

<p style="text-align: center;">COUNTY OF WASHINGTON</p> <p style="text-align: center;">Pennsylvania</p>	<p style="text-align: center;">HIPAA GENERAL PRIVACY POLICY</p>	<p>Approved Date:</p> <p>PAGE: 1 of 10</p>
---	--	--

POLICY

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the County's ability to use and disclose protected health information (PHI). It is the policy of the County not to use or disclose protected health information except as permitted by law and to adopt safeguards to protect the confidentiality of this health information.

As used in this policy "protected health information" (PHI) shall mean information which is created or received by Washington County departments that relates to an individual's medical information.

SCOPE

The County understands the sensitive nature of protected health information. The County also recognizes that Federal and State laws require that individually identifiable health information must be safeguarded against improper use or disclosure. It shall be the purpose of this policy to provide guidelines for the use and disclosure of protected health information of the County and various departments.

The County desires to fully comply with the HIPAA requirements. Thus, any of the County's workforce who have access to PHI must comply with this Privacy Policy. As to this Policy and the County's more detailed use and disclosure procedures, the term workforce includes individuals who would be considered part of the workforce covered by HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the County, whether or not they are paid by the County. The term "employee" includes all of these types of workers.

The County reserves the right to amend or change this Policy at any time without notice.

USE AND DISCLOSURE OF PHI:

All members of the County's workforce, who have access to PHI, previously described in the Scope section of the Policy and referred to herein as "employees", must comply with this Policy and with the County's detailed use and disclosure procedures set forth below.

The County may not use or disclose PHI except as permitted, or required, under HIPAA. The terms "use" and "disclosure" are defined as follows:

- **Use:** The sharing, employment, application, utilization, examination or analysis of protected health information.

- **Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of health information.

A. ACCESS TO PHI IS LIMITED

Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with the Policy and the detailed use and disclosure procedures.

B. PERMITTED USES AND DISCLOSURES

The County may use or disclose medical information about a participant to facilitate medical treatment or services by providers. For example, it may be disclosed that a participant either has certain coverage, or coverage under a particular plan to expedite services which are being questioned.

Exception: This does not include behavioral health, drug and alcohol, and AIDS/HIV information. Use and disclosure of this type of information requires a signed consent by the participant.

C. NO DISCLOSURE OF PHI

PHI may not be used or disclosed for the payment or operations of the County's "non-health" benefits (e.g. disability, workers compensation, life insurance, etc), unless the participant has provided an authorization for such use or disclosure or is required by applicable state law and particular requirements under HIPAA are met.

D. DISCLOSURES PURSUANT TO AN AUTHORIZATION

PHI may be disclosed for any purpose if an authorization satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

E. BUSINESS ASSOCIATE AGREEMENTS

Business Associate is an entity or person who:

- Performs or assists in performing a function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.) OR
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to protected health information.

F. DISCLOSURES OF DE-IDENTIFIED INFORMATION

The County may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

There are two ways a covered entity can determine that information is de-identified:

- Either by professional statistical analysis
- By removing specific identifiers
 - Names
 - Street address, city, county, ZIP code (except that geographic information may be aggregated by a five-digit ZIP code)
 - All elements of dates (except year)
 - Telephone numbers
 - Fax numbers
 - Electronic mail address
 - Social Security numbers
 - Medical records numbers
 - Health plan beneficiary numbers
 - Account numbers
 - Certificate/license numbers
 - Vehicle identifiers and serial numbers, including license plate numbers
 - Device identifiers and serial numbers
 - Web Universal Resource Locators (URL's)
 - Internet Protocol (IP) address numbers
 - Biometric identifiers, including fingerprints and voiceprints
 - Full-face photographic images and any comparable images
 - Any other unique identifying numbers, characteristic, or code

DEFINITIONS:

Verification: When implementing the procedures noted in this policy, the County shall take reasonable steps to verify the identity and authority of the person or entity requesting access to protected health information. Reasonable verification procedures include, but are not limited to: reviewing an identification badge; a written statement on letterhead; personal knowledge of the requestor.

Minimum Necessary: When implementing the procedures noted in this policy, the County shall make reasonable efforts to ensure that only the minimum amount of information necessary to satisfy the particular purpose of the use or disclosure is provided. Unless the circumstances indicate otherwise, the County shall presume the request from Elected Officials, Directors, Department Heads is for work-related purposes and the minimum amount of information necessary is provided.

The minimum necessary standard does not apply to any of the following:

- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to a valid authorization
- Disclosures made to the Department of Labor (DOL)
- Uses or disclosures required by law
- Uses or disclosures required to comply with HIPAA

All other disclosures must be reviewed on an individual basis with the Human Resources Department to ensure the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Obtaining a consent: The County shall only use or disclose protected health information for the purposes of treatment, payment, or health care operations. All other circumstances require a valid written consent from the individual or his/her legal representative.

Workforce access to medical information: The following classes of the County's workforce shall have access to an employee's medical information, as needed, in order to accomplish their job duties: Elected officials, Directors or designees, Department Heads or designees, the Occupational Safety and Health Coordinator or physicians retained by the County.

RESPONSIBILITIES OF A COVERED ENTITY

A. Personnel Designations – Complaint Procedure

If an employee has any questions about anything discussed in this Notice or about any of the County's privacy practices, or if you have any concerns or complaints, he/she are to contact the Human Resources Office at (724) 228-6738. An employees also has the right to file a written complaint with the Secretary of the U.S. Department of Health and Human Services. A copy of the complaint procedure is to be provided to any participant upon request. See Appendix A.

B. Training

In accordance with the HIPAA regulations the County will train members of its workforce, as needed, on its privacy policies and procedures. The Human Resources Department is charged with developing training schedules and programs so all necessary workforce members receive the appropriate training to permit them to carry out their functions within the County.

All new members of the workforce, or those who are affected by a material change in policies or procedures will be trained within a required reasonable time. All training will be documented. See Appendix B.

C. Safeguards

The County will establish appropriate administrative, technical and physical safeguards to prevent PHI from intentionally and unintentionally being used or disclosed in violation of HIPAA's requirements.

Physical safeguards will include, but not limited to, locking doors and filing cabinets, positioning computers out of non-users visual proximity, and keeping PHI in separate employee folders.

Technical safeguards will be covered in the HIPAA Security Policy.

D. Notice of Privacy Practices

This notice describes how health information about an employee may be used and disclosed and how to obtain access to this information. Please review this section carefully.

The County has the legal duty to safeguard their employees' protected health information. The County will protect the privacy of the health information that is maintained that identifies an employee, whether it deals with the provision of health care or the payment for health care. The County must provide employees with this Notice about its privacy practices. The notice explains how, when and why the County may use and disclose an employee's health information. With some exceptions, the County will avoid using or disclosing any more of an employee's health information than is necessary to accomplish the purpose of the use or disclosure. The County is legally required to follow the privacy practices that are described in this Notice.

The County reserves the right to change the terms of this Notice and our privacy practices at any time. Any changes will apply to any of your health information that is on file. Before an important change to our policies is made, the County will promptly change this Notice and post a new Notice in the Human Resources Department. Employees may also request, at any time, a copy of the Notice of Privacy Practices that is in effect at any given time, from the Human Resources Department.

A. Certain other uses and disclosures are permitted by Federal Law. We may use and disclose your health information without your authorization for the following reasons:

1. When a Disclosure is required by Federal, State or Local Law, in Judicial or Administrative Proceedings or by Law Enforcement.

For example, the County may disclose an employee's protected health information if ordered by a court, or if a law requires that sort of information is to be reported to a government agency or law enforcement authorities, such as in the case of a dog bite, suspected child abuse or a gunshot wound.

2. For Public Health Activities. Under the law, the County needs to report information about certain diseases, and about any deaths, to government agencies that collect that information. With the possible exception of

information concerning mental health disorders and/or treatment, drug and alcohol abuse and/or treatment, and HIV status (for which specific authorization may be required).

3. **For Specific Government Functions.** With the possible exception of information concerning mental health disorders and/or treatment, drug and alcohol abuse and/or treatment, and HIV status (for which specific authorization may be required), the County may disclose the health information of military personnel or veterans where required by the U.S. military authorities. Similarly, the County may also disclose an employee's health information for national security purposes, such as assisting in the investigation of suspected terrorists who may be a threat to our nation.
4. **For Workers' Compensation.** The County may provide an employee's health information as described under the workers' compensation law, if an employee's condition was the result of a workplace injury for which he/she is seeking workers' compensation.
5. **Appointment Reminders and Health-Related Benefits or Services.** Unless an employee tells the County that he/she would prefer not to receive them, the County may use or disclose information to provide an employee with appointment reminders or to alternative programs and treatments.

B. Other Uses and Disclosures require your prior written authorization. In situations other than those categories of uses and disclosures mentioned above, or those disclosures permitted under federal law, the County will ask for written authorization before using or disclosing any protected health information. In addition, the County needs to ask for an employee's specific written authorization to disclose information concerning his/her mental health, drug and alcohol abuse and/or treatment, or HIV status.

If an employee chooses to sign an authorization to disclose any of his/her health information, he/she can later revoke it to stop further uses and disclosures to the extent that we haven't already taken action relying on the authorization, so long as it is revoked in writing. See Appendix C.

- C. **The right to request limits on uses and disclosures of health information.** An employee has the right to ask the County to limit how we use or disclose health information. The County will certainly consider an employee's request, but an employee should know that the County is not required to agree with your request. If the County does not agree to an employee's request, the County will put the limits in writing and will abide by them, except in the case of an emergency. Please note that an employee is not permitted to limit the uses and disclosures that are required or allowed by law.
- D. **The right to choose how the County sends health information or how we contact employees.** An employee has the right to ask that the County contact him/her at an alternate address or telephone number (for example, sending information to a work address instead of a home address) or by

alternate means (for example, via e-mail/mail instead of telephone). The County must agree to an employee's request as long as we can easily do so.

- E. The right to see or to get a copy of protected health information.** In most cases, an employee has the right to look at or get a copy of his/her health information, but he/she must make the request in writing. A request form is available in the Human Resources Office. The County will respond within thirty (30) days after receiving your written request. If the County does not have the health information an employee is requesting, but the County knows who does, the County will tell he/she how to get it. In certain situations, your request may be denied. If the County denies your request, an employee will receive, in writing, the reasons for the denial. In certain circumstances, an employee may have the right to appeal the decision. See Appendix D.

E. Sanctions (See Section 2 of Sanctions)

1. Sanctions shall be imposed within the appropriate sanction ranges upon the finding that any of the following categories of breaches of employee confidentiality and/or violations of information privacy policies had been committed by a workforce member:

- Negligent or unintentional breach of employee confidentiality and/or violation of Privacy Policy Sanction Range A
- Actions demonstrating intent or willfulness to breach employee confidentiality and/or to violate Privacy Policy Sanction Range B
- Breach of employee confidentiality or violation of Privacy Policy, resulting in (or with the intention to result in) pecuniary gain to the workforce member or the County Sanction Range C
- Knowing participation in an action of another that breaches employee confidentiality and/or violates Privacy Policy Sanction Range A
- Participation in intimidating or threatening acts against any individual who exercises any right provided by the Federal HIPAA Privacy Regulations, and/or threatening and/or coercing an individual to waive any right provided by the Federal HIPAA Privacy Regulations Sanction Range B

2. Particular sanctions imposed should fall within the applicable sanction range:

Sanction Range A

- Counseling
- Verbal Warning
- Written Warning
- Suspension without pay
- Termination

Sanction Range B

- Written Warning
- Suspension without pay
- Termination

Sanction Range C

- Suspension without pay
- Termination

All such sanctions imposed shall be consistent with the terms of any applicable collective bargaining agreement.

F. Waiver of Rights

An employee may not be required to waive any of his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits.

The County or any member of its workforce will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his/her rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

G. Documentation

The County's privacy policies and procedures shall be documented and maintained for at least six (6) years in the Human Resources Department. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications, including changes and modifications in regulations. Any changes to policies or procedures must promptly be documented.

When a change in law necessitates a change to the privacy notice, the privacy policy will be promptly revised and made available to employees. Such change is effective only with respect to PHI created or received after the effective date of the notice.

The County shall document certain events and actions (including authorizations, requests for information, sanctions, complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The retention period for such documentation is at least six (6) years.

EMPLOYEE RESPONSIBILITY

HIPAA gives employees the right to access and obtain copies of their protected health information that the County maintains in designated record sets. HIPAA also provides employees the right to request to have their PHI amended. In accordance with the County's privacy procedures, the County will provide access to PHI and will consider requests for amendments that are submitted in writing by employees.

Designated record set is a group of records maintained by or for the County that includes:

- The enrollment or termination of an employee.
- Other protected health information used, in whole or in part, by or for the County to make coverage decisions about an employee.

A. Accounting of Disclosures

An employee has a right to receive an accounting of certain disclosures of his or her own PHI. The County must act on an employee's request for an accounting no later than 60 days after its receipt. If the County is unable to provide the accounting within 60 days, the County may extend the period by 30 days, provided it gives the employee written notice (including the reasons for the delay and the date the information will be provided) within the original 60 day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (and a copy of the written request for disclosure).

The first accounting in any 12 month period shall be provided free of charge. The Human Resources Department may impose reasonable production and mailing costs for subsequent accountings.

B. Requests for alternative communication means or locations

Employees are permitted to request to receive communication of their PHI by alternative means or at alternative locations.

HIPAA does not require the County to honor such requests except as described below:

The County shall accommodate such a request if the employee clearly provided information that the disclosure of all or part of that information could endanger the employee. The Human Resources Department has responsibility for administering requests for confidential communication.

INTERPRETATION AND ADMINISTRATION

Elected Officials, Directors and Department Heads, in conjunction with the Privacy Committee are responsible for overseeing this policy on a daily basis.

The Human Resources Department is responsible for the overall implementation and administration of this policy under the guidance of the County Solicitor.

The Board of Commissioners is responsible for the ultimate authorization and control of this policy.

The Human Resources Department is responsible for the daily administration of this policy.

ADOPTED this 19th day of June, 2003, per minute # 722 .

ATTEST:

Catherine E. Kresh
Catherine E. Kresh, Chief Clerk/
Administrator

COUNTY OF WASHINGTON

John P. Bevec
John P. Bevec, Chairman

Diana L. Irey
Diana L. Irey, Commissioner

J. Bracken Burns, Sr.
J. Bracken Burns, Sr., Commissioner

APPROVED AS TO FORM AND
LEGALITY:

Richard DiSalle
Richard DiSalle
County Solicitor

Michelle Miller Katula
Michelle R. Miller-Kotula
Human Resources Director

APPENDIX A

COMPLAINT PROCEDURE

If an employee believes his/her privacy rights have been violated by a member of the County's workforce, the employee may file a complaint with the Human Resources Department or with the Department of Health and Human Services.

A complaint must be made in writing to the County within 180 days of the alleged prohibited use or disclosure. All complaints should be made to:

**County of Washington
Attn: HIPAA complaint
Human Resources Department
100 West Beau Street
Suite 202
Washington, PA 15301
(724) 228-6738**

The complaint must state the employee's name, date the prohibited action is believed to have taken place, person believed to have committed the prohibited action and means in which the complainant desires to be contacted (i.e. via mail, phone, etc). Communication will only be with the person making the complaint.

The complaint must be signed and dated.

Upon investigation of the complaint, the complainant will be notified of any and all actions, i.e., such as the opportunity to mitigate damage, to resolve the offense, or sanctions performed.

APPENDIX A

PRIVACY COMPLAINT FORM

Employee name _____

Mailing address _____

Telephone number _____

Are you an employee of Washington County?

- Yes
- No

If you answered "No," what is your relationship to the County of Washington (family member of employee, legal representative of employee, etc.)? _____

Please explain your complaint about our privacy practices, providing details as appropriate: (Continue on reverse side, if necessary)

Please provide us with any suggestions as to how we may improve our privacy practices:

Signature of employee _____

Date _____

Appendix B

Privacy Training

Employee name _____

Department _____

Position _____

Date of training _____

Scope of Training _____

Trainer _____

Signature of trainer _____

Date _____

Signature of employee _____

Date _____

APPENDIX C

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Employee name _____

Social Security number _____

Date of Birth _____

1. I authorize the use or disclosure of the above named individual's health information as described below.
2. The following individual or organization is authorized to make the disclosure:

Address: _____

3. The type and amount of information to be used or disclosed is as follows:
(include dates where appropriate)

- _____ Enrollment
- _____ Payment
- _____ Claims adjustment
- _____ Case or medical management records including
 - _____ Problem(s) – list from date _____ to date _____
 - _____ Medication(s) – list from date _____ to date _____
 - _____ Most recent history and physical
 - _____ Most recent discharge summary
 - _____ Laboratory results from date _____ to date _____
 - _____ X-ray and imaging results from date _____ to date _____
 - _____ Consultation reports from (doctor names)
- _____ Entire record from date _____ to date _____
- _____ Other _____

4. I understand that the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental-health services, and treatment for alcohol and drug abuse.

5. This information may be disclosed to and used by the following individuals or organizations:

Address _____
for purpose of: _____

6. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization, I must do so in writing and present my written revocation to the Human Resource Department – Attn: HIPAA complaint. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy. Unless otherwise revoked, this authorization will expire on the following date, event, or condition: **upon separation of employment with Washington County**. If I fail to specify an expiration date, event, or condition, this authorization will expire in six months.
7. I understand that authorizing the disclosure of this health information is voluntary. I can refuse to sign this authorization. I understand that I may inspect or copy the information to be used or disclosed. I understand that any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules. If I have questions about disclosure of my health information, I can contact the Human Resources Department at (724) 228-6738.

Signature of employee _____

Date _____

Signature of witness _____

Date _____

APPENDIX D

REQUEST TO REVIEW OR OBTAIN COPY OF HEALTH INFORMATION

Employee name _____

Address _____

Date of Birth _____

Telephone number _____

Which of the following are you requesting? (Please check all that apply)

- Healthcare/Treatment Information
- Billing information
- Other: _____

Please describe the specific information that you wish to review or obtain a copy of, including the date(s) of the information (date of office visit, treatment, or other health care service):

If you would like a copy of these records, you will need to pay for copying and postage, as allowed by law. Payment will be required prior to the copy being made and sent to you. If you do not wish to pay for a copy of the records, you may make an appointment to come in to at these record(s) in the Human Resources Department of Washington County. Please note that we need at least two (2) full business days to get these records together for you.

Please check at least one of the following:

- I would like for Human Resources to send these records to me.
- I would like to make an appointment to review the records in the Human Resources Department.

Signature of employee _____

Date _____

Summary

This Policy establishes acceptable use guidelines for staff employed by the County of Washington's ("County") Department of Information Technology (IT). This Policy is enforced in addition to policies enumerated in "Information Confidentiality, Privacy, and Security Standards" in the Washington County Employee Handbook and in other formal computer usage policies and procedures documented by the County and/or IT. This Policy is intended to protect the County's computer systems and computer-based information and the rights and privacy of County citizens and employees, as well as IT staff.

This Policy applies to all IT employees and must be signed on the first day of employment prior to obtaining system access as an employee of IT. In addition, all IT employees must also sign the County's "Information Confidentiality, Privacy, and Security Standards" Acknowledgement Form ("Policy Acknowledgement Form"). The signed originals of both this Policy and the Policy Acknowledgement Form will be placed in the IT employee's personnel file, and a copy of the signed Policy and Form should be retained by the IT employee.

Definitions

- **Client:** A County staff member or authorized computer user or a County Department;
- **File:** A single piece or group of manual or electronic-based data or information. Examples are a document, a property record, groups of records or documents, health records, an individual's salary amount, employee address data, etc.

POLICY

Applicable Guidelines:

IT employees are required to abide by all items outlined in this Policy and the County's Policy Acknowledgement Form. In addition to being the guardians/supporters of the County's computer-based resources, IT employees also serve as examples of professionalism for the rest of the County's user community.

Many IT employees have some level of special access to or elevated privileges with the County's information systems. Special access is defined as having the password and privilege to use a special account or file system that provides extended privileges beyond those typically provided to non-IT users. Upon employment with IT and prior to the granting of any County computer access privileges, a IT employee must read and sign the County's "Information Confidentiality, Privacy, and Security Standards" Acknowledgement Form and this Policy as directed by the IT Area Manager to whom he/she reports. By signing this Policy, the IT employee agrees to comply with the items in this Policy for any current special

access or privileges he/she is granted with the County's information systems as well as any future, additional privileges that may be granted to him/her while employed in IT.

Privacy of Client's Data/Information:

During the normal course of their job functions, certain IT employees may view a manual or a file belonging to a client or another IT employee. Examples are when IT employees must view someone's file in the course of helping/supporting them, system trouble-shooting and correction, and system enhancement and implementation projects. Other, more technical examples include IT employees conducting file system and software audits; computer resource usage analysis; system security investigations; investigations into violations of the County computer usage policies; or other system monitoring, analysis, design, programming, data conversion, testing, installation, and troubleshooting activities at the request of the County's Human Resources Director and his/her designees for purposes of investigation.

The Area Manager for each IT employee will inform his/her employees of what access rights/ privileges are allowable for each of them. In all cases, IT employees must hold confidential and keep private computer-based files and information that IT management by policy and/or direction states may not be shared with any other IT employee(s), any other County employee(s), and/or a third party.

When assisting a County's client, IT employees should follow these guidelines:

- Usage, disclosure, and reproduction in full or in part of the client's data/information are allowed only to the extent necessary to perform the work required to assist the client. Emphasis should be placed on restricting disclosure of the data/information to those IT employees who have a defined need for the data to perform their work in assisting the client.
- Reproduction and/or disclosure of a client's data/information to other County departments and/or third parties is not permitted unless written consent is provided to the IT employee by the client or directed to do so by an Area Manager/Supervisor and/or the Director of Human Resources.
- Unless directed otherwise by an Area Manager/Supervisor and/or the Director of Human Resources, IT employees will inquire of the client or someone the client designates as to whether to destroy or return all data/information or copies thereof to them. IT employees will execute any request for return or destruction immediately.

Proprietary Information:

Due to the nature of County services, there are significant occurrences of proprietary and sensitive information stored on/in the County's information systems/computers. This information can include, but is not limited to, personnel and financial information, criminal records, health records, and other sensitive information. Because various IT employees have

I have read and understand this IT Employee Information Systems Information, Confidentiality, Privacy, and Security Standards completely and agree that failure to comply with the Policy constitutes grounds for immediate disciplinary action including but not limited to suspension or termination from employment with the County of Washington.

IT Employee Name - Print

IT Area working in - Print

IT Employee Signature

Date

full access to County systems and data files, they may have access to this proprietary and sensitive information. IT employees are responsible for ensuring that all such proprietary and sensitive information is protected from disclosure or modification. When dealing with sensitive information, IT employees shall use the following guidelines:

- Ensure appropriate measures are in place for protecting sensitive information.
- Will not attempt to access sensitive information or any electronic communications/media for which they have not been given authorization.
- Will not make manual or electronic copies of sensitive information unless specifically permitted by the owner of the information unless directed otherwise by their IT Manager who in turn will receive guidance from Human Resources and/or County management authorized by the Commissioners' office.
- Will not disclose sensitive information to third parties unless directed to do so by Human Resources and/or County management authorized by the Commissioners' office.

Security Investigations:

If the IT Director determines there is probable cause that a violation has occurred, Human Resources Management will be notified of the violation. Human Resources Management will then determine the next steps to be taken. Any investigation will be conducted by County staff as selected by Human Resources and/or County management authorized by the Commissioners' office. The County reserves the right to conduct any investigation and obtain any information contained in County computer systems, manual work files and documentation, or any other areas that are a part of the County necessary to support its investigation.

If a IT employee is requested to participate in an investigation of another County employee or must view an employee's files (after receiving consent) during the normal course of his/her job duties, the IT employee must not disclose any information or details of the investigation about the employee being investigated to any other County employee(s) or person(s) not associated with the County. Information concerning any County employee investigation should only be disclosed to the individual(s) as identified by Human Resources and/or County management authorized by the Commissioners' office and/or to a law enforcement agency.

ADOPTED this 19th day of June, 2003, per minute # 722 .

ATTEST:

COUNTY OF WASHINGTON

Catherine E. Kresh, Chief Clerk/
Administrator

John P. Bevec, Chairman

Diana L. Ireys, Commissioner

J. Bracken Burns, Sr., Commissioner

APPROVED AS TO FORM AND LEGALITY:

Richard DiSalle
County Solicitor

Michelle R. Miller-Kotula
Human Resources Director

Dan Briner
Director of Information Technology