePHl against improper alteration and destruction. Here are the key points contained in the County HTPAA Security Data Integrity Controls policy:

1. The intent is to protect ePHT from improper alteration or destruction.
2. Requires software applications to be managed by owners or designee with extensive knowledge of the application and its technical features.
3. Modification of ePHT shall be documented for audit purposes.
4. Systems shall be routinely backed up and the backups stored m a secure location according to the HIPAA media controls policy.

Entity /User Identification & Authentication

The County is required to implement technical solutions for User name and authentication such as User names and passwords. Here are the key points contained in the County HIPAA Security Entity/User Identification & Authentication policy:

1. Resetting forgotten Entity/User names / passwords will require supervisor approval.
2. Minimum authentication requirements include a unique User name and password.
3. Unacceptable use:
    a. Sharing User names and / or passwords.
    b. Allowing anyone to share the use of County software applications for any reason.
    c. Copying, transmitting or providing information about County software applications to any individual without proper authorization.

Facility Physical Security

Facility physical security will be implemented to limit access to County facilities and tangible information assets (ePHI and business confidential information).
Here are the key points contained in the County HIPAA Facility Physical Security policy:

1. Facility security wi11 check for ID badges and passes.
2. Workforce members must wear an ID badge.
3. Visitors must sign in and / or wear a visitor pass as dictated by facility policy.
4. A11 visitors must sign out and return passes and temporary ID badges to security.
5. Visitor logs will be audited by the facility manager periodically.
6. Any movement of County ePHI out of a County facility is prohibited unless authorized / approved by your department head.
7. Where installed, security shall monitor alarms, and cameras.
8. All physical access devices shall be tested on a periodic basis to ensure proper operability.
9. Where appropriate, "swipe" and proximity cards will replace key, combination and pin code locks.
10. Sharing of ID badges or other physical security devices is not permitted.
11. Temporary badges can NOT leave the facility.
12. Access to physical locations must be authorized.

HIPAA Education

County workforce (employees, volunteers, contractors, interns, temporary employees, etc.) must be educated on the County's HIPAA privacy and security policies and procedures. Here are the key points contained in the County HIPAA Education policy:

1. Education will be conducted during orientation and on an annual basis for all workforce members.
2. Education wi11 be conducted as new HIPAA policies and / or procedures are created and approved.
3. HIPAA workforce education is the responsibility of the County HIPAA Privacy and Security Officers.

Information Access Control

Access to County ePHJ is restricted to authorized workforce members and only for management approved purposes. Here are the key points contained in the County HIPAA Information Access Control policy:

1. All workforce members must sign a confidentiality statement.
2. Remote access can only be established when there is a legitimate business need to access County ePHI from a remote location and upon approval by your department head.
3. Information access will be removed upon termination, suspected misuse, or change in the system or job status resulting in a change to the workforce member's "need to know".
4. Authorized workforce members must not reveal their software application User name / password to anyone.
5. Workforce members must not access information that they do not need to know in order to do their job.

Information Security

The County will implement information security controls to protect the confidentiality, integrity and availability of County information assets (ePHI and critical business data) via reasonable and appropriate security measures and controls. Information security will be applied to the following County systems:

1. Software applications.
2. Networks.
3. Workstations.
4. Media.
5. Devices and facilities.
6. Information assets at rest and in transit.

Here are the key points contained in the County HIPAA Information Security policy:

1. County information assets shall be protected against reasonably anticipated threats or vulnerabilities.
2. County information assets shall be restricted to authorized users.
3. Physical safeguards shall be implemented to protect systems and related facilities and equipment from deliberate, accidental and environmental threats.
4. Information security assessments will be conducted on a periodic basis for change management.

Risk Analysis/ Risk Management

Here are the key points contained in the County HIPAA Risk Analysis / Management policies. The County will analyze and manage potential vulnerabilities and associated risk to the confidentiality, integrity and availability of ePHI and will:

1. Implement procedures to detect, contain and correct security violations.
2. Conduct risk analysis that addresses environmental, deliberate and accidental threats.
3. Evaluate the probability for the occurrence of each vulnerability, assess the potential impact due to the risk exposure, and prioritize mitigation of risks and vulnerabilities.

4. Periodically re-assess the risks and vulnerabilities and re-evaluate security procedures for change management and after any security incident.
5. Employ routine system activity reviews, evaluations, and sanctions for violations to support implementation and management.

Security Awareness Training

The County shall develop, maintain, implement and document its security awareness training program. Here are the key points contained in the County HIPAA Security Awareness Training policy:

1. Training is provided to assist County workforce with recognizing potential vulnerabilities to ePHI and ways to reduce the vulnerabilities.
2. The training subject matter includes security reminders, protection from malicious software (e.g. viruses, spy ware, etc.), log-in monitoring, password management, telephone and fax usage, Internet & Intranet usage, internal threats and defenses, external threats and defenses, and physical security.
3. The content of the County's security awareness training program must be presented to all members of the County workforce.
4. Each workforce member must sign to confirm completion of training.
5. The County must establish a timeline for refresher training and periodic reminders.

Security Evaluation

The County will perform periodic technical and non-technical security evaluations in response to environmental or operational changes affecting the security of ePHI. Here are the key points contained in the County HIPAA Security Evaluation policy:

1. Events that will cause security evaluations are:
    a. Changes to the HIPAA regulations.
    b. New local, state or federal laws.
    c. Changes in technical, environmental or business processes.
    d. A serious violation, breach, or other security incident.
2. All HIPAA security policies and procedures are subject to periodic audits by the County's internal audit department and / or the Information Security Officer.
3. Firewall and server event logs will record any event that is a threat to ePHI confidentiality, integrity or availability. MCITS or designee will monitor these logs on a regular basis.

Incident Response and Reporting

The County must have a documented process for responding to security incidents such as viruses and hackers. Here are the key points contained in the County HIPAA Security Incidents policy:

1. A security incident is an adverse incident that threatens the security of ePHT. Examples of security incidents include:
    a. Viruses which compromise of program or compromises data integrity.
    b. Denial of Service - can shut down a network.
    c. Misuse or unauthorized access to ePHT.

d. Damage to facilities, servers, etc.
e. Intrusions performed electronically when an intruder penetrates system security.

2. Incidents require a skilled and rapid response before significant damage can be done.

3. The MCITS goals in the event of a security incident are to:

a. Report the incident to a centralized location.
b. Coordinate a response.
c. Direct technical assistance.
d. Perform training and raise security awareness of users and vendors.
e. Create a knowledge base for security information.
    i) Create a contingency plan.
    ii) Implement security tools such as intrusion detection, intrusion vulnerability, virus protection, spy ware, ad ware, etc.
    iii) Ask vendors to respond to software related security problems.

Security Management

This policy describes the entire process for the County's compliance with HIPAA Security. Here are the key points contained in the County HIPAA Security Management policy:

1. Outlines requirements for creating, administering and overseeing the County security policies for prevention, detection and reaction to security incidents.
2. Comprised of security policies and procedures, security awareness trammg, security architecture, risk analysis, risk management, incident reporting, contingency planning, and accountability for violations via sanctions.
3. Applies to the County systems (software applications), networks, workstations, media, devices and facilities.
4. Applies to information assets at rest and in transit.
5. Security focuses on accessibility, integrity and availability of data through such mechanisms as firewalls, access controls, and encrypting data when the information is transmitted or stored.

Security Policies and Procedures

Yes, the County has a policy that documents the requirements for the development of comprehensive HIPAA security policies and procedures. If the County is ever audited, the Information Security Officer (ISO) will be able to provide this policy to the auditor. The auditor will then be informed of the process the County used to develop their HIPAA Security policies. Here are the key points contained in the County HIPAA Security Policies and Procedures policy:

The County will develop and implement reasonable and appropriate information security policies and procedures to protect County information assets (ePHI and business confidential information).

1. The security policies and procedures must address all requirements of the final HIPAA security rule.
2. The County Workforce members must be informed of all policies and procedures that apply to them in their individual roles.
3. The security policies and procedures must incorporate:

    a. The size, complexity and capabilities of the County.

b. The County's technical infrastructure, hardware, and software capabilities.
c. The cost of implementing security measures.
d. The probability and criticality of potential risks to the County's information assets.

4. The County must ensure that its HIPAA security policies and procedures are compatible with the County's culture and strategic planning activities.
5. The County must conduct an annual review and update them as necessary.

Technical Security Controls

The County must implement reasonable technical security controls (e.g. passwords) in order to protect ePHJ. Here are the key points contained in the County HIPAA Technical Security Controls policy:

1. The County must implement and maintain technical security controls for information assets including integrity controls, message authentication, data encryption, event reporting, network alarms, and audit processes.
2. Considerations for protecting stored data:
    a. Passwords.
    b. Encryption (mainly for mobile devices).
    c. Integrity software.
    d. Anti-virus software.
3. Considerations for protecting data in transit:
    a. Security communication protocols.
    b. Passwords.
    c. Encryption.
    d. Firewalls.
    e. Integrity mechanisms during transmission.
    f. Intrusion vulnerability.
    g. Intrusion detection.
    h. Anti Virus software.

Termination Policy

Separation of service requires that all access to County information assets be revoked in a timely manner to eliminate security exposures. Here are the key points contained in the County HIPAA Termination policy:

1. Any and all media and devices in the terminating individual's possession shall be collected and documented by management on or before the effective date of separation.
2. All access shall also be revoked, including:
    a. All keys, cards, badges or other physical devices that allow access to County equipment or facilities.
    b. All mobile devices, including laptops, pda's, cell phones, etc. shall be collected and documented by management.
    c. All software user accounts / data access shall be removed and security devices recovered (e.g. tokens, etc.).

d. All User names and passwords shall be disabled by MCITS or designee.
e. A terminating individual shall be removed from all file access, distribution lists, and / or any other access list.

Transmission Security

The County must protect ePHI that is transmitted to an open network (e.g. the internet). Here are the key points contained in the County HIPAA Transmission Security policy:

1. It is the policy of the County to implement and maintain transmission security controls for County electronic data, including ePHI in order to guard against unauthorized access to, or modification of ePHI that is being transmitted over an open network (e.g. Internet) or via any form of portable media.
2. This policy outlines the requirements for transmission of ePHI to Non-County entities, between County entities, using electronic portable media, and using wireless networks and devices.
3. The following information applies to all County workforce members regarding the transmission of ePHI:

    a. At this time the transmission of ePHI via email is prohibited.
    b. MCITS or designee must be informed of and must approve any and all transmissions of ePHI from the County network to an outside User by any means, including email, file transfer, portable media, etc. before you are authorized to transmit.

Workforce Security

Most information security breaches are internal to an organization. The County is required to manage their workforce and their access to PHI. Here are the key points contained in the County HIPAA Workforce Security policy:

1. The County performs a background check for workforce members.
2. County workforce shall obtain proper authorization from the appropriate County management.
3. All workforce members with access to County ePHI must be properly supervised.
4. All workforce members with access to County ePHI are required to complete County information security awareness training.

Complete List of the County HIPAA Privacy Policies and Procedures

Please note that you can ask your supervisor for a copy of one or more of these policies at any time. Here is the table of contents from the County HIPAA Privacy Policy book:

102 -Amendments to the Policies and Procedures.
103 - Definitions for the Policies and Procedures Manual.

Policy Area: Individual Rights
201 - An Individual's Right to Receive a Notice of Privacy Practice.
202 -An Individual's Right to Access Protected Health Information.
203 - An Individual's Right to Amend Protected Health Information.

204 - The Right of an Individual to an Accounting of Disclosures.
205- An Individual's Right to Request Restrictions on the Uses and Disclosures of Protected Health Information.
206- An Individual's Right to Communications by Alternative Means.
207- An Individual's Right to File a Complaint Regarding the Privacy Practices, Policies and Procedures.
208- Other Rights of an individual.

Policy Area: Uses and Disclosures of PHI - General
301 - Uses and Disclosures of Protected Health Information - General Rule.
302 - Condition-Specific Requirements in New Jersey Law for the Disclosure of Protected Health Information.
303 - Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations.
304 - Uses, Disclosures, and Requests of Only the Minimum Necessary Protected Health Information.
305 - Routine and Recurring Disclosures and Requests.
306 - Creation, Uses and Disclosures of Limited Data Sets.
307 - Creation, Uses and Disclosures of De-Identified Health Information.
308 - Disclosures to a Business Associate.

Policy Area: Uses and Disclosures of PHI That Require Authorization
401 - Uses and Disclosures of Psychotherapy Notes.
402 - Uses and Disclosures for Marketing.
403 - Uses and Disclosures for Fundraising.
404 - Uses and Disclosures for Research.
405 - Uses and Disclosures for Purposes Not Specifically Addressed m the Policies and Procedures Manual.

Policy Area: Uses and Disclosures of PHI That Require The Opportunity to Agree or Object
501 - Uses and Disclosures for a Facility Directory.
502 - Uses and Disclosures for Persons Involved in an Individual's Care and for Notification Purposes.

Policy Area: Uses and Disclosures of PHI That DO NOT Require An Authorization or the Opportunity to Agree or Object
503 - Uses and Disclosures Required by Law.
504 - Uses and Disclosures for Public Health Activities.
506 - Disclosures about Victims of Abuse, Neglect or Domestic Violence.
507 - Uses and Disclosures for Health Oversight Activities.
508 - Disclosures for Judicial and Administrative Proceedings.
509 - Uses and Disclosures about Decedents.
510 - Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation.
511 - Uses and Disclosures to Avert a Serious Threat to Health and Safety.
512 - Uses and Disclosures for Specialized Government Function.
513 - Disclosures for Workers' Compensation.

514 - Uses and Disclosures to the Secretary of Health and Human Services.
515 - Disclosures by Whistleblowers.
516 - Disclosures for Law Enforcement Purposes.
517 - Disclosures by Workforce Members Who are Victims of a Crime.

Policy Area: Administrative Requirements
601- General Documentation and Retention.
602 - Designation as a Covered Entity.
603- Designation of a Privacy Official and Contact Information.
604 - Standards for the Creation and Uses of Authorizations.
605 - Establishment of Personal Representatives.
606 - Verification ofldentity and Authority for the Disclosure of Protected Health Information.
607 - Employee Training on the Privacy Practices, Policies and Procedures.
608 - Employee Access to Protected Health Information.
609 - Prohibition on Intimidating and Retaliatory Acts.
610 - Safeguards to Protect the Privacy of Protected Health Information.
611 - Sanctions for Violating the Privacy Policies and Procedures.
612 - Accounting for Disclosmes of Protected Health Information.

Complete List of the County HIPAA Security Policies and Procedures

Please note that you can ask your supervisor for a copy of one or more of these policies at any time. Here is the table of contents from the County HIPAA Security Policy book:

HIPAA 101 -Audit Controls.
HIPAA 102 - AuthorizationControl.
HIPAA 103 - Breach Notification.
HIPAA 104 - Configuration Management.
HIPAA 105 - Data Integrity Controls.
HIPAA 106 - Education Policy.
HIPAA 107 - Email and Communication Systems.
HIPAA 108 - Entity Identification Authentication.
HIPAA 109 - Facility Physical Security.
HIPAA 110 - Incident Response and Reporting.
HIPAA 111 - Information Access Control.
HIPAA 112 - Information Security.
HIPAA 113 - Internet and Intranet Use.
HIPAA 114 - Media Controls.
HIPAA 115 - Password Policy.
HIPAA 116 - Portable Device Security.
HIPAA 117 - Risk Analysis.
HIPAA 118 - Risk Management.
HIPAA 119 - Security Awareness Training.
HIPAA 120 - Security Evaluation.
HIPAA 121 - Security Incidents / Response.
HIPAA 122 - Security Management.
HIPAA 123 - Security Policies and Procedures.
HIPAA 124 - Technical Secmity Controls.

HlPAA 125 -Termination Policy.
HIPAA 126 - Transmission Security.
HIPAA 127 - Workforce Security.
HlPAA 128 - Workstation Security.

The HITECH (the Health Information Technology for Economic and Clinical Health) Act of 2009

President Obama signed the HITECH Act in February of 2009. Also called "HIPAA on Steroids", it is the most expansive modification to the federal HIPAA privacy and security rules since the 1996 enactment of HIPAA.

The COUNTY workforce has been trained on HIPAA Privacy and Security for a number of years now. Ongoing training will include both HIPAA and HITECH.

The most important thing for all COUNTY work force is to understand that it is even more important now to protect and secw-e COUNTY health information. So everything that you have learned about HIPAA up to now takes on greater meaning because of the HITECH Act. We must continue to protect all hard copy, verbal and electronic health information. We should never leave hard copy health information unattended. We should be careful when talking about a resident or client to make sure other residents, clients and visitors cannot hear us. And, we need to protect electronic health information that is stored in a database and / or transmitted to the internet, via email or other means. And, you should never email health information to anyone outside of the COUNTY network, unless you have been authorized to do so.

So here is an introduction to HITECH:

We have all heard about the federal stimulus program called ARRA. It stands for the American Recovery and Reinvestment Act. Of the $700+ billion that has been set aside for ARRA, approximately $20 billion was targeted for healthcare information technology (HIT) under HITECH. The objective is to expand the use of electronic medical records throughout the healthcare system, including hospitals and physicians across the country. Another objective is to electronically exchange health information from individual health care providers like the COUNTY to other local, state and federal data repositories. So, for example, if you are traveling on vacation to another state (e.g. Florida) and need healthcare services, the healthcare provider in Florida will be able to access your latest information such as medications, allergies, and test results. By doing so, they will be able to provide a higher quality of care and reduce wasteful redundant testing. So, the electronic age of patient, resident and client medical records has begun. And with it, a greater need to protect the privacy and security of health information.

Your COUNTY HIPAA Privacy and Security Officers are working together to make sure that the COUNTY achieves compliance with the requirements of HJTECH.

Here are some highlights of the HITECH Act of 2009:

- Government audits and monitoring will mcrease, and will be funded by $$ penalties.
- $$ penalties have increased substantially.

- The State Attorney General can now take civil action on behalf of aggrieved individuals.
- Potential civil monetary penalties and criminal sanctions can be applied to the COUNTY and / or anyone at the COUNTY who violates HIPAA.
- If there is a breach of COUNTY resident or client information, the COUNTY may have to notify the media and post it on our website, depending on how large the breach is.
- COUNTY residents and clients will have more rights, such as the right to receive a copy of their electronic medical record, and to know who has accessed their electronic information.
- Companies that do work for the COUNTY and need to access COUNTY health information, also known as HIPAA Business Associates, now have to comply with HIPAA and are liable for the same penalties for violations.

The COUNTY has updated existing HIPAA policies, has added a new Breach Notification policy and procedure, has updated the COUNTY business associate agreements, and is in t he process of reviewing and potentially updating the COUNTY Notice of Privacy Practices (NPP) that is handed out to COUNTY residents and clients. In addition, a new training curriculum will be provided to the COUNTY workforce and it will include HITECH.

The next steps for you, our COUNTY workforce, is to continue to d o a great job protecting COUNTY health information, and to report any potential issues or violations to your manager.

Please remember that you are the eyes and ears of the COUNTY. The health information you are protecting today may someday be your own!

Computer Technology

General Security Practices

Do not leave your workstation without locking it or logging off. If you are away from your desk, and still logged in to the network, others can use your account without your knowledge. They could send email using your email account, or use yow- account for illegal purposes. You can log off, or lock, a computer running either Windows 2000, Windows XP, or Windows 7. Logging off and locking a computer are two separate actions. Both operating systems require a password to log on again, or to unlock the computer.

Log on and log off securely

Log on to your computer using only *your* User name and password.

You log on to your computer when you start the computer by pressing the power button. After the computer powers on, a log on screen should appear if you are logging in correctly to the County network, and to your assigned domain name. You will be prompted to enter in your User name, your password, and your correct domain name. If you do not see this, notify your supervisor.

To Log On your computer at initial start up:

1. Enter your User name.
2. Enter your password.
3. Ensure that you have selected the correct domain name.

To Log Off your computer:

1. Click the **Start** button on the taskbar.
2. Select **Log Off.**

The computer is still running, but you cannot gain access to any programs until you log onagam.

Lock your computer

To lock your computer (Windows 2000, Windows XP, or Windows 7):

1. Press the keyboard combination **CTRL+ALT+DEL.**
2. The Windows Security window will appear.
3. Select **Lock Computer.**

Your computer will lock, and only your wallpaper can be seen. Any windows you have open on your desktop cannot be viewed or accessed. You can unlock the computer by entering your password in the field provided for you after pressing CTRL+ALT+DEL.

Both Windows XP, Windows 2000, and Windows 7 will require a password to log on agam.

Enable a password protected screensaver:

1. Right-click on the desktop.
2. Select **Properties.**
3. Select the **Screen Saver** tab.
4. Select any screensaver from the drop-down menu.
5. Check the box On resume, password protect.
6. Click **OK.**

Selecting the On Resume, password protect check box will lock the computer when the screensaver is activated. When you begin working again you will be prompted to type your password to unlock the computer.

Note: In Windows XP, your screensaver password is the same as your log on password. If you do not use a password to log on, you cannot set a screensaver password.

Be prudent in allowing others to access your computer. Computer administrators who access your computer should log on as themselves and not use your usemame and password.

Whether you have an anticipated or unanticipated visit from MCITS, always ask for identification to ensure the protection of the files on your pc. If you receive an email asking for your username and password, do not reveal this information. No one from the County Information Services will solicit that information via email.

Power Off Your Computer

Shut down your computer at the end of the work day. This allows audits performed over the network to be completed successfully. In addition, should yow- computer be infected with a virus or spy ware, these applications may run in your absence. You can prevent this by shutting down your computer. To Shut Down your computer:

1. Click the **Start** button on the taskbar.
2. Select **Shut Down** from the menu.
3. The Shut Down Window appears. Depending on your operating system, select the option button next to Shut Down, or select Shut Down from the drop-down menu.

You should only press the power button to power off your computer if your mouse has frozen, and if pressing CTRL+ALT+DEL is unsuccessful in showing the window allowing you access to the Shut Down button.

Press the power button on the computer to start the computer again.

AutoComplete

AutoComplete is a function of Internet Explorer dealing specifically with passwords on a web page. The County is creating more applications run through the County Intranet. These web based applications will require passwords to access them. The browser may prompt you to save your log on name and password. Turn off this option if it occurs.

To change AutoComplete Settings:

1. Open Internet Explorer.
2. Select **Tools** on the menu bar.
3. Click **Options.**
4. Select the **Content** tab.
5. Click the **AutoComplete** button.
6. Deselect the checkbox next to User names and passwords on forms.
7. Click **Clear Passwords** to clear any existing saved passwords.
8. Click **OK.**

File Saving and File Protection

Save your files to the My Documents folder or to the folder on the Network that has been designated for your use by MCITS. All files on the County network are backed up for your security and protection. Files saved to your own computer are not backed up on the network.

Files on the network may be visible to everyone, or restricted to a group of certain users. Each department directory on the server is set up differently. Some files on the server will have permissions set so that only ce1iain people in a department can access the files. These files are protected.

All County computers have virus detection tools. If your computer alerts you to a virus attack, notify the MClTS Help Desk. Also notify the person you believe passed the virus to you.

Check to make sure you have antivirus software installed:

1. Click **Start** on the task bar.
2. Click **Programs.**
3. The Symantec Client Security folder or Norton Antivirus should be listed in the Programs menu.
4. Verify that the File Definition File box lists a Version date that is not older than a week.
5. If you do not see Symantec Client Security, contact the MCITS Help Desk

Email Usage and Prohibited Usage

For information about email usage and prohibited usage, see pages 24 & 25 of this manual.

Internet and Intranet usage and prohibited usage

For information about Internet and Intranet usage and prohibited usage, see page 27 of this manual.

Passwords

For information about passwords, see page 30 of this manual.

Modem Usage

Modem usage must be approved by the County Information Services. A modem allows you to connect your computer to the Internet using a telephone line. The modern dials into an Internet Service Provider (ISP), which in turn allows you access to the Internet. This is the slowest method of connecting to the Internet.

Modems present a special security risk. The County network is protected by a set of precautions designed to prevent an attack by public networks. Using a modem to connect to the Internet while your computer is still connected to the County network is prohibited.

lf you are permitted to use a modem, disconnect your computer from the County network before initializing use of the modem. Failure to disconnect increases the possibility of unauthorized users gaining access to computers on the County network.

Unauthorized modem use violates County security policies. A modem allows information to be shared, so coordination with MCITS is mandatory before using a modem.
When using a modem, ensure with MClTS that all security features are installed and set up correctly to offer your computer the greatest amount of protection. Turn on all the security featmes of your remote access software before allowing your computer to be accessed by phone. Turn auto-answer off unless you are prepared to have your computer respond to callers. Disconnect the modem from the phone line when not in use. Only plug in the phone line cord when you are going to use the modem.

Having an unlisted number will not protect you from direct attacks (breaking into your computer via a phone line). It is easy for a hacker to probe a phone line and detect a modem before launching an attack.

Networking

A network is a system of computers that are connected by either wires, or other means in order to share information.

On the following page is an illustration of the County network. A firewall is depicted in the center of the diagram that is made up of software that monitors and restricts network access in both directions. The diagram shows County department network traffic having to travel from the County servers, through the firewall to connect to the Internet. It also illustrates how all Internet activity must first travel through the firewall prior to entering the County network. On the outside of the firewall are the library system and Wide Area Network (WAN). Both of these systems must travel through the firewall before reaching the County servers on the other side of the firewall.

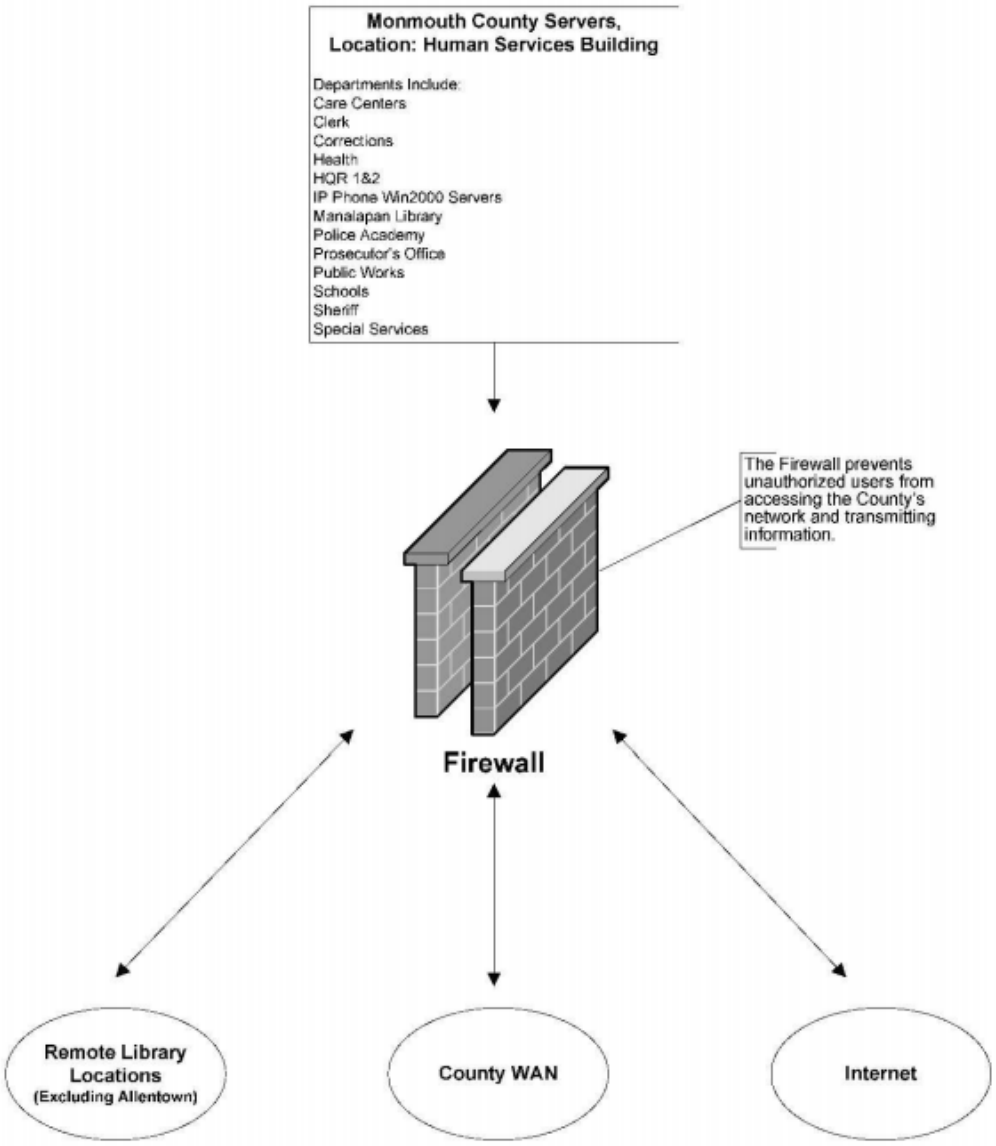

Figure 1 – The County Network

Reporting Abuses

If an individual, a member of the public, or an employee suspects your facility is not complying with HIPAA, he or she may file a complaint with the Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services.

A complaint must be filed in writing (either on paper or electronically) within 180 days of when the violation of privacy was discovered. The OCR has the authority to audit a facility's privacy practices for HIPAA compliance, and will likely do so by reviewing your facilities' policies and procedures and interviewing staff.

All facilities must also designate who handles complaints. This person may or may not be the facility's privacy officer.

You should feel free to contact this person if you think there are privacy violations occurring regularly in your facility. Ask your supervisor or consult your facility's privacy policy to find out who handles complaints in yow- facility.

County Resources

- County Information Services Help Desk: 732-577-5877
- County Information Security Officer: 732-431-7845
- County Information Privacy Officer: 732-409-4898
- County Safety Officer: 732-409-4898
- County Employee Intranet: simply type "Intranet" into your Web Browser address line. No other prefix orsuffix is necessary.
- County Web site: http://www.co.monmouth.nj.us

APPENDIX A- HIPAA Definitions

Covered entity
A health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy Regulations.

Covered functions
Those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Disclosure
The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

ePHI (electronic Protected Health Information)
Electronic protected health information is individually identifiable health information that is transmitted or maintained by / in electronic media.

Health care clearinghouse
A public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and "value-added" networks and switches, that processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care component
A component or combination of components of a hybrid entity designated by the hybrid entity in accordance with the HIPAA Privacy Regulations.

Health care provider
A provider of services (as defined in section 186l(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information
Any information, whether oral or recorded in any form or medium, that 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 relates to the past, present, or future physical or mental health or condition of an individual; the provision of health

care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HHS
The Department of Health and Human Services.

Hybrid entity
A single legal entity that is a covered entity; whose business activities include both covered and non-covered functions; and that designates health care components in accordance with the HIPAA Privacy Regulations.

Individual
The person who is the subject of protected health information (PHI).

Individually identifiable health information
Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate
A person incarcerated in or otherwise confined to a correctional institution.

Law enforcement official
An oflicer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

PHI (Protected Health Information)
Protected health information (PHI) is individually identifiable health information that is transmitted by electronic media, maintained in electronic media, and / or transmitted or maintained in any other form (including oral or written PHI).

Psychotherapy notes
Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any

summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Standard
A rule, condition, or requirement describing the following information for products, systems, services or practices: classification of components; specification of materials, performance, or operations; or delineation of procedures; or with respect to the privacy of individually identifiable health information (also known as protected health information (PHI)).

Transaction
The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: health care claims or equivalent encounter information; health care payment and remittance advice; coordination of benefits; health care claim status; enrollment and disenrollment in a health plan; eligibility for a health plan; health plan premium payments; referral certification and authorization; first report of injury; health claims attachments; Other transactions that the Secretary may prescribe by regulation.

Treatment
The provision, coordination, or management of health cai·e and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use
With respect to protected health information (PHI), the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce
Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

APPENDIX B - HITECH Definitions

ARRA
American Recovery and Reinvestment Act

Breach
"Breach" is defined in the Act as "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."

The HITECH ACT includes exceptions to this definition for cases in which:

(1) An unintentional acquisition, access or use of PHI by a <Your Entity Initials> workforce member or a person acting under the authority of a <Your Entity Initials> or your business associate, if such acquisition , access or use was made in good faith and within the scope of authority and does not result in further use or disclosure
(2) Any inadvertent disclosure by a person who is authorized to access PHI at <Your Entity Initials> or your business associate to another person authorized to access PHI at the same <Your Entity Initials > or your business associate and the information received as a result of such disclosure is not further used or disclosed
(3) A disclosure of PHI where <Your Entity Initials> or your business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

Data in motion
Data in motion is data that is moving through a network, including wireless Transmission.

Data at rest
Data a rest is data that resides in databases, file systems, and other structured storage methods.

Data in use
Data in use is data in the process of being created retrieved, updated, or deleted.

Data disposed
Data disposed is discarded paper records or recycled electronic media.

Destruction
The media on which the PHI is stored or recorded has been destroyed in one of the following ways:

Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Encryption
The guidance states that PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following applies:

Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. Encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described in NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPSec VPNs; or 800- 113 , Guide to SSL VPNs, and may include others which are FIPS 140-2 validated.

HHS
Health and Human Services

Secured protected health information
In consultation with information security experts at NIST, HHS has identified two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals:

- encryption and
- destruction.

The guidance also addresses the destruction of PHI both in paper and electronic form as a method for rendering such information unusable, unreadable, or indecipherable to unauthorized individuals.

If PHI is encrypted or destroyed prior to disposal in accordance with the guidance, no breach notification is required following access to the encrypted or disposed hard copy or electronic media by unauthorized persons.

The HITECH Act of 2009
Health Information Technology for Economic and Clinical Health Act; part of the ARRA law

Unsecured protected health information
Section 13402(h) of the HITECH Act defines "unsecured protected health information" to mean protected health information that is not secured through the use of a technology or methodology specified in the guidance.

APPENDIX C - Computer Technology Definitions

Acceptable Use Policy (AUP)
A set of rules and guidelines that specify the expectations and appropriate use of a network.

Account
The authorization to access a specific computer system or network. Authorization is achieved by accessing the computer system with a User name and password.

Asymmetric Cryptography Key
Asymmetric keys are determined using mathematical algorithms. Asymmetric keys are then shared, perhaps only one time. Asymmetric keys are also commonly referred to as 'Public Keys.' Examples of asymmetric-key or public-key cryptosystems are Pretty Good Privacy (PGP) and Secure Socket Layer (SSL). Asymmetric encryption systems have two important properties: (1) the key used for encryption is different from the one used for decryption, (2)neither key can feasibly be derived from the other.

Auditing tool
An application that analyzes the security status of a computer system or network. The County uses Track-It.

Authentication
Mechanisms used to verify the identity of a user. The process of authentication typically requires the user to supply a User name and password.

Biometric identification systems
Biometric identification systems, or biometrics, identify a human being from a measurement of a physical feature or repeatable action of the individual referred to as "something you are." Examples of biometric measures are hand geometry, retinal or iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voiceprints and written signatures.

Browser (see Web Browser)

Centrally-administered network
When a network of systems is cared for, or administered, by a centrally located group of administrators.

Certificate
Data which is used to verify a digital signature. A ce1iificate is only as trustworthy as the agency which issued it. A certificate is used to verify a particular signed item, such as an email message or a web page.

Clean system
A computer which is installed with an operating system and software obtained from a trusted source of media distribution.

Client
A computer system a user uses to access services hosted by a server, or by another computer system.

Compound documents
A document is a file containing a set of data. Files may consist of multiple parts: a plain document, an encrypted document, a digitally-signed document or a compressed document. Compound documents are multi-part files that may require several applications to interpret them.

Computing environment
A data processing system consisting of hardware, application software, data, procedures, and operations and can extend to external entities. Computing environments may also be connected to telecommunications facilities.

Cookies
Tiny bits of data that register information on your computer about a visit to a website. This information is for future use by the server hosting that website. That server may also receive information about cookies from other sites visited by your computer. These files are automatically saved to your computer. However, various settings may clear the cookies upon closing of the Internet browser.

Daemons
Processes that run on computer systems to provide services to other computer systems. A daemon is usually a server.

Decrypting
The process of reversing the encryption of a file or message to recover the original data in order to use it or read it.

Default account
Some systems and server software come with preconfigured accounts. These accounts are set up with a predefined User name and password to allow anyone access to the account. A default account makes it convenient for users to initially log on. To reduce the risk of abuse to the system, default accounts should be turned off or have their predefined passwords changed.

Dial-in service
Providing access to computer systems or networks via a telecommunications network. A computer uses a modem to make a telephone call to another modem, which in turn provides network access service.

Digital Signature
An electronic signature created by a mathematical computer program. A digital signature is not a hand-written signature or a graphic picture of a signature. It is as unique as a thumbprint. Attaching a digital signature to an email message gives the recipient of the message verification of the validity of the sender.

Directory
A shared folder on a network server. Some directories are password protected so that only certain users can access the folder.

Downloaded software
Software packages retrieved from the Internet.

Downloading
The act of retrieving files from a server on the network, or from the Internet.

Email package
An application that enables a user to communicate electronically with other users. There are different email applications; each with its own interface. Every email package allows the user to create, send, retrieve and read messages.

Encryption
A mathematical process of scrambling data for privacy protection.

Encryption software
Software that provides a user with the ability to encrypt messages and files.

End-user
An individual who uses computer systems and computer networks. An end-user is also known as a user.

File
The basic unit of storage that enables a computer to distinguish one set of information from another. It is a collection of data that a user can change, use, retrieve, delete, or send to an output device, such as a printer or email program. It includes user data, applications, operating systems and a system's configuration data.

File server
A computer system that provides users the ability to share and work on files stored on the system network.

File transfer
The process of transferring files between two computer systems over a network, using a protocol such as FTP or HTTP.

Fixes and patches
Sets of files that have to be installed on computer systems in response to the discovery of security vulnerabilities in a software application or operating system. These files remove the security vulnerability by fixing or patching the computer system or programs.

FTP (File Transfer Protocol)
A protocol that allows for the transfer of files between an FTP client and FTP server.

Group of users
Security software often allows permissions to be set for groups of users as opposed to allowing permissions for only an individual user.

Guest log on
Computer services are available without any kind of authentication.

Help desk
A support entity that gives assistance with a computer or technology related problem.

HTTP
Hypertext Transfer Protocol is the way data is transferred over the Internet.

Internet
A collection of interconnected networks that use a common set of protocols to enable communication between the connected computer systems.

Intranet
An internal or private Internet used strictly within the confines of an organization.

Logged On
When a user has successfu11y authenticated themselves to a system, proving to have legitimate access to that system by entering in a User name and password. The screen that displays the fields for the User name and password is called the log on window, or log on prompt.

Logging
Systems and server software have the ability to keep track of events that occur on the system. Events can be configured to be written to a log file, which can be read later. This allows for system failures and security breaches to be identified.

Log on scripts
Commands that are executed when a user logs in on a PC.

Masquerade
Anyone who pretends to be someone they are not in order to obtain access to a computer account. Masquerading can be accomplished by providing a false User name, or by stealing someone else's password and logging in as them.

Message Authentication Code
Message authentication codes (MAC) offer protection against message tampering and against injection of false messages by a third pai1y and serve as message integrity checks using secret keys.

Mobile devices
Transportable workstation devices include but are not limited to laptops, palm pilots, text pagers, notebooks, and wireless communications systems.

Modem
The hardware that allows a computer to connect to the Internet.

Network File System
NFS is an application and protocol suite providing a way of sharing files between clients and servers. There are other protocols which provide file access over networks. These provide similar functionality, but do not interoperate with each other.

Networking features of software
Software that contains features which make use of the network to retrieve or share data.

Network services
Services which are provided on a server located on the network, and not on a local computer system.

Open network
A network that is exposed to various external networks during the course of carrying out daily business operations. Examples of external networks would be the Internet and vendor connectivity and email systems.

Pass phrase
A pass phrase is a long password. It is often composed of several words and symbols to make it harder to guess, e.g., too&hot*to$handle

Password-protected screensaver
A screensaver obscures the normal display of a monitor when idle. A password protected screensaver will prompt for the employee's password when the screen saver is deactivated. It prevents unauthorized users from gaining access to files on your computer.

Patch (see Fixes and Patches)

PC
An individual workstation, also referred to as a personal computer.

Permissions
Another word for the access controls that are used to control the access to files and other resources on a server.

Platform
A systemic environment capable of hosting and storing applications, files, directories and electronic data Plug-in Modules
Software components that integrate into other software to provide additional features.

PPP (Point to Point Protocol)
A mechanism that establishes a network connection between the PC and Internet Service Provider. Once connected, the PC is able to transmit and receive data to any other system on the network.

Private network
A network established and operated by an organization or corporation for users within that organization or corporation.

Public network
A network established and operated by a telecommunication administration or by a Recognized Private Operating Agency (RPOA) for the specific purpose of providing circuit-switched, packet-switched, and leased-circuit services to the public.

Privacy programs
Encryption software that protects the confidentiality and privacy of the users that make use of it.

Public record
A record that is made by a public official in the pursuance of a duty to disseminate information to the public or to serve as a memorial of official transactions for public reference.

Remote access software
Software that allows a computer to use a modem to connect to another system. It also allows a computer to listen for calls on a modem. Remote access software may provide access to a single computer or to an entire network.

Remote Log on
The act of an end-user using a network to log on to a system.

Security features
Features which provide protection or enable end-users and administrators to assess the security of a system.

Security policy
A policy written by organizations to address security issues. Guidelines and rules are created for users with respect to physical security, data security, information security, and content.

Server
A computer system, or a set of processes on a computer system providing services to clients across a network.

Shared account
A common account is one which is shared by a group of users as opposed to a normal account which is available to only one user.

Sharing permissions
Computer systems allowing users to share files over a network. These systems invariably provide a mechanism for users to use to control who has permission to read or overwrite these files.

Site
Depending on the context in which this term is used, it might apply to computer systems that are grouped together by geographical location, organizational jurisdiction, or network addresses. A Site may refer to a network under a common administration.

SSH (Secure Shell)
SSH provides a protocol between a client and server, allowing for encrypted remote connectivity.

SSL (Secure Sockets Layer)
This protocol provides security services to otherwise insecure protocols which operate over a network. SSL is typically used by web browsers to encrypt data sent to and from a server.

Spy ware
Software that sends information about your Web surfing habits to the website, or an individual outside the network. Often built into free downloads from the Web, it transmits information in the background while visiting websites. It tracks and records your Web browsing habits without your consent. Spy ware is known to be problematic with certain software, and slows down a computer.

Symmetric Cryptography Key
Symmetric cryptography keys are based on mathematical algorithms and a string of bytes called a key. The strength of symmetric cryptography keys is based on the strength of the algorithm and the length of the key. Symmetric keys are also commonly referred to as 'Secret Keys' or 'Private Keys.'

System
A functionally related group; a network of related computer hardware, software, and data transmission devices.

Systems Administrator
An individual who maintains the system and has system administrator privileges. Most County employees will not be systems administrator; rather they are users.
System administrators have more rights (greater permissions) as their work involve the maintenance of system files on the network.

System files
The set of files on a system which govern the functionality of the system. System files do not belong to end-users.

Telnet
A protocol that enables remote log on to other computer systems over the network.

Temporary Internet files
Files that download to your computer when you surf the Internet. In order to view a page on the Internet, you need to download the page. All Internet pages are downloaded to a specific folder and should be removed so that they are not taking up space on your hard drive.

Terminal
A workstation device connected to a computer system in order to provide text-based access to the system by users and administrators.

Threats
The potential that an existing vulnerability can be exploited; compromising the security of systems or networks. Even if vulnerability is not known, it represents a threat by definition.

Token
A physical item that contains the identity of the holder or "something you have." Examples of tokens include ID badges and smart cards.

Trojan Horse
A program which carries within itself a means to allow the creator of the program access to the system using it.

User
Refers to all employees, elected and appointed officials, independent contractors, and persons or entities accessing or using any of the County's electronic technology resources.

User name (User name, User ID, User identification, Log on name)
A group of characters that are used to identify a person or other entity when accessing networks, systems or applications. User names accompanied by a password, known only to the individual associated with the ID, are used to gain access to a system or application.

Virus
A program which replicates itself on computer systems by incorporating itself (secretly and maliciously) into other programs. A virus can be transferred onto a computer system in a variety of ways.

Virus-Detection Tool
Software that detects and removes computer viruses, alerting the user appropriately through scans and updated virus definitions.

Vulnerability
The existence of a weakness, a design error, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

URL
Uniform Resource Locator; also known as the web address of a website.

Web browser
An application that provides access to the Internet and to other programs that are Internet based. This is also referred to as an Internet browser.

Web browser cache
A component of the file system that is used to store web pages and related files. It can be utilized to reload recently accessed files from the cache instead of loading it every time from the network.

Web browser capabilities
The set of functionalities on a web browser for use by the end-user. This may affect the presentation of a web page when viewing it.

Web server
A server program that provides access to web pages. Some web servers provide access to other services, such as databases and directories.

Workstation
A workstation allows a user to transmit or receive information from a computer as needed to perform a job. Workstations (e.g. personal computers, laptops, etc.) can be used in a stand-alone mode or can be connected to a mainframe in terminal emulation mode.

Workstation device
A workstation device includes but is not limited to printers, copiers, fax machines, and any other mechanisms that replicate sensitive corporate information such as information assets and financial statistics.

Worm
A computer program which replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments.

APPENDIX D-Email Subscription Policy

County of Monmouth Email Subscription Policy

To address the essential need for communication with residents and members of the community, the County of Monmouth has established an email subscription service. The County of Monmouth recognizes the importance of meeting the growing demand for electronic communication with the public and providing timely information through email.

The Board of Chosen Freeholders and the County Administrator have a vested interest and expectations in deciding the message "spoken" on behalf of the County of Monmouth through email communication. This policy establishes acceptable practices and guidelines for the use of email and email subscription services.

POLICY

1. The County of Monmouth will use an email subscription service (software, etc.) to provide one-way email communication. The use of an outside hosting service will ensure that the County of Monmouth is not blacklisted on various email services. This service will be an "opt - in/opt - out" application, allowing subscribers, to unsubscribe from a list.

2. The County of Monmouth Public Information Office and Information Technology Services department will research and review the email subscription service on a yearly basis to ensure that it is meeting the needs of the County. Information Technology Services reserves the right to transition from one subscription service to another as deemed appropriate.

3. All official County of Monmouth email messages and/or templates will be reviewed and revised or written and approved by the County of Monmouth Public Information Office. All individual list descriptions (on the subscription sign-up pages) will also be written by the Public Information Office in conjunction with the respective department/agency pertaining to the list.

4. The County of Monmouth Information Technology Application Development Group will be responsible for testing, approving, and/or authorizing email messages that are sent out to subscribers. This will mitigate possible errors and redundant email messages.

5. All email templates shall be consistent with the "look and feel" of the County of Monmouth and its departments. All email message and branding should be consistent with the goals of the County of Monmouth.

6. New requests for email subscription lists will be reviewed and approved by the County of Monmouth Public Information and Information Technology Services departments.

7. The County of Monmouth will respect its subscribers' privacy. The County will not use the email addresses for any other purpose other than the retention on the list they have elected to sign up for.

8. The Public Information Office and Information Technology Services will monitor the lists. If deemed necessary, a list may be deleted if the sign-up is low

APPENDIX E- Social Media Policy

County of Monmouth Social Media Policy

To address the fast-changing landscape of the Internet and the way residents communicate and obtain information online, the County of Monmouth and its departments may consider participating in social media formats to reach a broader audience. The County of Monmouth encourages the use of Social Media to further the goals of the County and the missions of its depru1ments where appropriate.

The Board of Chosen Freeholders and the County Administrator have an overriding interest and expectation in deciding who may "speak" and what is "spoken" on behalf of the County of Monmouth on social media sites. This policy establishes guidelines for the use of social media.

The County of Monmouth, Information Technology Services, shall approve what social media outlets may be suitable for use by the County and its departments. The Information Technology Services Application Development Group shall serve to educate departments on how to best use various social media outlets to achieve their goals.

POLICY

1. All official County of Monmouth presences on social media sites or services are considered an extension of the County's information networks and are governed by all policies applicable to the use of County computer s and electronic media as well as the County of Monmouth Internet Access and Use Guidelines.

2. The County Administrator will review department requests to use social media sites and may delegate this review function to the Information Technology Services Application Development Group and the Director of Public Information.

3. The Application Development Group will advocate using social media to help departments reach their stated goals, by assisting departments in developing appropriate uses for social media, assisting the selecting of appropriate social media outlets, and helping departments define a strategy for using social media.

4. Agencies requesting representation, including separate media accounts must have approval and work with Public Information and Information Technology Services. This measure will ensure consistency and reduce the possibility of duplicity among departments that utilize social media.

5. Departments that use social media are responsible for complying with applicable federal, state, and county laws, regulations, and policies. This includes adherence to established laws and policies regarding copyright, records retention, Freedom of lnformation Act (FOTA), Open Public Records Act (OPRA), First Amendment,

privacy laws and information security policies established by the County of Monmouth.

6. Wherever possible, links to more information should direct users back to the County's official website for more information, forms, documents or online services necessary to conduct business with the County of Monmouth.

7. Employees representing County government via social media outlets must conduct themselves properly at all times as representatives of the County of Monmouth. Employees that fail to conduct themselves in an appropriate manner shall be subject to revocation of Internet and Intranet privileges, disciplinary action and criminal prosecution in the event of illegal Internet or social media use.

8. Information Technology Services in conjunction with Public Information will monitor content on all social media sites to ensure adherence to the Social Media Policy for appropriate use, message and branding consistent with the goals of the County of Monmouth.

9. Violation of these standards may result in the removal of department pages from social media outlets and revocation of permission to use social media sites. The Public Information Director and/or the Application Development Group retain the authority to remove any information at any time from any County of Monmouth social media site.

10. Information Technology Services reserves the right to stop using social media outlets at any time. Information Technology Services also reserves the right to transition from one social media outlet to another as deemed appropriate.

11. The County will only "follow" other government and nonprofit agencies on social media sites. The county will not link or "follow" to individual accounts, celebrity, political or commercial sites.

12. Information Technology Services will set up the social media accounts. Public Information will be responsible for managing the social media accounts.

APPENDIX F- Website Policy

County of Monmouth Website Policy

To address the essential need for communication with residents and members of the community, the County of Monmouth has established a County Website, known as www.visitmonmouth.com, herein referred to as the County Website. The County of Monmouth recognizes the importance of meeting the growing demand for electronic communication with the public and providing timely information through the County Website.

The Board of Chosen Freeholders and the County Administrator have a vested interest and expectations in deciding the message "spoken" on behalf of the County of Monmouth through the County Website. This policy establishes acceptable practices and guidelines for the use of the County Website.

POLICY

1. All centralized communication for major changes to the County Website must be communicated through the WAG (Website Advisory Group). It is a committee that meets monthly and is comprised of stakeholders. To attend a meeting, please contact the Application Development Group Supervisor of information Technology Services.

2. No third party applications shall be embedded into any web page on the County Website.

3. All third party applications must be approved by Information Technology Services before creating a link on the County Website to those applications.

4. All external links that go outside the County Website must be approved by Information Technology Services before being added to any web page.

5. Any user of the content management system must use it according to how they were trained and use the manual that was provided to them. Information Technology Services reserves the right to pull a user off the content management system if members of the agency are not conducting themselves properly as representatives of the County of Monmouth and/or the agency is improperly using the Content Management System and training has not improved the situation.

6. Any PDF document that is linked on the County Website must be properly titled and will be reviewed by Information Technology Services.

7. All copy content should be approved by Public Information prior to posting on the County Website.

8. Images that are created for the County Website must meet the criteria set forth in the content management system (CMS) manual.

9. Once a request is placed to Information Technology Services for changes or edits to the County Website, the change will follow Application Development Service Level Agreement Policy. This policy is on the County Intranet.