VENANGO COUNTY

PENNSYLVANIA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

COMPLIANCE POLICIES AND PROCEDURES

EFFECTIVE DATE:
APRIL 14, 2003

APPROVAL DATES:
APRIL 2, 2003
April 12, 2010
December 15, 2013

REVISED

JULY 18, 2007
FEBRUARY 10, 2010
JULY 21, 2011
December 1, 2013

VENANGO COUNTY PENNSYLVANIA
HIPAA COMPLIANCE POLICIES AND PROCEDURES

TABLE OF CONTENTS

VENANGO COUNTY PENNSYLVANIA
HIPAA/HITECH COMPLIANCE
POLICIES AND PROCEDURES

EFFECTIVE DATE: 04/14/2003
APPROVAL DATE: 04/02/2003
REVISION DATE: 12/01/2013

I. Overview

The agencies and departments of the government of Venango County, Pennsylvania are participating in compliance with the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191 (hereinafter referred to as "The Act") and the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law as a "Hybrid Covered Entity: Broad Designation." Under this compliance option, although some departments and agencies of this county government will be required to comply with all or at least a substantial portion of the regulations emanating from "The Act", and contained in 45 CFR Subtitle A, Subchapter C and ARRA/HITECH, other agencies/departments shall be exempt due to the nature of the normal business transacted in those agencies or departments.

It is and shall remain the policy of the County of Venango that individual agencies within county government will remain obligated to follow all federal and state laws, policies, procedures, regulations and guidelines governing their particular agency's activities. In any case of conflict between these County Policies and Procedures and state or federal laws, policies, procedures, regulations or guidelines the involved county agency shall obey the more stringent set or combination of requirements.

Agencies and/or departments within the Venango County Government, which are covered under the provisions of "The Act", are those agencies or departments that provide, purchase or coordinate health care to/for the residents of Venango County (physical health, mental health, mental retardation services, substance abuse services or any combination of such services) and shall hereinafter be referred to simply as agencies. Additionally any agency that serves as a "Health Plan" because it provides, administers or pays for the cost of healthcare for residents, employees or retired employees of this county will be governed by "The Act." Finally those administrative agencies that actually pay the invoices for (or bill insurance companies, medical assistance, Value Behavioral Health for) healthcare services, or in some other way actively manage those procedures, will require HIPAA compliance. At this time there are no county agencies that fit the HIPAA guidelines as a Health care Clearinghouse so no policies or procedures emanating from that designation will appear in these policies and procedures.

Specific Venango County Agencies identified as "Covered Agencies" shall include:

- Area Agency on Aging
- Children, Youth and Family Services
- Data Processing
- Early Intervention
- Fiscal
- Human Resources
- Human Services
- Mental Health
- Developmental Services
- Community Support Services / OEO
- Prison
- Substance Abuse
- County Veterans Office

The Venango County Prison, as an agency of Venango County government covered under the HIPAA mandate, has by its nature as a "Correctional Institution" several exemptions built into the HIPAA regulations. These exemptions, as well as the unique services provided by the prison, created the need for a set of policies and procedures exclusive to the prison and its administration. That set of policies and procedures defers to this document (the Venango County Pennsylvania HIPAA Compliance Policies and Procedures) for any HIPAA contingency not covered by the "Venango County Prison HIPAA Compliance Policies and Procedures," as well as for incidents, inquiries, requests or complaints filed by former inmates residing outside of any correctional institution or the lawful custody of a law enforcement official, or by the legal representatives of inmates, involving the use, storage, dissemination, retention or destruction of the inmate's protected health information.

Those agencies of Venango County government not identified, as "Covered" shall be listed in Appendix I along with the rationale used in classifying each as an "Exempt Agency."

Exempt county agencies may still receive and/or store limited amounts of individually identifiable health information for non-healthcare reasons during the normal course of their daily activities. These exempt agencies shall be subject to essentially the same level of security for this protected information as covered agencies unless the information used or stored by those exempt agencies is by law, a matter of public record.

All county employees will receive a level of HIPAA training based upon their designated job function, location and responsibilities. In addition, contract workers will be instructed in the county policies and procedures and will have language added to their contracts identifying them as non-traditional workforce members and identifying their obligations to the county under the HIPAA regulations.

II. VENANGO COUNTY PRIVACY POLICY ON PRIVACY OFFICIALS

HIPAA COMPLIANCE OFFICER

Purpose

45 CFR ss 164.530 (a) (1) Administrative Requirements, states that a covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. Additionally the entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by ss 164.520. Finally, in ss (j) of the aforementioned section the covered entity must document the personnel designations in this section by maintaining a written or electronic record of such action, activity or designation.

Policy

The Commissioners of Venango County shall designate a county employee to serve as the HIPAA Compliance Officer. This employee shall be responsible for the development and implementation of privacy policies and procedures and shall oversee all ongoing activities related to the maintenance of, and adherence to the county's policies and procedures covering the use, and access to, protected health information in compliance with federal and state laws.

The designated Compliance Officer shall have that designation added to his/her personnel record in the Human Resources Department, and his/her name, address, phone number, e-mail address, fax number and office location shall be listed on the "Venango County, Pennsylvania Notice of Privacy Practices" so that any consumer of county provided or funded health care or health plan services will be able to communicate concerns, complaints or questions relative to the security, privacy, disclosure or use of their protected health information.

Compliance Officer Responsibilities

It shall be the responsibility of the compliance officer to:

1. Provide guidance and assistance in the identification, implementation, and maintenance of information privacy policies and procedures in coordination with the administration of the County of Venango and those Venango County agencies providing HIPAA covered functions for the citizens, residents and employees of said county.

2. Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with Venango County's other compliance and operational assessment functions.

3. Work with individual units of county government to ensure that the county has and maintains appropriate private consent and authorization forms, privacy notices and materials reflecting current policies and procedures.

4. Oversee delivery of initial and updated HIPAA/HITECH training to all County employees to the level of their particular responsibility under "the Act" and the county policies and procedures.

5. Coordinate delivery of initial and updated guidance to contractors, business associates and other appropriate third parties.

6. Participate in the development and necessary revisions of "Business Associate Agreements."

7. Work with Management Information Systems (MIS) to establish security and accountability processes for protected health information stored or transmitted by electronic means.

8. Work cooperatively with individual county units to oversee client rights to inspect, amend, and restrict access to protected health information, when appropriate.

9. Establish and administer a process for receiving, documenting, tracking, investigating and taking action, when appropriate, on all complaints concerning the county's privacy policies and procedures in coordination with other similar functions.

10. Ensure compliance with privacy practices and, in cooperation with the Human Resources Department, consistent application of sanctions for failure to comply with privacy policies.

11. Initiate, facilitate and promote activities to foster information privacy awareness throughout county government as well as with contractors and business associates.

12. Work with county personnel involved with the release of protected health information to ensure full coordination and cooperation under the county's policies and procedures.

13. Monitor changes in applicable federal and state privacy laws and advancement in information privacy technologies to ensure county compliance.

14. Cooperate with the Department of Health and Human Services (DHHS), Office for Civil Rights and any compliance auditors or investigators from those or appropriate state agencies in any compliance review or investigation.

15. Other duties as assigned.

Venango County Privacy Review Official

Purpose

45 CFR ss 164.524(a)(4) identifies that "If access (to protected health information) is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity (county) to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section."

Policy

When or if a client is denied access to protected health information pursuant to the above captioned regulations, it shall be the responsibility of the Compliance Officer to contact an appropriately licensed health care professional (who is in no way personally involved with the denial) and ascertain that health care professional's availability to act as the County Review Official

Whenever possible, the healthcare professional in question will be chosen from a list of appropriately credentialed Venango County Employees made available by the Human Resources Department.

In the event of a total lack of available qualified employees, the Compliance Officer will request permission from the office of the Venango County Commissioners to appoint an appropriately licensed health care professional working under contract to one or more Venango County agencies, as an acting County Review Official.

The position of County Review Official will be a temporary appointment on an as needed basis and will be expected to complete the review of the "Denial of Access to Protected Health Information" during their normal working or contracted hours.

Venango County Privacy Review Official Responsibilities

It shall be the responsibility of the Privacy Review Official to:

1. Receive from the Venango County Compliance Officer a copy of "Client Access Denial Forms" along with any supporting documentation.

2. Review the denial process and documents and, if necessary, review the protected health information in question in order to establish the appropriateness of the denial in light of governing legislation and client rights.

3. Send a letter to the complaining client, with a copy to the Compliance Officer, identifying his/her findings either confirming the denial of access or recommending that the client be given access to the file information in question.

Venango County HIPAA Security Officer

The position of the Venango County HIPAA Security Officer shall be the responsibility of the Venango County Management Information Systems Director.

III. VENANGO COUNTY PRIVACY POLICY ON BUSINESS ASSOCIATE AGREEMENTS

Purpose

45CFR ss164.502 (e)(1)(i) Disclosures to Business Associates, states that "A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.

45CFR ss164.502 (e)(1)(ii) The standard does not apply:

> (A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of an individual;
>
> (B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor...

45CFR ss164.502 (e)(2) Documentation. A covered entity must document the satisfactory assurances required by paragraph (e)(1) of this section through a written contract or other written agreement or arrangement with the business associate.

BUSINESS ASSOCIATE OBLIGATIONS:

a) Business Associates is required to implement the same security safeguards and restrictions on uses and disclosures, to protect individually identifiable health information as the Covered Entity. Business Associate is also subject to the same potential civil and criminal liability for breaches as covered entities. Title XIII of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

b) Business Associates must take responsibility for maintaining policies and procedures to ensure full compliance with the following: Title XIII of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") security rules:

- Administrative Safeguards including designating a security official who will be responsible for developing, implementing and evaluating policies to prevent, detect and correct security violations and ensuring that the workforce has appropriate access and training relating to PHI.

- Physical Safeguards to limit physical access to electronic information systems and to address the functionality, accessibility, and movement of workstations utilizing e-PHI.
- Technical Safeguards including limiting the people or software programs who can access e-PHI, putting in place mechanisms to record the activity of systems that contain or use e-PHI, and protecting e-PHI from improper destruction or unauthorized access.
- Business Associates who receive PHI under a Business Associate Agreement will be responsible, along with the Covered Entity, for ensuring that Business Associate Agreements satisfy certain HIPAA privacy rules. Business Associates must also take reasonable steps to cure a breach if they know that a Covered Entity is committing a breach. If such steps are unsuccessful, Business Associates must, if feasible, terminate the arrangement or report the problem to HHS.

c) Limits on Use And Further Disclosure Established By Law. Business Associate must agree that the PHI provided or made available by Covered Entity shall not be further used or disclosed other than as permitted or required by contract or as required by law. 45 CFR §165.404(e)(2)(ii)(A).

d) Appropriate Safeguards. Business Associate must establish and maintain appropriate safeguards to prevent any use or disclosure of PHI other than as provided for by Law and approved contract. 45 CFR §164.504(e)(2)(ii)(B).

e) Reports of Improper Use Or Disclosure. Business Associate must agree that it shall report to [name of Agreement officer for program and Department] within two (2) days of discovery any use or disclosure of PHI not provided for or allowed by Law or contract. 45 CFR §164.504(e)(2)(ii)(C) and shall provide Breach Notification as otherwise required by Title XIII of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

f) Subcontractors and Agents. Business Associate must agree that anytime PHI is provided or made available to any subcontractors or agents, Business Associate shall provide only the minimum necessary PHI for the purpose of the covered transaction and must enter into a subcontract or contract with the subcontractor or agent that contains the same terms, conditions and restrictions on the use and disclosure of PHI as contained in Law and any contract. 45 CFR§ 164.504 (e)(2) (ii)(D).

g) Right of Access to PHI. Business Associate must agree to make available to an individual who is the subject of the PHI the right to access and copy that individual's PHI, at the request of the individual or of the Covered Entity, in the time and manner designated by the Covered Entity. This right of access shall conform with and meet all of the requirements of 45 CFR §164.524 and 45 CFR §164.504(e)(2)(ii)(E).

h) Amendment and Incorporation of Amendments. Business Associate must agree to make any amendments to PHI that have been agreed to by the Covered Entity, at the request of Covered Entity or of the individual, in the time and manner designated by Covered Entity, in accordance with 45 CFR164.526 and 45 CFR §164.504(e)(2)(ii)(F).

i) Provide Accounting. Business Associate must agree to document and make available to Covered Entity or to the individual, any information necessary to provide an accounting of disclosures in accordance with 45 CFR §164.528 and 45 CFR §164.504 (e)(2)(ii)(G), within 30 days of receipt of a request for an accounting, in the manner designated by the Covered Entity.

j) Access to Books and Records. Business Associate must agree to make its internal practices, books, and records relating to the use or disclosure of PHI received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of Health and Human Services or designee for purposes of determining compliance with the HIPAA Privacy Regulations. 45 CFR §164.504(e)(2)(ii)(H).

k) Return or Destruction of PHI. At termination of any contractual arrangement, Business Associate must agree to return or destroy all PHI received from, or created or received by Business Associate on behalf of Covered Entity. Business Associate must agree not to retain any copies of the PHI after termination of contract. If return or destruction of the PHI is not feasible, Business Associate must agree to extend the protections of the contract to limit any further use or disclosure until such time as the PHI may be returned or destroyed. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed. 45 CFR §164.504(e)(2)(ii)(I).

l) Mitigation Procedures. Business Associate must agree to establish and to provide to the Program and Department upon request, procedures for mitigating, to the maximum extent practicable, any harmful effect from the use or disclosure of PHI in a manner contrary to this Appendix or the HIPAA Privacy Regulations. 45 CFR §164.530(f). Business Associate must further agree to mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the contract.

m) Sanction Procedures. Business Associate must agree that it will develop and implement a system of sanctions for any employee, subcontractor or agent who violates this Appendix or the HIPAA Privacy Regulations. 45 CFR §164.530(e)(1).

n) Grounds for Breach. Any non-compliance by Business Associate with the contract or the HIPAA Privacy Regulations will automatically be considered to be grounds for breach pursuant to the underlying agreement, if Business Associate knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance. Business Associate must further acknowledge that it is subject to the same potential civil and criminal liability for breaches as covered entities. Title XIII of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

o) Termination by Covered Entity. Business Associate must authorizes termination of the underlying contract by the Covered Entity if the Covered Entity determines, in its sole discretion, that the Business Associate has violated a material term of the contract or appropriate law.

OBLIGATIONS OF COVERED ENTITY:

a) Provision of Notice of Privacy Practices. Covered Entity must provide Covered Entity produces in accordance with 45 CFR §164.520, as well as changes to such notice.

b) Permissions. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individual to use or disclose PHI, if such change affect Business Associate's permitted or required uses and disclosures.

c) Restrictions. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR §164.522.

Policy

It is the policy of Venango County, Pennsylvania to include language guaranteeing the appropriate safeguarding of protected health information in all contracts for service between county agencies performing covered functions and business partners who must utilize said information in the performance of their contracted duties.

Services and individuals included in this policy shall include but not be limited to: legal services, consulting services, accounting services, management services, accreditation services, financial services, medical records services, temporary employment agencies, interns, managed care organizations, transcriptionists, computer software vendors, computer hardware vendors, payroll services, banks with trust accounts, insurance consultants, carriers & brokers, collection agencies, peer review or quality assurance experts or consultants, landlords, medical staff members, security agencies, marketing firms, research agencies,.

Contracts between the County of Venango and providers of general services that would include services for, or in proximity to, county agencies performing covered functions shall include language guaranteeing the appropriate safeguarding of protected health information. Services included in this paragraph shall include but not be limited to; custodial, garbage collection, building repair or maintenance, and repair of telephones, FAX machines, computers, photocopiers or shredders.

Providers of services, who work at the convenience of county agencies or on an "as needed" basis but who do not have a county contract per se, shall be expected to sign an agreement guaranteeing the appropriate safeguarding of protected health information prior to performing any services in agencies performing covered functions or in buildings where these agencies are located. This would include, but not be limited to: Boards of Directors, grievance or complaint committee members who are not employed by the county, union representatives telephone, FAX, computer and photocopier repairmen as well as maintenance, custodial and garbage collection workers for offices located in non-county owned buildings.

Copies of all Business Associate Agreements shall be maintained for a minimum of six years after the termination of their effective date.

IV. VENANGO COUNTY PRIVACY POLICIES ON NOTICE OF PRIVACY PRACTICES

Purpose

45CFR ss 164.520 (a) (1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans.

(3) Exception for inmates.

Policy

It is the policy of The County of Venango to provide our clients with written notice of our privacy practices, including among other things a statement of each client's rights as set out by the HIPAA Privacy Regulations. The written Notice of Privacy Practices adopted by this Organization shall be distributed to each client or their legal representative pursuant to the guidelines set forth below:

1. Each client and/or their legal representative shall be provided a copy of the most current Notice of Privacy Practices at the time of their initial [visit/admission/intake into one or more of our programs], unless impracticable in the case of emergency treatment. In the case of emergency treatment, it shall be the responsibility of caseworker to provide this notice and take the further steps described below, at the first opportunity available.

2. Each client or their legal representative shall be asked to sign an Acknowledgement of Receipt of Notice of Privacy Practices to acknowledge that they received a copy of the Notice of Privacy Practices. If the client or legal representative is unwilling or unable to acknowledge receipt in this way, the workforce member shall document his/her effort to obtain this acknowledgement and the refusal or the reason the client or legal representative did not sign the acknowledgement on the Acknowledgement form with the date and the workforce member's signature.

3. The acknowledgement form or the documentation of refusal or inability to sign shall be immediately placed in the client's chart in the administrative section and a colored dot with the date of provision of the Notice shall be placed on the upper left corner of the front of the jacket of the client's chart indicating provision of the Notice of Privacy Practices.

4. At each treatment visit of each client after April 14, 2003, when pulling the chart for treatment purposes, the caseworker shall check the front of the chart jacket for the existence of a colored dot. If there is no colored dot indicating the prior provision of the Notice of Privacy Practices and there exists no indication of provision of the Notice of Privacy Practices within the chart, it shall be the responsibility of the case worker to provide a copy of the Notice of Privacy Practices and attempt to obtain the written acknowledgement of receipt of the notice, under the guidelines set forth above.

5. The Notice of Privacy Practices shall also be posted upon a bulletin board or wall visible to waiting areas for all county agencies that provide covered functions, as well as upon the Venango County Web site and the Web site of any county agency that provides covered functions.

V. VENANGO COUNTY PRIVACY POLICIES ON VERIFICATION OF IDENTIFICATION

Purpose

45CFR ss 164.514 (h)(1) Requires that, prior to any disclosure, a covered entity verify the identity of the person requesting protected health information and the authority of that person to have access to the protected health information.

Policy

It is the policy of the County of Venango to ensure the security and privacy of each client's health information, by protecting such information from unauthorized disclosure.

Any workforce member processing a client health information request of any sort shall take appropriate steps to verify the identity and/or authority of any requestor of client health or billing information (including demographic information) by any person not known to the workforce member, or by any person whose authority to obtain such information is not certain. Workforce members should refer to the guidelines for verifying identity and/or authority set forth below:

1. Information authorized by the client, or by the client's legal representative, to be disclosed, may only be disclosed to the person or business entity specifically named on the signed Authorization form.

2. Where the identity of the requestor is unknown to the workforce member, the workforce member should request proof of identification from the requestor. If the requestor is a workforce member or agent of an unknown business entity, including but not limited to health care providers and/or law firms authorized by the client to receive such information, it is sufficient for the County workforce member to mail the requested information to the business' address, as listed in the telephone directory or on the business' website, or to otherwise verify the identity of the business entity.

3. If the signature upon an Authorization form does not appear to be that of the client or the client's legal representative, the client or the client's legal representative should be contacted by telephone, or otherwise, for confirmation.

4. Where an Authorization has been signed by the legal representative of the client, the workforce member processing the request should verify that a copy of the legal representative's authority (as indicated in the chart below) has been attached to the Authorization or is otherwise maintained in the client's chart.

Guardian of an Incapacitated Client:	Guardianship Order
Legal Guardian of Minor (Non-Parent):	Guardianship Order
Attorney-in-Fact of Client:	Power of Attorney
Executor/Executrix of Deceased Client's Estate:	Letters Testamentary or Short Certificate (copy of Will is not sufficient)
Administrator/Administratrix of Deceased Client's Estate:	Letters of Administration or Short Certificate

5. The workforce member processing a health information request is responsible for assuring that any documentation, statements or representations are obtained from the requestor, if required as a condition of the disclosure pursuant to the applicable Authorization, or by State or federal law.

6. Wherever possible, all warrants, court orders, or other legal process issued by a judge, grand jury or administrative judge, and any subpoenas of an unusual nature, shall be reviewed by the Compliance Officer prior to processing.

7. If reasonable under the circumstances, the County will rely upon any of the following as verification of the identity of a public official or person acting on behalf of a public official:

    (a) An agency identification badge, official credentials, or other proof of government status;

    (b) A written request on the appropriate government letterhead;

    (c) A written statement on the appropriate government letterhead that the person to whom the disclosure is to be made is acting under the government's authority; or

    (d) A contract for services, memorandum of understanding, or purchase order that establishes that the person is acting on behalf of a public official.

    Such verification shall be charted and/or a copy of such verification shall be placed in the chart with documentation of the request.

All health information requests of any sort (including requests for demographic or billing information) shall be documented in the client's chart, with a copy of all applicable documents.

VI. COUNTY OF VENANGO PRIVACY POLICY ON THE "MINIMUM NECESSARY STANDARD"

Purpose

45 CFR ss 164.502 (b) Identifies that when using or disclosing protected health information, or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Policy

It is the policy of The County of Venango to ensure that its workforce members only request, use and/or disclose the minimum amount of a client's individually identifiable health information that is reasonably necessary to achieve the intended purpose of the permitted use or disclosure. This Policy does **not** apply to:

- **Disclosures to, or requests or use by, a health care provider for purposes of treatment;**
- **Disclosures to the client, the client's legal representative, or anyone designated to receive such information in an Authorization form signed by the client or the client's legal representative; or**
- **Disclosures required to be made to the Secretary of the Department of Health and Human Services or its agent.**

1. Each covered county agency shall determine what information that it shall deem to be "Minimum Necessary" to be requested, used and disclosed for routine and recurring treatment or billing activities under contractual arrangements with outside treatment or service providers.

   It shall be the responsibility of the director or supervisor of each covered county agency to instruct their workforce members on the particular types and levels of protected health information that they may request or have access to, based upon their specific job functions. It shall further be the covered agency director or supervisor's responsibility to identify which workforce members may disclose protected health information, and specifically what types and amounts of information that they may disclose based upon the appropriate sections of this document.

   Covered agency directors or supervisors shall document the types and levels of information that each of their workforce members or each job title of their workforce members may request, have access to, or disclose. This documentation shall be updated as appropriate, retained by the agency director or supervisor and a copy sent to the county Compliance Officer upon his/her request (such as during investigations of complaints of inappropriate disclosure or breach of confidentiality/security.)

2. For all other requests, uses and/or disclosures of individually identifiable health information by any member of the County workforce, the following criteria shall be applied prior to making such a request, use or disclosure:

   - There must be a determination that the information to be used or disclosed does not include any information beyond that which is specifically requested, in terms of scope of time, type of information, etc.;

- There must be a determination that the information to be requested, used or disclosed does not include any information beyond what a reasonable person would believe is needed for the stated purpose; and

- There must be a determination that the amount and type of information to be requested, used or disclosed cannot be reduced or limited any further without adversely affecting the ability to use the information for its stated purpose.

3. Each member of a Venango County covered entity workforce may only access the minimum information that is necessary to perform that workforce member's particular job functions, as defined in his/her job description.

4. At no time shall any workforce member review any portion of any client's chart or billing information that is not required by his/her specific job duties.

De-Identified Information

Health information that does not identify an individual, and to which there is not reasonable basis to believe that information can be used to identify any individual, is not subject to the privacy requirements and may be disclosed.

There are two mechanisms under which a covered agency may determine that health information is not individually identifiable:

1. A person with appropriate knowledge and expertise, applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines and documents that the risk is "very small" that the information could be used to identify an individual; or

2. All identifiers are removed from the information regarding the individual, relatives, employers or household members.

VII. COUNTY OF VENANGO PRIVACY POLICY ON USES AND/OR DISCLOSURES OF HEALTH INFORMATION

Purpose

45 CFR SS 164.506, 164.508, 164.510 and 164.512 prescribe when a covered entity, including the County of Venango, may use or disclose protected health information.

Policy

The County of Venango, and particularly those county agencies that perform covered functions, will limit use and disclosures to those permitted or required by the relevant privacy provisions of this policy and procedure statement and/or any applicable federal or state law.

Permitted Uses and Disclosures (General Rules)

Under the privacy regulations a county covered agency may use or disclose protected health information:

(1) When the disclosure is to the individual who is the subject of the information or a designated personal representative.

(2) To carry out treatment, payment or health care operations, except with respect to psychotherapy notes. Each county agency providing covered functions will attempt to obtain consent for such use or disclosure when the individual commences receipt of services or benefits. If necessary, the agency may condition the provision of services or benefits upon the individual's consent.

(3) When the agency receives a valid authorization for releases that are for other than treatment, payment or health care operations.

(4) When use or disclosure is permitted without the need for consent, authorization or the opportunity to agree or object.

(5) Where the agency is sharing the information with a relative, close friend or other person identified by the individual. This can only be accomplished with the agreement of the individual expressed either on a written authorization or orally unless the situation is an emergency or the individual lacks the capacity to agree or object.

A Venango County agency providing covered health care functions must disclose protected health information:

(1) When an individual requests an accounting of the disclosures of his/her protected health information or asks to inspect and/or copy that information.

(2) When required by the Secretary of Health and Human Services to investigate or determine the agency's or the county's compliance with the privacy regulations.

A Venango County agency providing covered functions may, without consent, use or disclose protected health information to carry out treatment, payment or health care operations if:

(a) The covered health care agency has an indirect treatment relationship with the individual; or

(b) The covered health care agency created or received the protected health information in the course of providing health care to an individual who is an inmate.

A county agency providing covered health care may, without prior consent to carry out treatment, payment or health care operations, use or disclose protected health information that was created or received:

(a) In emergency treatment situations, if a member of the provider agency attempts to obtain the proper consent as soon as reasonably practicable after the delivery of the emergency treatment;

(b) If the covered health care provider is required by law to treat the individual, and the provider attempts to obtain such consent but is unable to obtain such consent; or

(c) If the covered provider attempts to obtain such consent from the individual but is unable to obtain the consent due to substantial communications barriers with the individual and the provider determines, in the exercise of professional judgment that the individual's consent to receive treatment is clearly inferred from the circumstances.

A covered county agency that fails to obtain a valid consent in accordance with the above paragraphs must document the attempt to obtain the consent and the reason that the consent was not obtained.

A consent obtained by one county covered agency, under this section, is not effective to permit any other covered entity to use or disclose protected health information.

Consent Content Requirements

Consent under this section must be in plain language and:

(1) Inform the individual that protected health information may be used and disclosed to carry out treatment, payment or health care operations;

(2) Refer the individual to the "Notice of Privacy Practices" for a more complete description of such uses and disclosures and state that the individual has the right to review that notice prior to signing the consent;

(3) As Venango County has reserved the right to change its privacy practices in accordance with **ss 164.520 (b)(1)(v)(C)** of the Final Privacy Rule, the consent must state that the terms of its notice may change and describe how the individual may obtain a revised notice;

(4) State that:

(i) The individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment or health care operations;

(ii) The covered entity is not required to agree to requested restrictions; and

(iii) If the covered entity agrees to a requested restriction, the restriction is binding on the covered entity;

(5) State that the individual has the right to revoke the consent in writing, except to the extent that the covered entity has taken action in reliance thereon; and

(6) Be signed by the individual and dated.

Defective Consents

There is no consent under this section, if the document submitted has any of the following defects:
(1) The consent lacks an element required under the "Content Requirements" section of this policy; or
(2) The consent has been revoked in accordance with the "General Requirements" section of this policy.

Resolution of Conflicting Consents and Authorizations

(1) If a Venango County covered agency has obtained a consent under this section and receives any other authorization or written legal permission from the individual for a disclosure of protected health information to carry out treatment, payment or health care operations, the agency may disclose such protected health information only in accordance with the more restrictive consent, authorization or other written legal permission from the individual.

(2) A covered agency may attempt to resolve a conflict between consent and an authorization or other written permission from the individual described in this section by:

(i) Obtaining a new consent from the individual for the disclosure; or

(ii) Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered agency must document the individual's preference and may only disclose protected health information in accordance with that preference.

Uses and Disclosures of Protected Health Information for which an Authorization is required

45 CFR ss 164.508 (a) states that except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with the authorization.

It shall be the policy of Venango County that those agencies performing covered functions, with the exception of the county prison, shall obtain or receive a valid authorization prior to any use or disclosure of information protected by this Act.

Psychotherapy Notes

Any agency of Venango County providing covered functions shall obtain an authorization for any use or disclosure of psychotherapy notes, **except:**

To carry out treatment, payment or health care operations, consistent with consent requirements of 45 CFR ss 164.506:

(A) Use by originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual.

Valid Authorizations

A valid authorization is a document that contains the following elements:

(1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosures;

(3) The name of other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

(4) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

(5) A statement or the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

(6) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosures by the recipient and no longer be protected by this rule;

(7) Signature of the individual and date;

(8) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and

(9) The authorization must be written in plain language.

A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

Defective Authorizations

An authorization is not valid if:

(1) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(2) The authorization has not been filled out completely;

(3) The authorization is known by the covered entity to have been revoked;

(4) The authorization lacks a required element;

(5) Any material information in the authorization is known by the covered entity to be false.

Combined Authorizations

An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except:

(1) An authorization for the use or disclosure of protected health information created for research that includes treatment of the individual may be combined;

(2) An authorization for use or disclosure of psychotherapy notes may only be combined with another authorization for the use or disclosure of psychotherapy notes.

Conditioning of Authorizations

No Venango County covered entity, except the county prison, shall condition the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except:

(1) The health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for use or disclosure of psychotherapy notes;

(2) The health plan may condition payment of a claim for specified benefits upon provision of an authorization if:

(A) The disclosure is necessary to determine payment of such claim; and

(B) The authorization is not for a use or disclosure of psychotherapy notes;

(3) The covered county entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of protected health information to such third party.

Revocation of Authorization

An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(1) The covered county agency has taken action in reliance thereon; or

(2) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

Documentation

It shall be Venango County Policy that any signed authorizations for the use or disclosure of protected health information shall be retained by the covered county agency for a period of not less than seven years from the date of its creation or the date when it was last in effect, whichever is later.

Authorizations for County Covered Agency Internal Uses and Disclosures, or for Covered County Agencies to receive Protected Health Information from another Covered Entity

If an authorization is requested by a covered county agency for its own use or disclosure of protected health information that it maintains, or to receive protected health information from another covered entity, the agency must comply with the following elements:

(1) The authorization must contain all of the elements of a Valid Authorization identified in this document and:

(i) If applicable, a statement that the covered agency will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;

(ii) A description of each purpose of the requested use or disclosure;

(iii) A statement that the individual may:

(A) Inspect or copy the protected health information to be used or disclosed; and

(B) Refuse to sign the authorization; and

(iv) If the use or disclosure of the requested information will result in direct or indirect remuneration to the county covered entity from a third party, a statement that such remuneration will result.

(2) A covered county agency must provide the individual with a copy of the signed authorization.

Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object

45 CFR ss 164.510 states that a covered entity may use or disclose protected health information without the written consent or authorization, previously described, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure.

It shall be the policy of the County of Venango to permit county agencies performing covered functions to:

(1) Disclose to a family member or other relative or close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

(2) A covered agency may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

If the individual is present for, or otherwise available prior to a use or disclosure as previously described and has the capacity to make health care decisions, the agency may use or disclose the protected health information if it:

(1) Obtains the individual's agreement;

(2) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(3) Reasonably infers from the circumstances, based upon the exercise of professional judgment that the individual does not object to the disclosure.

If the individual is not present for, or the opportunity to agree or object to the use of disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the agency may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the individual's health care. A covered agency may use professional judgment and experience with common practices in allowing a person sufficient information to act on behalf of the individual to pick up prescriptions or medical supplies, arrange transportation to or from appointments or other similar activities.

Disaster Relief Purposes

A covered county agency may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted in the previous sections if the agency determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is not required

45 CFR ss 164.512 States that a covered entity may use or disclose protected health information without the written consent or authorization of the individual as described in ss 164.506 and 164.508, respectively, or the opportunity for the individual to agree or object as described in ss 164.510, in the situations covered by the applicable requirements of this section.

It shall be the policy of the County of Venango to permit covered agencies to use or disclose protected health information without the individual's consent, authorization, or the opportunity to agree or object in the following circumstances:

(1) Uses and disclosures required by law

(2) Uses and disclosures for public health activities, for example, cancer and trauma registries, the FDA, etc.

(3) Disclosures about victims of abuse, neglect or domestic violence which are required by law.

(4) Uses and disclosures for health oversight activities authorized by law.

(5) Disclosures for judicial or administrative proceedings.

(6) Disclosures for law enforcement purpose.

(7) Uses and disclosures about decedents to coroners, medical examiners and funeral directors.

(8) Uses and disclosures for cadaveric organ, eye or tissue donation.

(9) Uses and disclosures to avert a serious threat to health or safety.

(10) Uses and disclosures for specialized government functions, including military and veterans activities.

(11) Disclosures for workers' compensation.

If there is some question on the part of the county agency director as to whether a use or disclosure does or does not require consent, authorization or an opportunity to agree or object, the agency office should seek clarification from the County Compliance Officer.

VIII. COUNTY OF VENANGO PRIVACY POLICY ON CLIENT REQUESTS FOR ACCESS TO PROTECTED HEALTH INFORMATION

Purpose

45 CFR ss 164.524 Gives an individual the right to access, inspect and obtain a copy of protected health information in a "Designated Record Set" (the non-duplicative collection of records regarding individuals applied by covered entities in the decision making process) for as long as the information is maintained in the designated record set.

POLICY

It is the policy of The County of Venango County to provide for an appropriate level of access to an individual client's own private health information maintained within a designated record set, consisting of mental health, medical and billing records prepared by, or on behalf of, Venango County covered agencies. [The term "designated record set" shall exclude any records prepared and maintained by another health care provider, unless a treating physician within this Organization documents his/her intention to incorporate such records as a part of this Organization's designated record set.]

It shall be the duty of each Venango County covered agency's Compliance Officer, or in the absence of an agency Compliance Officer the county Compliance Officer, to receive and process all client requests for access pursuant to the procedure set forth below and the federal privacy regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Procedure:

1. All client requests for access to the client's own health information shall be made in writing and signed by the client, or the client's legal representative, on the form entitled "Client Request to Review or Obtain Copy of Health Information." The blank forms shall be available from the county Compliance Officer and distributed upon request by the secretary, receptionist, caseworker and/or Compliance Officer in each agency.

2. Upon receipt of the request, the agency Compliance Officer shall document receipt of the request, upon the Client Request form by indicating the date received. The Client Request form and any corresponding forms shall thereafter be maintained as a part of the client's chart.

3. All processing of client requests for access shall be completed within thirty (30) days of receipt, unless the designated record set is maintained offsite. In the case of offsite records, the processing of the request shall be completed within a total of sixty (60) days, with a written explanation of the reason for the delay and the date by which the processing will be completed, being sent to the client.

4. Whenever access is permitted, it shall be provided in the form requested by the client, if readily producible in that form; if not, then it shall be provided in a readable hard copy form. Access, if appropriate, shall be provided in the manner requested by the client, whether by mailing a copy to the client's stated address, by allowing review of the record(s) by appointment at the office of the covered county agency or by electronic transmission of the designated record set to the client if the records are maintained in electronic format and the client has the appropriate equipment to receive and translate the data from encrypted to readable format. Prior to mailing a copy of the requested record(s) to the client, if that is the chosen format, the agency Compliance Officer shall compute and obtain payment from client for all copying and postage charges permitted by law, and document the same upon the Client Request form. If unable or unwilling to pay such charges, the client shall be permitted to schedule an appointment to review the requested record(s) at the agency office. Confirmation of the grant of access and the date(s) upon which copies of the requested record(s) were mailed, transmitted electronically and/or were reviewed by the client shall be documented by agency Compliance Officer upon the Client Request form.

5. In the case of any denial of a client's request for access to his/her own health information, the agency Compliance Officer shall complete and mail to the client the form entitled "Notice of Denial of Client Request to Review or Obtain Copy of Health Information," maintaining a copy of this form in the client's chart and documenting the mailing of this form upon the Client Request form.

6. Non-reviewable grounds for denial of access under the HIPAA privacy regulations include:

    (a) No right to access psychotherapy notes;
    (b) No right to access information compiled in reasonable anticipation of civil, criminal or administrative proceedings;
    (c) No right to access information protected under the Clinical Laboratory Improvements Amendments of 1988 or corresponding regulations;
    (d) The direction to deny access to an inmate, made by the correctional facility in which the client is incarcerated;
    (e) The record(s) requested are subject to the federal Privacy Act, 5 U.S.C. §552a.
    (f) The information requested was obtained from someone other than a health care provider under a promise of confidentiality and access would likely reveal the source of the information.
    (g) The client agreed to a temporary denial of access to this information by consenting to participate in a research study in which treatment is being provided; and
    (h) The Organization does not maintain the requested record(s), in which case, [title of person/department] must tell the client where to direct his/her request, if known.

7. Any licensed health care professional within the covered county agency who is involved with the treatment and/or care of the client, may indicate the need to deny access to any portion or all of a record within the designated record set, for any one of the reasons set forth below, by placing in the pertinent portion of the chart a readily visible [red flag, marked with the professional's name or initials] to indicate that client access to the record shall not be granted without the express permission of that licensed health care professional. Such reviewable grounds for denial of access include:

(a) A determination has been made, using professional judgment, that access to the information requested is reasonably likely to endanger the life or physical safety of the client or another;

(b) A determination has been made, using professional judgment, that access to the information requested is reasonably likely to cause substantial harm to a non-healthcare provider referenced within the record(s); or

(c) A determination has been made, using professional judgment, that access to the information requested by the client's legal representative is reasonably likely to cause substantial harm to the client or another person.

Prior to the granting of client access to any record, the agency Compliance Officer shall thoroughly inspect all requested record(s) for the placement of a [red flag] for access denial, and shall discuss the continued validity of any such [red flags] with the treating professional. Access to such portions of the designated record set shall not be granted without the express authorization of the treating professional who noted the denial by placement of the [red flag] upon the chart.

8. Written requests for review of such reviewable denials of access are to be made by the client by signing and dating the statement at the bottom of the Notice of Denial form, and returning the form to the Venango County Compliance Officer. Upon receipt of the request for a review of such a denial, the date received shall be documented upon the original Client Request form.

9. Upon receipt of a request for review of a reviewable denial of access, the Venango County Compliance Officer shall immediately designate a reviewing official who shall be a licensed health care professional who did not participate in any way in the making of the underlying access denial decision. [If the reviewing official is not a member of the workforce of the agency, the agency shall have the designated reviewing official sign an appropriate confidentiality agreement pursuant to the requirements of the HIPAA privacy regulations.]

10. The reviewing official shall immediately be granted access to any portion of the chart and/or other record(s) deemed necessary to make a proper assessment and determination of whether the underlying access denial was proper. Any treating professional involved in the underlying decision shall cooperate in the reviewing official's investigation.

11. The designated reviewing official shall reach a prompt decision upon whether the access denial was proper, but in any case no later than thirty (30) days from receipt of the appeal, and shall mail a letter stating the decision to the client, providing a copy to the agency for its records. Upon receipt of this determination letter, the agency Compliance Officer shall document its date upon the original Client Request form. The decision of the reviewing official shall be binding upon the agency, and, if awarded by the reviewing official, access shall be provided to the client in the manner requested as soon as reasonably possible.

12. The original request form, as well as copies of any denial forms and the reviewing official's determination letter shall be placed in the client's chart, outside of the designated record set, with a copy sent to the county Compliance Officer.

IX. COUNTY OF VENANGO PRIVACY POLICY ON CLIENT REQUESTS FOR ACCOUNTING OF DISCLOSURES

Purpose

45 CFR ss 164.528 States those individuals have a right to receive an accounting of instances when protected health information about them is disclosed by a covered entity. The American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) requires an accounting for instances when health information is released for the purposes of Treatment, Payment for treatment or the operation of the agency for those agencies that acquire Electronic Health Records (EHR) after 01/01/09. The County of Venango has developed policies and procedures to address the accounting of instances when protected health information has been used or disclosed.

POLICY

It is the policy of the County of Venango to guarantee the right of our clients to obtain an accounting of disclosures of their health information, by covered county agencies and/or their business associates, pursuant to the requirements of the HIPAA Privacy Regulations. In order to be able to account for disclosures under these regulations, it is the policy of the County of Venango that workforce members document within the client's chart upon a unique "Disclosure Sheet" the following information about each disclosure of health information: (a) the date of the disclosure, (b) the name and address of the recipient of the information, (c) a brief description of the information disclosed, and (d) the general purpose of the disclosure of health information. Copies of all authorizations and/or other written requests for disclosures shall be maintained within the client's chart. Documentation of the following types of disclosures is not required:

A. Disclosures to carry out treatment, payment, and/or health care operations of the Organization unless the agency has acquired EHRs after 01/01/09;
B. Disclosures of health information to the client or to the client's legal representative;
C. Disclosures made pursuant to an Authorization signed by the client or the client's legal representative;
D. Disclosures permitted under the HIPAA Privacy Regulations to be made to family members or other persons involved in the client's care (and/or payment for care) and/or to family members or other persons for notification purposes;
E. Disclosures for national security or government intelligence purposes;
F. Disclosures to correctional institutions and/or law enforcement officials, where the client, at the time, was in custody;
G. Disclosures occurring prior to April 14, 2003.

It shall be the duty of the particular county agency privacy person to process all client requests for accountings of disclosures of that client's health information, and to prepare a complete accounting under the HIPAA Privacy Regulations and the guidelines set forth below:

1. A client's request for an accounting shall be made in writing on the Client Request for Accounting of Disclosures form, blank copies of which are to be available from the county Compliance Officer or on regular white paper. Forms must be filled out completely, and signed by the client or the client's legal representative and must include the name of the client, the dates of the disclosure and the name of the agency who has disclosed the protected health information.

2. A client does not have the right to receive an accounting of any disclosures made prior to April 14, 2003, or made more than six (6) years prior to the date of the Request or disclosures for TPO (Treatment, Payment, or Operation) prior to January 1, 2009 if the agency has acquired Electronic Health Records after that date.

3. Upon receipt of the Request, the recipient of the Request shall document the date of its receipt upon the request form and immediately forward the Request to the covered agency or county Compliance Officer.

4. Each Request for Accounting shall be processed, with an accounting being prepared and sent to the client or legal representative, within sixty (60) days of the date of the agency's receipt of the Request, absent extenuating circumstances. Under extenuating circumstances only, the agency Compliance Officer may extend this deadline by no more than an additional thirty (30) days, so long as a letter explaining the reason for the delay and the date that the requestor can expect the accounting to be completed, is sent to the requestor prior to the expiration of the usual sixty (60) day deadline.

5. Each client has the right to one accounting within each calendar year, free of charge. The cost of each additional accounting for that client within the same calendar year shall be $ 20.00, which is based upon the cost of preparing such an accounting. Whenever this charge is applicable to a Request for Accounting, the requestor shall be notified of this charge in writing, and no such Request shall be processed further until payment has been made. Documentation of this notification of the charge shall be made upon the request document.

6. Upon receiving the Request, the agency director shall review the client's chart for documentation of disclosures (other than the types described above) for which an accounting may be prepared. The agency Compliance Officer shall contact each business associate to whom protected health information of the client has been disclosed; a list of all disclosures made during the relevant period (other than the types described above) by each such business associate shall be obtained from that business associate.

A written accounting shall be prepared for the client or the client's legal representative listing the following information about each disclosure of health information by the covered agency and/or its business associates: (a) the date, (b) the name and address of the recipient of the information, (c) a general description of the information disclosed, and (d) the general purpose of the disclosure.

7. Copies of the client's Request for Accounting and the written accounting shall be maintained within the client's chart outside of the designated record set, and a copy forwarded to the county Compliance Officer.

X. COUNTY OF VENANGO PRIVACY POLICY ON PRIVACY COMPLAINTS

Purpose

45 CFR ss 164.530(d) Requires covered entities to provide a process for individuals to make complaints to the covered entity concerning its privacy policies and procedures, its compliance with those policies and procedures, breaches of confidentiality or with the HIPAA privacy rule itself. The covered entity is also required to document all complaints received and their disposition.

Policy

It is the policy of The County of Venango to provide our clients with a process by which they may complain and/or make suggestions or other comments about our privacy policies and procedures and our compliance with the requirements of the HIPAA Privacy Regulations.

Venango County covered agencies will in no way discriminate against or take any form of retaliatory action against, any individual for exercising his/her right to file a complaint pursuant to this process, for exercising any other right described in the HIPAA Privacy Regulations, for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, or for assisting in any way with any investigation, compliance review, proceeding or hearing under the HIPAA Privacy Regulations.

Venango County covered agencies will never require any individual to waive his/her right to file a complaint pursuant to this process, or any other right described in the HIPAA Privacy Regulations, as a condition for treatment.

Procedure

It shall be the duty of the Venango County Compliance Officer, or the individual covered agency Compliance Officer (if one exists), to receive and to process all client complaints, and to respond to clients' requests for information about the Venango County or individual agency's privacy practices, under the guidelines set forth below:

1. Any client or other individual wishing to make a complaint shall, whenever possible, be offered a Privacy Complaint Form upon which their complaint, suggestions and/or other comments may be fully explained. Blank Privacy Complaint Forms shall be available from the county Compliance Officer. In the absence of the complaint form, the individual making the complaint may reduce the issue to written form on standard white or white lined stationary insuring that the complaint includes the date or dates of the incident, breach or issue relative to the complaint, the name or names of any or all county employees involved and the name and contact information of the complainant. The complaint must also be signed and dated.

2. Each privacy complaint made verbally shall be documented by the county Compliance Officer on a blank Privacy Complaint Form or on standard stationary and in a Complaint Log maintained by the county Compliance Officer. Such documentation shall include: the date the complaint was made; the name of the complainant; whether the complainant was a client, legal representative, a client's family member, or an unrelated person; a description of the discussion in which the complaint was voiced; any suggestions made by the complainant; and the name of the workforce member receiving the complaint.
3. Upon receipt of a Privacy Complaint, the recipient shall date stamp the complaint form and immediately forward the complaint form to the agency or county Compliance Officer as appropriate.

4. All complaints, whether written or oral, shall be immediately reviewed by the receiving Compliance Officer. A response shall be made by the County or agency to any privacy complaint within thirty (30) days of the date of the Compliance Officer's receipt of the complaint, absent extenuating circumstances. Under extenuating circumstances, the Compliance Officer may extend this deadline as necessary, so long as a letter explaining the reason for the delay and the date that the complainant can expect a disposition on the complaint is sent to the complainant prior to the expiration of the thirty (30) day deadline. The date the response is sent shall be documented by the responding Compliance Officer upon the Privacy Complaint Form/document.

5. Copies of all written Privacy Complaints shall be maintained by the county privacy office. NOTE: Complaints originating in the county prison, handled within that organization and not being referred to the county Compliance Officer will be maintained in the Prison Compliance Officer's files.

6. The ultimate disposition of the complaint shall be documented by responding Compliance Officer upon the Privacy Complaint Form, whenever a complaint form exists. Whenever a verbal complaint is received and documented, the ultimate disposition of the complaint, as well as the date of the response, shall also be documented on the transcription performed by the receiving Compliance Officer as well as within the Complaint Log.

7. Client complaints about privacy issues shall never be documented within the client's [medical] chart.

8. All requests for information about the covered agency's privacy practices, shall be responded to by the agency Compliance Officer as soon as reasonably possible, but, in any event, no later than ten (10) days from the date of the request.

9. The Complaint Log may be maintained in either electronic or hard copy form at the discretion of the County Compliance Officer.

XI. COUNTY OF VENANGO PRIVACY POLICY ON CLIENT REQUESTS FOR RESTRICTION OF USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION AND ALTERNATE MEANS OF COMMUNICATING

Purpose

45 CFR ss 164.522 (a) Guarantees individuals the right to request restrictions in the way that covered entities use and disclose the individual's protected health information. Covered entities are not required to agree with these requests, but if they do they may not make uses or disclosures that are inconsistent with the requested restrictions. These restrictions do not apply to health care provided to an individual on an emergency basis.
The American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act HITECH imposes an additional obligation on covered entities to agree to a requested restriction if the disclosure is to a health plan for purposes of payment or health care operations *and* the PHI relates to a health care item or service for which the health care provider has been paid out of pocket in full.

Policy

It is the policy of the County of Venango to provide our clients with a process by which they may request the restriction of uses and disclosures of their private health information for purposes of treatment, payment and health care operations, as well as the restriction of any disclosures that may be otherwise permitted for purposes of providing limited information to family or others involved in the client's care or for notification purposes, in accordance with the HIPAA Privacy Regulations. Venango County and its covered agencies will consider all such requests, although the county and agencies are in no way mandated by the federal HIPAA Privacy Regulations to agree to any such requests.

It is also the policy of this county to accommodate reasonable requests by clients to receive communications of private health information from Venango County covered agencies by alternative means or at an alternative location, without explanation from the client as to the reason.

Procedures

It shall be the duty of the individual agency Compliance Officer to review, make a determination as to disposition of and to respond to all such client requests, under the guidelines set forth below:

1. Any client or other individual wishing to make such a request shall do so in writing, upon a Client Request Form for Restriction of Uses/Disclosures of Private Health Information or for Confidential Communications ("Request Form"). Blank Request forms are available from the county Compliance Officer and shall be provided to any client (or any legal representative) that indicates a desire to request any such restriction or to request confidential communications. If the client prefers to use standard white or lined paper they may do so as long as the appropriate identification information and the request are clearly indicated and explained where necessary.

2. Upon receipt of a Request Form or written request it shall be date stamped and immediately forward it to either the county or the appropriate agency Compliance Officer.

3. All Request Forms shall be immediately reviewed by the Compliance Officer. A response shall be made by the agency to any such request as soon as reasonably possible, but, in any event, no later than within ten (10) days of the date of the agency's receipt of the Request Form. The date that the response is provided to the client shall be documented by the Compliance Officer upon the Request Form.

4. Copies of all Request Forms shall be maintained by the receiving agency with a copy sent to the county Compliance Officer.

5. The ultimate disposition of the request shall be documented by the Compliance Officer upon the Request Form, with any restrictions clearly documented both on the Request Form and in the client's chart, where appropriate.

6. If such a request is granted, the agency shall not use nor disclose the applicable health information in violation of the restriction, unless the information is necessary to treat the client in an emergency. If the information is disclosed to another healthcare provider under such emergency circumstances, the workforce member making the disclosure shall request that that healthcare provider not further use nor disclose the information.

7. Notwithstanding any granted request for a restriction of uses or disclosures, the agency is permitted to disclose the information:

    (a) To the client, or the client's legal representative, where permitted under an approved request for access; or

    (b) To an appropriate party under any of the provisions of Section 164.512 of the HIPAA Privacy Regulations (45 C.F.R. §164.512), concerning permitted uses and disclosures for which a consent, an authorization, or opportunity to agree or object, is not required.

8. To terminate any restriction that has been granted, the agency shall do at least one of the following:

    (a) Obtain the written agreement of the client, or the client's legal representative;

    (b) Obtain the verbal agreement of the client, or the client's legal representative, and document that verbal agreement in the client's chart; or

    (c) Inform the client, or the client's legal representative, that the Organization is terminating its agreement to the restriction with regard only to health information created or received after the date upon which the client or his/her legal representative is informed of the termination.

    The date and manner of such a termination of restriction shall be documented upon the Request Form.

10. At no time shall the Compliance Officer, or any other workforce member receiving a request to receive confidential communications by an alternative means or at an alternative location, require an explanation from the client as to the basis for the request as a condition of providing such communications on a confidential basis.

11. No request to receive confidential communications by an alternative means or at an alternative location shall be granted without the client providing both of the following:

    (a) The client's specification of an alternative address or other method of contact; and

    (b) Information as to how payment will be handled, if appropriate.

12. All granted requests for confidential communications shall be documented clearly within the administrative section of the client's [medical] chart and client's billing file.

XII. COUNTY OF VENANGO PRIVACY POLICY ON
CLIENT REQUEST TO AMEND

Purpose

45 CFR ss 164.526 Enables individuals who believe the protected health information in their record is incorrect or incomplete to request an amendment to the information.

Policy

It is the policy of the County of Venango to guarantee the right of our clients to request an amendment of their health information maintained within the designated record set by the appropriate covered agency, pursuant to the requirements of the HIPAA Privacy Regulations. Copies of all written requests for amendment of health information and any corresponding documentation shall be maintained within the client's chart.

It shall be the duty of the Compliance Officer to process all client requests for amendment of that client's health information pursuant to the procedure set forth below and the federal privacy regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Procedure:

1. A client's request for amendment shall be made in writing on the Client Request to Amend Health Information form, blank copies of which are to be available from the Compliance Officer, or on standard white or lined paper. Forms must be filled out completely, and signed by the client or the client's legal representative. (Change of address, demographic information or insurance can be handled by the case manager without the need for the request process.)

2. Upon receipt of the Request to Amend, the recipient of the request form shall document the date of its receipt upon the request form and immediately forward the request to the agency or county Compliance Officer for processing.

3. All Requests to Amend shall be processed, with action being taken (whether that action is a grant or denial of amendment) and the response being sent to the client or legal representative, within sixty (60) days of the date of the agency's receipt of the Request, absent extenuating circumstances. Under extenuating circumstances only, the Compliance Officer may extend this deadline by no more than an additional thirty (30) days, so long as a letter explaining the reason for the delay and the date that the requestor can expect the response to the request, is sent to the requestor prior to the expiration of the original sixty (60) day deadline.

2. Upon receiving the Request, the Compliance Officer shall, wherever possible, discuss the Request to Amend with those members of the agency's workforce who were originators of the particular health information at issue, for purposes of determining whether the information was complete and accurate as documented.

5. Wherever amendment is granted, in whole or in part, the Compliance Officer, or the originator of the health information at the request of the Compliance Officer, shall make the appropriate amendment to the client's chart or billing record. The amendment shall clearly identify the records in the designated record set that are affected by the amendment, with a clearly documented link being provided to the location of the amendment within the chart or billing record. The date upon which the amendment was made shall be documented upon the Request for Amendment form.

6. Immediately upon amending the record, the Compliance Officer shall notify the client for the following purposes:

    (a) To inform the client that the action has been taken;

    (b) To ask the client to identify any persons who had previously received the health information that is the subject of the amendment, and who may need the amendment; and

    (c) To obtain the client's agreement to have the agency notify such persons who may have relied, or may likely rely in the future, on the information that is the subject of the amendment.

    The date of the notification of the client shall be documented upon the Request for Amendment form.

7. The Compliance Officer shall take all reasonable steps to provide the amendment in writing to the following persons, within a reasonable time under the circumstances of the amendment:

    (a) All persons identified by the client as having received health information about the client and as needing the amendment; and

    (b) All persons, including business associates, known to have the information at issue that may have relied, or may likely rely in the future, on the original information, to the detriment of the client.

    The names and addresses of all persons other than the client who have been provided with the amendment shall be documented on the reverse side of the Request for Amendment form (or an attached sheet, if necessary), along with each date of notification.

8. Grounds for denial of a request for amendment under the HIPAA privacy regulations include:

    (a) The information is accurate and complete.

    (b) The information was not created by the Organization. (Should the client provide a reasonable basis to believe that the originator of the health information is no longer available to act upon a request to amend, the request should be granted if there are no other applicable grounds for denial)

    (c) The information is not part of the Organization's designated record set.

    (d) The information would not be available for inspection under the HIPAA Privacy Regulations, as explained in more detail in the County's Policy and Procedure for Client Requests for Access to Health Information.

    In the case of any denial of a client's request for amendment, the Compliance Officer shall complete and mail to the client the form entitled "Notice of Denial of Client Request to Amend Health Information," maintaining a copy of this form in the client's chart and documenting the date of the mailing of this form upon the Request for Amendment form.

9. The Compliance Officer shall accept any written statement of disagreement that is submitted by the client whose request for amendment was denied, so long as that statement of disagreement does not exceed one side of an 8½ x 11 inch piece of paper. A copy of any such statement of disagreement should be immediately forwarded to each workforce member who was an originator of the health information at issue in the request for amendment.

    In the alternative, the client may request that the agency provide a copy of the client's Request to Amend Health Information and the denial form with any future disclosures of the health

information requested to be amended. **All such requests shall be honored. Whether or not an express request has been made to do this, the client's Request to Amend Health Information and the denial form shall become part of the designated record set and shall be included whenever the health information at issue in the Request for Amendment is disclosed.**

10. The Compliance Officer shall work with any workforce member who was an originator of the health information at issue in the request for amendment, in the preparation of an appropriate rebuttal statement on behalf of the agency, to be made a part of the chart or billing record, along with the client's statement of disagreement. Upon incorporating the rebuttal statement into the chart or billing record, a copy of the rebuttal statement shall immediately be mailed to the client by the Compliance Officer, and the dates of such actions shall be documented upon the Request for Amendment form.

11. Copies of the client's Request to Amend Health Information form and all corresponding documentation concerning the grant or denial of the request, including any denial form, any statement of disagreement and any rebuttal statement, shall be maintained within the client's chart. **Where no amendment was made, each portion of the chart or billing record at issue as the result of the Request to Amend shall be marked [with the phrase "Client Request for Amendment" in the margin] to link the information to the portion of the designated record set containing the request form, denial form, statement of disagreement and/or rebuttal form.**

13. Should the agency be informed of an amendment to a client's health information by another health care provider, health plan or healthcare clearinghouse, the Compliance Officer shall ensure that the amendment is appropriately incorporated into the Organization's designated record set.

XII. COUNTY OF VENANGO PRIVACY POLICY ON PROTECTED HEALTH INFORMATION FOR MINORS

Purpose

45 CFR ss 164.502(g)(3) Identifies that where no other law addresses the situation, the control of an unemancipated minor's health information would fall to the parent, guardian or person acting in *loco parentis*.

Policy

The County of Venango, through its covered agencies, shall permit a parent, guardian or other person acting *in loco parentis* to act on behalf of an unemancipated minor in making decisions relative to health care and shall treat such person as a personal representative with respect to protected health information unless the minor has the authority to act as an individual under state or other applicable law.

Procedures

Under the following four situations the parent does not control a minor's health care decisions and would therefore not control, nor be given access to that minor's protected health information related to that care without the minor's authorization:

1. When state or other law does not require consent of a parent or other person before a minor can obtain a particular health service, and the minor consents to the health care service, the parent is not the minor's representative. One example under Pennsylvania Law, an adolescent has the right to consent to substance abuse services without parental consent. The parent is not the personal representative under the Privacy Rule for this type of service.

2. When a court determines, or other law authorizes, someone other than a parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the specified treatment.

3. When a parent agrees to a confidential relationship between the minor and a physician, the parent does not have access to the health information related to that conversation or relationship.

4. When a health care professional, in his or her professional judgment, reasonably believes that the child has been or may be subject to abuse, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

XIV. COUNTY OF VENANGO PRIVACY POLICY ON PROTECTED HEALTH INFORMATION FOR DECEDENTS

Purpose

45 CFR ss 164.502(f) Requires a covered entity to comply with use and disclosure rules for deceased persons. It further identifies that the rules for protected health information for decedents are the same as for any other individual.

Policy

It shall be the policy of the County of Venango, through its covered agencies, to release protected health information about deceased individuals only as permitted by appropriate federal and state law.

Procedures

Prior to the release of any protected health information the county agency possessing the protected health information shall:

1. Verify the identity of the person requesting health information of a deceased individual and the authority under which he/she is requesting the information.

2. Obtain written documentation of representations required as a condition of disclosure.

3. The executor or administrator authorized by law to act on behalf of an individual's estate shall be identified as the personal representative of the decedent. This personal representative will be treated as the individual for purposes of disclosure of protected information.

The following shall be considered the permitted disclosures of the decedent's protected health information:

1. Law Enforcement official to alert if death is due to criminal conduct pursuant to **45 CFR ss 164.512(f)(4).**
2. Coroners/medical examiners for identification, cause of death, other duties Pursuant to **45 CFR ss 164.512(g)(1).**
3. Funeral directors as necessary to carry out their duties pursuant to **45 CFR ss 164.512(g)(2).**
4. Organ/tissue donation procurement agencies pursuant to **45 CFR ss 164.512(h).**
5. Research on decedent's information pursuant to **45 CFR ss 164.512(i).**

XV. COUNTY OF VENANGO PRIVACY POLICY ON USE OF ELECTRONIC MAIL, FACSIMILE TRANSMISSIONS AND TELEPHONE COMMUNICATIONS

Purpose

45 CFR ss 164.530(c)(1) Requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. **The American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH)** identifies the requirement that covered entities and their Business Associates must either adequately encrypt and otherwise protect all electronically stored or transmitted Protected Health Information or provide for breach policies should the data be lost or the system breached.

Policy

It is the policy of the County of Venango to protect and safeguard the privacy of its clients' private health information, including information that may be contained in electronic, written and/or oral communications, pursuant to the requirements of the HIPAA Privacy Regulations.

Procedures

Venango County recognizes that communication mechanisms such as electronic mail, facsimile transmission and telephone communication carry with them risk of interception, whether intentional or inadvertent. As such, all workforce members of the covered agencies of the County of Venango shall exercise a high level of caution and adhere to the following guidelines when using electronic mail ("e-mail"), facsimile transmission ("fax") or telephone communications to transmit the individually identifiable health information of any client:

Electronic Mail

1. The County of Venango will provide separate User Ids and assist employees in creating their own non-generic passwords for the purpose of isolating the electronic communications of each workforce member. Each workforce member's password shall be maintained confidentially and shall not be revealed to, nor shared with, any other person, except under the direction of the county Compliance Officer or an authorized representative of the Management Information Systems (MIS) Office. No workforce member shall in any way intercept, disclose or assist in the interception or disclosure of any e-mail communication except under the direct supervision of the Director of the MIS office (network administrator). Any workforce member who becomes aware of any violation(s) of this section, or any other section of this policy, shall immediately report the violation(s) to the Compliance Officer and/or network administrator.

2. The County of Venango reserves the right to monitor, audit, delete and read all e-mail messages created and/or received by workforce members upon the Organization's computer system and/or relating to the Organization and/or its clients. The network administrator may override workforce members' passwords and may monitor the contents and usage of e-mail messages to support operational, maintenance, auditing, security, privacy and/or investigative activities.

3. At no time shall any private health information of any client(s) (including not only treatment information, but also billing information and even client identity) be transmitted via electronic mail outside of the Venango County internal network, unless it is encrypted or if encryption is not an available option unless there is in place a policy to notify clients of any breach of confidentiality of their protected health information. In addition, due care shall be used when transmitting private health information of any client(s) by electronic mail (or otherwise) within Venango County's internal network, to prevent the transmittal and/or receipt of such information

to/by any workforce member not authorized to have access to the information. **See Breach Notification Policy**

4. Workforce members shall not transmit confidential client information or proprietary information via e-mail to unauthorized recipients. Proprietary information is any information that belongs to any agency of the County of Venango.

5. Since e-mail messages can be easily misaddressed, workforce members should, wherever possible prior to transmitting any private health information, input the e-mail address to be used into the computerized "address book" or "contact list" and send a test e-mail requesting confirmation of receipt from the addressee. Wherever possible thereafter, the workforce member should use the address book/contact list function to select the addressee's name, so as to avoid the potential for mistyping the e-mail address.

6. Any e-mail transmissions concerning any form of individually identifiable health information shall include the following language on the e-mail message:

This electronic message and its attachments may include information from Venango County that is confidential and may be protected under Federal and/or State law. This information is intended to be for the use of the intended addressee only. The improper use of this information is prohibited. If you have received this e-mail in error, please notify us by telephone at (814) 432-9750 immediately or by e-mail at kkoyack@co.venango.pa.us so that we may arrange for the appropriate retrieval of this document at no cost to you.

7. Workforce members shall not "forward" to any third party outside of the County Network any e-mail messages that contain any form of individually identifiable health information, unless expressly authorized by the client on a signed Authorization for Use/Disclosure of Health Information form. Workforce members shall not forward any E-mail message received from any third party outside of their individual agency to any client of the agency, regardless of the subject matter of the e-mail.

8. Venango County covered agencies will incorporate e-mail messages sent or received that concern the diagnosis or treatment of a client, or payment for treatment, into the client's chart and/or billing file, and shall maintain such information with the same degree of confidentiality as the remainder of the client's chart and billing file.

9. Upon incorporation of an e-mail message into a client's chart or billing record, the e-mail message shall be fully deleted from the workforce member's e-mail files, and the workforce member's computerized "trash bin" shall be immediately emptied. Workforce members shall periodically purge from their e-mail files (as well as the "trash bin"), all other e-mail messages that contain any form of individually identifiable health information, including but not limited to the identity and/or e-mail address of any client of their agency. At intervals to be determined by the Compliance Officer or Network Administrator, the County Network shall delete all copies of all e-mail messages containing clients' protected health information that have been "backed-up" to a separate data storage media, for purposes of protecting the private health information and to free storage space on the system. Prior to the sale, trade in or any other disposition of any county computer, the Venango County MIS Office shall reformat that computer's hard drive to insure that all client protected health information has been completely removed from the unit.

Facsimile Transmission

1. All incoming faxes should be immediately removed from each fax machine by the receptionist, the department secretary or the nearest available workforce member and delivered to the intended recipient or secured within a closed file folder until the intended recipient can retrieve the fax.

2. All outgoing faxes shall be sent under a separate cover sheet that shall include the following language:

The documents included with this facsimile may include information from an agency of Venango County (*agency name*) that is confidential and may be protected under federal and/or state law. This information is intended to be for the use of the intended addressee only. The improper use of this information is prohibited. If you have received this fax in error, please notify us by telephone at (814) 432-9750 or by e-mail at kkoyack@co.venango.pa.us immediately so that we may arrange for the appropriate retrieval of these documents at no cost to you.

3. If possible, the receptionist or secretary of each protected agency where a Fax machine is located shall coordinate the assignment and programming of the fax numbers of those healthcare providers, health plans and other payors to whom the agency regularly faxes the protected health information of its clients, uniformly into the memory of each fax machine used by the agency. The "speed-dial" numbers shall be reserved primarily for other healthcare providers, health plans or other payors. Each such programmed number shall be tested prior to the transmission of any protected health information. A directory of these "speed-dial" numbers shall be maintained and made available to all workforce members, and shall be posted near each fax machine. All workforce members are to use those "speed-dial" numbers when faxing protected health information to these locations.

4. Should it be determined, or suspected, at any time, that a facsimile transmission containing the protected health information of one or more clients, may have been transmitted to an unintended recipient, a telephone call shall immediately be placed (or, if necessary, an additional fax shall be sent) to make arrangements to retrieve the errant fax.

Telephone Communications

1. All workforce members shall use caution to protect the confidentiality of a client's protected health information, including but not limited to the client's identity, in the course of telephone discussions with the client or any third party. Wherever possible, such telephone discussions should be conducted away from other people, preferably in a conference room or office with the door closed. Other measures to minimize the risk of another person overhearing the discussion include the use of a low voice, with the workforce member's back turned toward others in the immediate vicinity.

2. A workforce member shall not initiate a telephone discussion that will include the discussion of protected health information within the immediate vicinity of another client or any other third party.

3. If the workforce member has a need to discuss a client's protected health information over the telephone, and another client or third party is standing nearby seeking attention from the workforce member, the workforce member shall, wherever possible, request in a courteous manner that the client have a seat in an alternative location while the client waits, or courteously suspend the discussion of protected health information until that client has received assistance and moved from the vicinity.

4. Whenever a telephone call is placed to a client, a workforce member shall make a reasonable attempt to confirm that the person with whom they are speaking is, in fact, the client, prior to the commencement of a discussion of any protected health information.

5. At no time shall any workforce member leave any detailed health information in a message on any answering machine, in a voice mail message, with an answering service or with a family member, friend, colleague or any other third party answering the telephone. Messages should be limited to the workforce member's name and the agency's telephone number.

6. Wherever possible, workforce members shall refrain from the discussion of individually identifiable health information over a cellular or other mobile or cordless telephone, or from the

provision of such information in digital form on a pager or other portable data messaging system, choosing instead a hard wired, land-based telephone line for such communications. Should it be necessary to use a cordless phone of any type, discussions relative to individual consumers should be brief, general and if possible only using first names or numerical identifiers.

XVI. COUNTY OF VENANGO PRIVACY POLICY FOR TRANSCRIPTION OF RECORDS

Purpose

45 CFR ss 164.530(c)(1) Requires a covered entity to have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.

Policy

It is the policy of the County of Venango to protect and safeguard the privacy of its clients' private health information, including information that has been verbally dictated and, thereafter, transcribed into typewritten form.

Procedures

All workforce members shall adhere to the following guidelines when involved in the dictation of individually identifiable health information, transport of dictation prior to transcription, and/or the transcription of such health information:

1. The information contained within a dictated or transcribed document, irrespective of the media or format in which it is being maintained, may include protected health information that is subject to the protections of the HIPAA Privacy Regulations. No portion of the dictated and/or transcribed record shall be used or disclosed to any person, unless permitted under the HIPAA Privacy Regulations.

2. The County of Venango reserves the right to review, monitor, audit and/or read dictated and/or transcribed health information, irrespective of employment status of the dictator or transcriptionist. The network administrator, at the direction of the Compliance Officer, may override transcriptionists' or other workforce members' passwords, and may monitor the content of transcription and/or dictation to support operational, maintenance, auditing, security, privacy and/or investigative activities.

3. Dictation of individually identifiable health information, as well as dictation playback, shall take place only in an environment in which the workforce member is reasonably able to prevent the information from being overheard by unauthorized persons. Wherever possible, dictation shall take place in a wholly private setting, such as a conference room or office with the door closed. Dictation should never take place through a cellular or other mobile telephone, through a public telephone in a location in which others may overhear the call, or onto an unsecured answering machine or voice mail message.

4. A workforce member dictating protected health information shall never leave their dictation unsecured.

5. No two members of the Organization's workforce shall dictate upon the same audiotape, CD or voice file.

6. Audiocassettes, voice files, compact discs or other media containing dictation shall be hand delivered to the transcriptionist, unless an alternative method of delivery is approved by the Compliance Officer. At all times during the transport of the dictation file(s) to the transcriptionist, the workforce member shall make every reasonable effort to protect, lock, or

otherwise physically or technologically secure (i.e., by a non-generic password, transport in a locked case, etc.) the dictation file(s).

7. Transcriptionists are required to log off, or otherwise immediately secure, their computers and/or dictation equipment at all times when not transcribing, so as to prevent the unauthorized access, viewing or hearing of dictated and/or transcribed information.

8. No workforce member shall electronically transmit transcribed health information, except as authorized by the Compliance Officer and as provided for in the Venango County Privacy Policy for Use of Electronic Mail, Facsimile Transmission and Telephone Communications for the Transmission of Individually Identifiable Health Information.

9. Covered agencies of the County of Venango shall store dictation on audio cassettes, voice files, compact discs or other related media only for the length of time necessary to transcribe and review the transcription. At all such times, the dictation shall be secured in a manner that reasonably protects the privacy of the information contained therein. Once the dictation has been transcribed and the transcription has been reviewed and approved, the dictation shall be erased and/or otherwise deleted from the tape, CD, voice file or other medium upon which it had been recorded. No transcribed tape, CD, voice file or other medium shall be reused until it has first been purged of all other dictation.

10. After completion of transcription of any dictation, the transcriptionist shall authenticate it by electronically signing the document with an identifier assigned by the Compliance Officer or network administrator. It should be noted that this authentication process does not constitute the formal authentication of the record as required by legal and professional standards.

XVII. COUNTY OF VENANGO PRIVACY POLICY FOR STORAGE, FILING AND ACTIVE USE OF PROTECTED HEALTH INFORMATION

Purpose

45 CFR ss 164.530(c)(1) Requires a covered entity to have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.

Policy

It is the policy of the County of Venango to protect Individuals' health information and documentation, in whatever format they may be, in compliance with HIPAA Privacy Regulations by insuring the physical security of all active and inactive files.

Procedures

Paper Files

All paper files containing health information and/or health billing information shall be stored in either locked file cabinets or in a limited access locked security room.

Active health records shall be maintained in a locking cabinet or drawer within the treating Venango County covered agency with access limited to caseworker, supervision and administrative staff only. Files that are in use should be placed on counters, desks or other work surfaces that are out of sight of the general public, other clients or unauthorized workforce members.

All individual client treatment and billing files shall have a separate section for the "Designated Record Set" which shall include all medical information available to a particular client or his legal representative for inspection or accounting as well as any documentation identified in other sections of these Policies and Procedures requiring maintenance in this specified area of the file.

All data entry into client files shall be performed so that the written or typed pages of the file or the active computer screen are positioned away from the line of sight of the public or unauthorized workforce members. On no account are pages or files to be left open and unattended where they could be observed or read by any unauthorized person.

On no account shall any individually identifiable client document, form, file or portion thereof be left in or on any surface of any office or public area where unauthorized persons might have access. Workforce members must exercise extra caution during their use of photocopiers, fax machines, postal meters etc. so that protected materials are not inadvertently left at any of those locations.

Every effort must be made by the caseworker, supervisor, Compliance Officer and administrative staff of each covered agency to avoid allowing access to any individual's protected health information by anyone who is not specifically authorized to do so.

When workforce members must work away from their agency office or program site and are required to carry with them (or are likely to create) documents, files, forms or papers containing any individual's protected health information they must protect that individual health information from loss, theft, or unauthorized viewing by the use of a carrying case, folder or other container with a lock or other mechanism to restrict access.

Computer Files

In addition to precautions and safety measures identified in this document under the heading of "Privacy Policy on the use of Electronic Mail…" workforce members shall make every effort to protect the security of client information stored or transmitted by electronic means.

All client files maintained in computer memory shall be accessible only by workforce members authorized by agency supervisors using unique password and/or access codes provided or enabled by the MIS Department.

The individual workforce member shall only be permitted access to that portion of a client's file necessary for that workforce member to perform his or her specific job function(s).

Should a workforce member be called away from his/her computer terminal while a file containing protected health information is open, the workforce member will either close the file, or lock the computer by depressing the Ctrl, Alt and Delete keys simultaneously and then choosing the option of "Lock Computer" so that no one else will be able to access the file until his or her return. The second option will allow the workforce member to return to his/her work exactly where they were interrupted while protecting the confidentiality of the client information.

Computer screens shall be physically located so that they do not face doorways or public areas, so that no client, visitor or other workforce member can inadvertently see the screen. Screen savers shall be set to come on at the shortest possible time consistent with the workforce members work habits.

When files are no longer being worked on they shall be immediately closed.

As technology becomes available or security of HIPAA or other federal or state regulations upgrade, additional security actions and requirements will be added to this section. This will in no way change any consumer or client privacy right and will not require any change to any Venango County Privacy Notice.

XVIII. COUNTY OF VENANGO PRIVACY POLICY FOR RETENTION AND DESTRUCTION OF HEALTH INFORMATION

Purpose

45 CFR ss 164.530 (j)(2) Requires that a covered entity retain the documentation required by the provisions of HIPAA and the Final Privacy Rule be maintained for a period of six (6) years from the date of its creation or the date that it was last in effect, whichever is the later.

Policy

It is the policy of The County of Venango to retain clients' health information and documentation of compliance with the HIPAA Privacy Regulations, pursuant to the following schedule:

Client's Medical/Treatment Chart	• Minimum of 7 years from last date of treatment • If the client is under the age of 18, the chart shall be retained for at least 2 years after the client's 18th birthday
Client's Billing File	• Minimum of 7 years from last date of treatment • If the client is under the age of 18, the billing file shall be retained for at least 2 years after the client's 18th birthday
Psychotherapy Notes	• Minimum of 7 years from last date of treatment, • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Each Version of Notice of Privacy Practices	• 7 years from last date in effect
[Consents for Use/Disclosure of Health Information for Treatment, Payment or Health Care Operations] [Acknowledgments of Receipt of Notice of Privacy Practices]	• Indefinitely, if not revoked. • If revoked, document shall be retained with revocation form for 7 years from date of revocation
Authorization Forms	• 7 years from expiration date • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Responses to Requests for Release of Client Information Pursuant to Authorization Form	• 7 years from date of response to request for release of information • If request involves a client under

	the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Warrants, Subpoenas, Court Orders and/or Administrative/Governmental Requests Concerning Release of Client Information	• 7 years from date of response • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Responses to Warrants, Subpoenas, Court Orders and/or Administrative/Governmental Requests Concerning Release of Client Information	• 7 years from date of response • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Requests for Accounting	• Minimum of 7 years from date of accounting • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Disclosure Sheets [Client's Disclosure Information Maintained in Computerized Database and/or Print-Out Form]	• Minimum of 7 years from last date of treatment • If disclosure sheets involve a client under the age of 18, all disclosure sheets shall be retained for at least 2 years after the client's 18th birthday
Accountings of Disclosures	• Minimum of 7 years from date of accounting • If accounting involves a client under the age of 18, all accountings produced shall be retained for at least 2 years after the client's 18th birthday
Requests for Restriction on Uses and/or Disclosures and/or for Confidential Communications	• Minimum of 7 years from date of response to or denial of request • If request involves a client under the age of 18, request forms shall be retained for at least 2 years after the client's 18th birthday
Denials of Requests for Restriction on Uses/Disclosures and/or for Confidential Communications	• Minimum of 7 years from date of denial of request • If response involves a client under the age of 18, response

	shall be retained for at least 2 years after the client's 18th birthday
Responses to Requests for Restriction on Uses/Disclosures and/or for Confidential Communications, where Request has been Granted	• Minimum of 7 years from last date of treatment • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Complaint Forms Concerning Privacy Practices	• Minimum of 7 years from date of response to complaint • If complaint involves a client under the age of 18, complaint forms shall be retained for at least 2 years after the client's 18th birthday
Responses to Complaint Forms Concerning Privacy Practices	• Minimum of 7 years from date of response to complaint • If complaint involves a client under the age of 18, response to complaint shall be retained for at least 2 years after the client's 18th birthday
Requests for Amendment of Health Information	• Minimum of 7 years from date of response to request • If request involves a client under the age of 18, request form shall be retained for at least 2 years after the client's 18th birthday
Responses to or Denials of Requests for Amendment of Health Information	• Minimum of 7 years from date of response to complaint • If complaint involves a client under the age of 18, response to request for amendment shall be retained for at least 2 years after the client's 18th birthday
Requests for Access to Health Information by Clients and/or Legal Representative	• 7 years from date of response to or denial of request, or from date of reviewing official's letter of decision (if review requested)
Responses to or Denials of Requests for Access to Health Information by Clients and/or Legal Representative, with or without Requests for Review of Access	• 7 years from the date of response to or denial of request, or from date of reviewing official's letter of decision (if

Denial	review requested)
Decisions of Reviewing Official on Review of Access Denial	• 7 years from the date of reviewing official's letter of decision
Copies of Powers of Attorney, Guardianship Orders, Letters of Administration, Letters Testamentary, Custody Orders, or Other Proof of Status of Legal Representative	• As long as the client's medical chart and/or billing record [or consent for use/disclosure for treatment, payment or healthcare operations and/or acknowledgment of receipt of notice of privacy practices] is maintained
Policies and Procedures Concerning Maintaining, Retaining, Safeguarding, Requesting, Using and/or Disclosing Health Information and Related Documentation	• 7 years from last date policy or procedure was in effect
All versions of [Job Descriptions] [Schedule/Table of Workforce Access Determinations pursuant to Minimum Necessary Standard]	• 7 years from last date each version of [job description/table of workforce access determinations] was in effect
All Versions of Personnel and Other Designations Made Pursuant to the HIPAA Privacy Regulations	• 7 years from last date each version of personnel or other designation was in effect
Contracts with "Business Associates" as defined by HIPAA Privacy Regulations	• 7 years from expiration date of contract or from termination of contract, whichever occurs first
Correspondence to and/or Received from HIPAA Business Associates Concerning Breach, Accounting of Disclosures, Amendment of Information, Termination of Agreement Due to Breach, Destruction or Return of Information, or Other HIPAA-related Obligations	• 7 years from date of most recent correspondence
Certificates of Destruction by Third Party (including HIPAA Business Associates)	• Indefinitely
Destruction Log	• Indefinitely
Documentation of Completion of Workforce Training	• 7 years from last date of employment

Personnel File Documentation of Workforce Privacy Sanctions Applied	• 7 years from date of completion of workforce sanction

Procedures

It is further the policy of The County of Venango that whenever destruction of client health information of any sort, or other related documents, is permitted pursuant to this retention schedule; destruction shall be completed pursuant to the following guidelines:

1. Documents shall only be destroyed by a process of shredding [and/or incinerating] each document, leaving no readily readable portion of the document. Shredding will be either cross-cut or straight cut across the lines of print effectively eliminating the continuity of the information or documents shall be transported to a bonded shredding company who shall completely destroy the documents in question.

2. Immediately upon destruction of any documentation listed in the schedule above, the workforce member charged with the duty shall enter in an approved Destruction Log: (1) the date of destruction; (2) a description of the documents destroyed consistent with the titles in the schedule above, including where appropriate the name of the client(s) to whom individually identifiable health information relates; (3) the manner of destruction; and (4) the signature of the person completing the destruction.

3. When destruction of any such documentation is completed by anyone other than a member of the workforce of the Organization, including a business associate of the Organization, a Certificate of Destruction shall be presented to the county along with the invoice for such service. The certificate shall be forwarded to and maintained by the Compliance Officer.

4. It shall be the responsibility of all workforce members to either shred or to deposit for appropriate destruction any and all copies of documents containing individually identifiable health information, that are no longer in use, as soon as this information or copy is no longer in use. Covered containers for such deposits shall be maintained in various locations around the agency area. These containers shall be emptied by a representative of the contracted shredding company as necessary.

5. Individual case files ordered expunged by a court of competent jurisdiction or under regulation by an agency of state government shall be destroyed completely within the guidelines established by the judge or agency in question.

XIX. COUNTY OF VENANGO PRIVACY POLICY ON BREACH NOTIFICATION

Purpose

To provide guidance for breach notification by covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

Background

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIP AA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

Policy

Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the covered agency, or, by exercising reasonable diligence would have been known to the covered agency (includes breaches by the agency's business associates). The agency shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the agency (see attachment for examples of breach of unsecured protected heath information). Following the discovery of a potential breach, the agency shall begin an investigation, notify the Venango County HIPAA Compliance Officer who will conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed by the agency to have been, accessed, acquired, used, or disclosed as a result of the breach. The agency with the assistance of the Compliance Officer shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

Breach Investigation: The agency shall name an individual to act as the investigator of the breach (e.g., Compliance Officer, security officer, county solicitor, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the Venango County Administration as appropriate (e.g., County Commissioners, administration, human resources, legal counsel, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the agency will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The agency shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The agency has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the Compliance Officer, Security Officer and County Solicitor will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed

B. The type and amount of PHI involved.

C. The potential for significant risk of financial, reputational, or other harm.

Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the agency involved or the business associate involved. It is the responsibility of the county to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the agency that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or

B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Content of the Notice: The notice shall be written in plain language and must contain the following information:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:

A. Notice to Individual (s): Notice shall be provided promptly and in the following form:

1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the agency knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

2. Substitute Notice: In the case where there is insufficient or out-of- date contact information (including a phone number, email address, etc.) that precludes direct

written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals) then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the county's web site, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

3. If the Compliance Officer determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet web site a list identifying covered entities involved in all breaches in which the **unsecured** PHI of more than 500 patients is accessed, acquired, used, or disclosed.

1. For breaches involving 500 or more individuals, the Compliance Officer or County Solicitor shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

2. For breaches involving less than 500 individuals, the Compliance Officer will maintain a log of all county breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the Compliance Officer shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach:

A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).

C. A description of the action taken with regard to notification of patients regarding the breach.

D. Resolution steps taken to mitigate the breach and prevent future occurrences.

Business Associate Responsibilities: The business associate (BA) of the covered agency/county that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the agency of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the agency with any other available information that the agency/Compliance Officer is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the agency will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

Workforce Training: Venango County shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within their particular agency.

Complaints: Venango County shall provide a process for individuals to make complaints concerning the county's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the county's breach notification processes.

Sanctions Venango County has in place and shall apply as appropriate sanctions against members of its - workforce who fail to comply with privacy policies and procedures.

Retaliation/Waiver: Venango County covered agencies may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The county may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Applicable Federal/State Regulations:

- ARRA Title XIII Section 13402 -Notification in the Case of Breach.
- FTC Breach Notification Rules -16 CFR Part 318
- .45 CFR Parts 160 and 164 -HIPAA Privacy and Security Rules
- WI § 134.98 -Notice of Unauthorized Acquisition of Personal Information (Note: Not applicable to Covered Entities under HIPAA).

Examples of Breaches of Unsecured Protected Health Information –

- Workforce members access the electronic health records of a celebrity who is treated within the facility.
- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).

- Misdirected e-mail.
- Lost flash drive containing database of patients participating in a clinical study.
- A workforce member accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- Misfiled patient information in another patient's record which is brought to the organization's attention by the patient.
- Medical record copies in response to a payers request lost in mailing process and never received.
- Misdirected fax of patient records to another entity instead of the requesting provider's fax.
- Briefcase containing patient documents stolen from car.
- PDA with patient information.
- Intentional and non-work related access by staff member of neighbor's information.
- Patient documents left in public access area by mistake.

Federal Breach Penalties

Penalties for Breach: Penalties for violations of HIPAA have been established under HITECH as indicated below. The penalties do not apply if the organization did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty days. Penalties will be based on the agency's culpability for the HIPAA violation. The Secretary of HHS will base its penalty determination on the nature and extent of both the violation and the harm caused by the violation. The Secretary still will have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

- The minimum civil monetary penalties are tiered based upon the entity's perceived culpability for the HIP AA violation, as follows:

  Tier A -*If the offender did not know*

  - $100 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $25,000.

  Tier B -*Violation due to reasonable cause, not willful neglect* e

  - $1,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $100,000.

  Tier C -*Violation due to willful neglect, but was corrected.*

  - $10,000 for each violation, total for all violations of an identical requireme11t during a calendar year cannot exceed $250,000.

  Tier D -*Violation due to willful neglect, but was NOT corrected.*

  - $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $1,500,000.

XXI. COUNTY OF VENANGO PRIVACY POLICY ON WORKFORCE TRAINING AND SANCTIONS

Purpose

45 CFR ss 164.530 (b)(1) Requires covered entities to train all members of its workforce on the policies and procedures with respect to protected health information required by that subpart, as necessary and appropriate for the members of the workforce to carry our their function within the covered entity. **The American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH)** Requires HHS to formally investigate any complaint of a violation of HIPAA if a preliminary investigation indicates a possible violation due to willful neglect, and to impose civil penalties for these violations. In addition it allows state Attorneys General to bring civil actions in federal court on behalf of state residents if there is reason to believe that the interest of one or more residents has been threatened or adversely affected by a person who violates HIPAA.

HITECH Act created tiered approach to civil monetary penalties for violations of HIPAA.

• If the person did not know (and by exercising reasonable due diligence would not have known) that he or she violated the law, the penalty shall be at least $100 for each violation not to exceed $25,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

• If the violation was due to reasonable cause and not to willful neglect, the penalty shall be at least $1000 for each violation not to exceed $100,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

• If the violation was due to willful neglect AND the violation was corrected, the penalty shall be at least $10,000 for each violation not to exceed $250,000 for all such identical violations during a calendar year, but may be no more than $50,000 for each violation not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year.

• If the violation was due to willful neglect and was not corrected, the penalty shall be at least $50,000 for each violation not to exceed $1.5 million for all such violations of an identical requirement or prohibition during a calendar year

Policy

It is the policy of The County of Venango to safeguard the private health information of its clients by imposing appropriate sanctions for any breaches of confidentiality, or violations of this Organization's information privacy policies, committed by any member of this Organization's workforce. This policy shall apply to all employees, volunteers, and any other persons designated as members of the County of Venango's workforce, whether or not receiving payment from the Organization.

It is further the policy of the County of Venango that each member of its workforce shall receive training on the privacy policies of the Organization applicable to his/her job functions, including but not limited to this policy as it relates to sanctions.
Privacy training shall be conducted, under the supervision of the Compliance Officer, under the guidelines set forth below:

1. Training shall be provided to each new member of Organization's workforce on the privacy policies of this Organization applicable to his/her job functions, as determined by the Compliance Officer from the workforce member's agency description. Such training shall be completed within the workforce member's orientation period prior to the workforce member's unsupervised access to clients' private health information.

2. Completion of the privacy training for each workforce member shall be documented [within the workforce member's personnel file], and shall include a statement of the scope of training, the date completed, and the signature of the workforce member supervising the training.

3. Should any material change to any privacy policies be made that would require the publication of a revised Notice of Privacy Practices under the federal HIPAA Privacy Regulations, each workforce member shall receive training on the revised privacy policies applicable to his/her job functions. Wherever possible, this training shall be completed prior to the effective date of the revised Notice of Privacy Practices, but, in any event, within a reasonable time of the effective date of the revised Notice of Privacy Practices.

4. Upon completion of privacy training, all workforce members shall sign a confidentiality agreement, acknowledging completion of the training and understanding of County of Venango's privacy policies.

5. It shall be the duty of the Compliance Officer to make a recommendation to the Director of Human Resources as to sanctions to be imposed for any breach of client confidentiality and/or for violation of any information privacy policy by any member of the workforce of this Organization, considering the severity of the particular breach or violation.

6. All sanctions imposed shall be consistent with the terms of, and imposed pursuant to the processes set forth in, any applicable collective bargaining agreement and/or employment contract in place at the time of the violation.

7. Sanctions shall be imposed within the appropriate sanctions range by the County Commissioners at the recommendation of the Director of Human Resources or, where appropriate, the recommendations of the Compliance Officer in conjunction with the Director of Human Resources upon finding that any of the following categories of breaches of client confidentiality and/or violations of information privacy policies had been committed by any workforce member:

- Negligent or Unintentional Breach of Client Confidentiality and/or Violation of Privacy Policy — Sanctions Range A

• Actions Demonstrating Intent or Willfulness to Breach Client Confidentiality and/or to Violate Privacy Policy	Sanctions Range B
• Breach of Client Confidentiality or Violation of Privacy Policy, Resulting in (or with the Intention to Result in) Pecuniary Gain to the Workforce Member or the Organization	Sanctions Range C
• Knowing Participation in an Action of Another that Breaches Client Confidentiality and/or Violates Privacy Policy	Sanctions 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	Sanctions Range A

Particular sanctions imposed shall be at the discretion of the County Commissioners at the recommendation of the Human Resources Director and the Compliance Officer, but must always fall within the applicable sanctions range:

Sanctions Range A	• Written Warning • Probation (3 month, 6 month or 1 year) (the terms of which shall include immediate termination upon any breach of client confidentiality or violation of privacy policy during term of probation) • Suspension with Pay • Suspension without Pay • Termination (with or without immediate removal from premises)
Sanctions Range B	• Probation (1 year) (the terms of which shall include immediate termination upon any breach of client confidentiality or violation of privacy policy during term of probation)

	• Suspension with Pay • Suspension without Pay • Termination (with or without immediate removal from premises)
Sanctions Range C	• Suspension without Pay • Termination (with immediate removal from premises)

8. Should a workforce member receive two written warnings, the lowest minimum sanction that may be imposed is a [one-year] probation, the terms of which shall include immediate termination upon any breach of client confidentiality or violation of any privacy policy during the term of the probation.

9. Breaches of confidentiality and/or violations of privacy policies shall be sanctioned pursuant to these guidelines, whether occurring within or outside of the workplace.

10. All written warnings and documentation of sanctions imposed shall be maintained in the workforce member's personnel file.

11. Any workforce member against whom sanctions have been imposed pursuant to this policy shall have the right to submit a written statement of disagreement or explanation [to the Director of Human Resources and/or the Compliance Officer]. All such statements shall be maintained within the workforce member's personnel file for as long as the documentation of the sanction is maintained.

12. The Venango County Director of Human Resources or the Compliance Officer acting in conjunction with the Director of Human Resources shall at all times have the ability to recommend to the County Commissioners that they lift a previously imposed sanction should the allegation later be determined to be unfounded. Should any such sanction be lifted, all documentation of the sanction shall be removed from the personnel file of the workforce member, and shall be placed in a confidential file maintained by the Compliance Officer to be used only for purposes of compliance with the documentation requirements of the federal HIPAA Privacy Regulations.

13. There shall be nothing in the description or enforcement of these sanctions that shall in any way invalidate any prosecution under applicable state or federal statutes for the same action or inaction on the part of any workforce member.

XXII. COUNTY OF VENANGO PRIVACY POLICY ON EMPLOYEE HEALTH CARE PLAN

Purpose

45 CFR ss 160.103 "Definitions" Defines a "Group Health Care Plan" as an employee welfare benefit plan...including insured and self insured plans, to the extent that the plan provides medical care...including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants; or

(2) Is administered by an entity other than the employer that established and maintains the plan.

45 CFR ss 164.504 (f) "Uses and disclosures: organizational requirements." Establishes standard requirements for group health plans, requirements for plan documents and specifications for uses and disclosures from the plan to the plan sponsors

45CFR ss 164.530 "Administrative requirements" (k) "Standard: group health plans." Describes standards and implementation specifications as they apply to group health plans

Policy

It is the policy of The County of Venango to make available group health care coverage to its employees and eligible family members. In doing so it is and shall continue to be the policy of the County of Venango that communications between the health insurance issuer or HMO and the county office administering the health care plan shall be limited in scope and content in order to avoid any violation of the language or spirit of the HIPAA Privacy Regulations.

It is also the policy of the County of Venango that any protected health information received from any health insurance issuer or HMO providing group health care coverage will be used only for the administration of the group health care plan and that it shall never be disclosed or used for employment related actions or decisions or in connection with any other benefit or employee benefit plan of the county.

It is further the policy of the County of Venango that all group health plan documents be consistent with the standards and specifications found in 45 CFR ss 164.504 (f) and administered in accordance with the provisions of 45 CFR ss 164.530 (k) and any other applicable section of the HIPAA Privacy Regulations.

Procedures

It shall be the responsibility of the Venango County Human Resources Office, with the assistance of any other appropriate administrative agency, including but not limited to the Commissioner's Office, the Compliance Officer etc. to insure that all group health plan documents contain the appropriate HIPAA compliant language, standards and specifications.

All Venango County Employee group health plan documents shall at a minimum incorporate the following provisions:

- A provision to establish the permitted and required uses and disclosures of individually identifiable health information by the county (plan sponsor) provided that such permitted uses and disclosures may not be inconsistent with the provisions of the Privacy Regulations.

- A provision to provide that the group health plan will disclose protected health information to the plan sponsor (county) only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor (the county) agrees to:

    - Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

    - Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor (the county) with respect to such information;

    - Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor (the county);

    - Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for, of which the sponsor becomes aware;

    - Make available protected health information to the subject of said information or the parent or legal guardian of the subject of the information for all purposes permitted by the provisions of the HIPAA Privacy Regulations;

    - Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with the provisions of the HIPAA Privacy Regulations.

It shall be the responsibility of the Venango County Human Resources Department or other appropriate agency to provide for adequate separation between the group health plan and the plan sponsor (the county). This shall be accomplished by insuring that the plan documents must:

Describe those employees or classes of employees or other persons under the control of the plan sponsor (the county) to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

- Restrict the access to and use by such employees and other persons described in the preceding paragraph to the plan administrative functions that the plan sponsor (county) performs for the group health plan; and

- Provide an effective mechanism for resolving any issues of noncompliance by persons identified in this section. To wit the enforcement of the sanction provisions of this county policy.

VENANGO COUNTY, PENNSYLVANIA

HIPAA COMPLIANCE PLAN AND PROCEDURE

APPENDIX I EXEMPT AGENCIES

"All county employees will receive a level of HIPAA training based upon their designated job function, location and responsibilities."

Agriculture: This agency of Venango County Government provides no health care, does not bill for health care, does not pay for health care and does not receive or maintain any individually identifiable health information and is therefore exempt from involvement as a covered agency under HIPAA.

Airport: This agency of Venango County Government provides no health care, does not bill for health care, does not pay for health care and does not receive or maintain any individually identifiable health information and is therefore exempt from involvement as a covered agency under HIPAA.

Auditors: This agency audits the financial transactions of all county agencies to insure that financial transactions are properly conducted and that expenditures are properly authorized by contract or other legal agreement. The Venango County Auditors do not routinely access or review individual consumer records unless they are part of a larger audit question. If individual records must be reviewed no individual information is ever included in an audit report and if individual records are ever removed from a covered agency for further review, it is the responsibility of that individual agency's fiscal technicians, accountants or supervisors to de-identify individual health payment records prior to that removal.

Auditors are elected county officials and are not providers of health care, nor do they pay or arrange payment for health care. The primary responsibility of the Auditors is to guarantee overall Venango County Governmental fiscal integrity and only a small portion of this overall activity involves access to any health care consumer financial information; as such this office has been identified as exempt from involvement as a covered agency under HIPAA.

As an added level of security for health consumer privacy, Venango County Auditors will be required to sign a "Workforce Confidentiality Agreement" at the conclusion of their HIPAA training with the original filed in the Venango County Privacy Office, and copies available to individual covered agencies for their privacy files.

Commissioners: The three elected Venango County Commissioners, and their office staff, are charged with the executive management of all county government. Included in the responsibilities of the commissioners is the review and signing of contracts for health services; however this is only a portion of their overall responsibilities and does not generally include access to or review of individual client health information or health payment information.

As signatories and negotiators of labor agreements and employee health contracts, the commissioners and their staff do receive information on complaints, grievances, job related injuries, accidents and safety concerns. The information reviewed for these activities is not maintained in the commissioners' office, and with the exception of information established by law as being "public record" or which the individual involved has authorized, is de-identified prior to their review; as such this office has been identified as exempt from involvement as a covered agency under HIPAA.

Coroner: The Venango County Coroner and his staff do not provide health care, bill for health care or pay for health care as a normal part of their regular business. In addition, Section 1251 of the Commonwealth of Pennsylvania County Code states that "Every coroner, within thirty (30) days after the end of each year, shall deposit all of his official records and papers for the preceding year in the office of the Prothonotary for the inspection of all persons interested therein. Coroner reports, etc. become "Public Record" by law, and therefore are not protected under the HIPAA guidelines.

45 CFR ss 164.512 (g) states that: "A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph." This section further removes the covered entity status from the office of coroner since the only time the coroner would be a covered entity would be for a function beyond or in addition to that of coroner.

As the work of the coroner and his staff do not fit the definitions for a covered entity under the HIPAA administrative requirements, this office is identified as an exempt county agency.

Courts: The Venango County Courts do not provide health care, bill for health care or pay for health care as a normal part of their regular business. Orders relating to evaluations or treatment for physical or mental conditions are more in relationship to culpability for criminal or civil law violations, court orders or sentence compliance than the individual's medical necessity and as such are not health care per se. Payment for evaluations are considered court costs and are assessed to the individual if found guilty and to the county if not.

45 CFR ss 164.512 (e) (1) states: "A covered entity may disclose protected health information in the course of any judicial or administrative proceeding..." and then limits what the health care covered entity may disclose, to the court, based upon the type of order

or proceeding that the report is in response to. This clearly identifies the "Court" as a recipient of information or of a report from a covered entity, not the covered entity itself and as such this office has been identified as exempt as a covered entity under HIPAA.

In the interest of maintaining the security of protected health information reported to the court, but not released as a matter of public record or in a public proceeding, the offices of the Venango County Courts will be expected to provide adequate physical security for all such information.

Court Supervision Service: The primary responsibility of this agency is the supervision of adult and juvenile offenders referred by the Venango County Courts in lieu of incarceration or as a sentence element after incarceration. The Venango County Court Supervision Service is not a provider of health care, does not pay for health care and does not bill for health care. What health information that is received by this agency is used only to insure compliance with sentence orders or probation elements and as such is for purposes other than health care. For these reasons, the Court Supervision Service has been identified as exempt from being a covered entity under HIPAA. The Court Supervision Service will be expected to provide a HIPAA level of physical security for the limited amount of health information that it does receive.

District Attorney: As an officer of the courts the District Attorney and the District Attorney's staff are in receipt of the same level of health information as the Court and are exempt for the same reasons. This office will also be expected to provide physical security for any health information that does not become a matter of public record.

District Justices 3-1, 3-2, 3-3 and 3-4: Are magisterial courts and are exempt for the same reasons as the County Court. Also like the County Court, the District Courts will be expected to provide physical security for health information that does not become a matter of public record.

Domestic Relations: The only health information received by this agency is a medical notice advising the agency of the ability of the payer of child support to work in his/her normal occupation and therefore make mandated payments. This department does not provide health care, pay for health care or bill for health care and is therefore an exempt agency under HIPAA.

Economic Development: This agency is in no way involved with health care and is exempt by definition.

Emergency Management: Does not generally deal with individual health information, but rather the planning for and coordination of all emergency services during times of natural or man made disaster. Any health information is anecdotal and generally anticipated to be identifying raw numbers of victims or individuals in need of services. As individual health care, payment or billing is outside of the realm of responsibilities for the Emergency Management agency it is exempt from HIPAA involvement.

Garage: As access to protected health information is totally outside of the responsibilities assigned to the county vehicle maintenance garage, it is exempt from HIPAA involvement.

Jury Commissioner: This agency does not provide, pay for or bill for health care, nor does it retain any type of health records and is therefore exempt from HIPAA involvement.

Law Library: There is no involvement with any consumer health information in this agency; it is therefore exempt from HIPAA involvement.

Maintenance: The only access that any maintenance workforce member would have to protected health information would be an accidental observation while working in a HIPAA covered agency. Maintenance as an agency is exempt from HIPAA involvement.

Prothonotary: The Prothonotary office is primarily a record-keeping agency and does not receive or retain health information; provide health care, pay for or bill for health care and is therefore exempt from HIPAA involvement.

Public Defender: This is an office of the courts, and is exempt from HIPAA involvement for the same reason as the courts.

Register and Recorder: This is an office of the courts in which only information specifically sealed by a court action or protocol is **not** considered a public record. As this agency neither provides, pays for or bills for health care it is considered exempt from HIPAA involvement.

Sheriff: This office of county government is part law enforcement, part security and often involved with processing court papers as well as inmates, prisoners and defendants. The Sheriff and his staff do not provide, pay for or bill for health care, and are therefore exempt from HIPAA involvement.

Tax Claim Bureau: Receives, stores, and uses no health information, whatever. This department has no involvement with health care and is therefore exempt from HIPAA involvement.

Treasurer: This agency does not maintain health information, provide health care, pay for or bill for health care and is therefore exempt from HIPAA involvement.

Voter Registration: All records in Voter Registration are open to the public as a requirement of law. This agency does not provide, pay for or bill for health care and is therefore exempt from HIPAA involvement.

Weatherization: This program is not in any way involved with health care and is therefore exempt from HIPAA involvement.

911: The Venango County 911 center is the radio dispatch center for police, fire and ambulance emergency calls. Upon a recent review it was determined that the ambulance portion of the 911 activities made up approximately 25% of the business. Individual medical information is often not received and discernable files based upon individual identification do not exist. As an Emergency dispatch center no direct contact exists between the subject of the dispatch and the 911 staff and therefore no direct service relationship does exist. There is no opportunity to protect health information as all medical information received is transmitted by open frequency radio communications to the actual providers of emergency medical services and for that reason no expectation of privacy can exist.

Because of the emergency nature of the 911 center operations it is exempt from HIPAA compliance, however any physical records, which may be hereinafter exist, will be subject to a HIPAA level of physical security.

VENANGO COUNTY, PENNSYLVANIA
HIPAA –HITECH POLICIES AND PROCEDURES

SECURITY

Purpose
45 CFR ss 164.530(c)(1) Requires a covered entity to have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. The American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) identifies the requirement that covered entities and their Business Associates must either adequately encrypt and otherwise protect all electronically stored or transmitted Protected Health Information or provide for breach policies should the data be lost or the system breached.

Policy
It is the policy of the County of Venango to protect and safeguard the privacy of its clients' private health information, including information that may be contained in electronic, written and/or oral communications, pursuant to the requirements of the HIPAA Privacy Regulations. The following HIPAA Security Policies when fully in effect shall be considered the county's process for protecting all confidential client information: recorded, transmitted or stored in electronic or magnetic format.

NOTE:
Throughout the following sections, Venango County is hereinafter referred to as "county."

TABLE OF CONTENTS

I. COUNTY OF VENANGO HIPAA SECURITY POLICY ACCEPTABLE USE POLICY & PROCEDURES

Overview

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the county network. This policy explains how county information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using county resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

Purpose

Since inappropriate use of county systems exposes the county to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of county information technology resources for the protection of all parties involved.

Scope

The scope of this policy includes any and all use of county IT resources, including but not limited to cell phones, tablets, computer systems, email, the network, the county Internet connection, any digital device.

Policy

E-mail Use: Personal usage of county email systems is permitted as long as A) such usage does not negatively impact the county computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

- The user is prohibited from forging email header information or attempting to impersonate another person.

- E-mail is an insecure method of communication, and thus information that is considered confidential or proprietary to the county may not be sent via email, regardless of the recipient, without proper encryption.

- It is the county policy to utilize ZIX encryption email when sending information to an outside entity containing any identifiable client information or e-mails of a confidential nature.

- Forwarding of e-mail generated through the County e-mail system to a staff's personal e-mail account is strictly prohibited.
- Synching of county e-mail to a county owned or personal cell phone/ tablet is permissible if the cellular devise is password protected. Should the device be lost or stolen, it is staffs responsibility to inform the Security Officer immediately. Steps will then be taken to remotely wipe all data from the device.

- It is county policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that detailed information about the use of email may be covered in the county's Email Policy.

Confidentiality: Confidential data:
A) The need to provide confidential data to sources outside the county often occurs. It is staff responsibility to relay information in accordance with County security policies and procedures.

B) Should not be posted on the Internet or any publicly accessible systems, and

C) Should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

Network Access: The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

Social Networking: Blogging or other forms of social media or technology include but are not limited to video, pictures, or wiki postings, sites such as Facebook and Twitter, chat rooms, personal blogs or similar forms of online journals, diaries or personal newsletters. At no time is identifying information (i.e. name, picture, etc.) about clients to be exchanged through or posted on any social media belonging to employees, volunteers, or contractors. On occasion social networking is used to promote County activities and events; this is done only with the permission of the Security Officer.

Monitoring and Privacy: Users should expect no privacy when using the county network or county resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The county reserves the right to monitor any and all use of the computer network. To ensure compliance with county policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

Circumvention of Security: Using county-owned or county-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited

Non-County-Owned Equipment: Non-county equipment is prohibited on the county's network, unless authorized by the Security Officer.

Personal Storage Media: The County does not permit the use of personal storage media, (which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers), on the county network. Use of county issued

individual storage media (including USB or flash drivers, external hard drives or CD/DVD writers) will be permitted only if the media is capable of being password protected and encrypted.

Reporting of Security Incident : If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or the HIPAA Confidentiality and Security Officers and follow any applicable guidelines as detailed in the county Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains county information.
- Loss or theft of ID badge or keycard (Contact Human Resources rather than HIPAA Officers)
- Suspected compromise of information sent/ received via e-mail or fax.
- Any other suspicious event that may impact the county's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor and/or agency director as well as the HIPAA Confidentiality and/or Security Officers. Users must not withhold information relating to a security incident or interfere with an investigation.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

II. COUNTY OF VENANGO HIPAA SECURITY POLICY BACKUP POLICY & PROCEDURES

Overview

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will

be used more frequently than a contingency planning document. A county's backup policy is among its most important policies.

Purpose
The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

Scope
This policy applies to all data stored on county systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

Definitions
Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Backup Media: Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Backup: A backup that makes a complete copy of the target data.

Incremental Backup: A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

Restoration: Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

Policy
Identification of Critical Data: The county must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.
Data to be Backed Up: This backup policy balances the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to county operation and/or employee job function.

- All information stored on the county file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.

- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

Backup Frequency: Backup frequency is critical to successful data recovery. The county has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Incremental: Monday thru Thursday

Full: Weekly (Friday)

Off-Site Rotation: Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the county's uptime requirements. The county has determined that backup media must be rotated off-site at least once per week.

Backup Storage: Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, county data, precautions must be taken that are commensurate to the type of data being stored. The county has set the following guidelines for backup storage.

When shipped off-site, backups should be reasonably secured from theft or fire. A hardened facility (i.e., commercial backup service or safe deposit box) can be used but is not required. Online backups are allowable if the service meets the criteria specified herein.

Backup Retention: When determining the time required for backup retention, the county must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The county has determined that the following will meet all requirements (note that the backup retention policy must confirm to the county's data retention policy and any industry regulations, if applicable):

Incremental Backups must be saved for one week.

Full Backups must be saved for one month.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

III. COUNTY OF VENANGO HIPAA SECURITY POLICY CONFIDENTIAL DATA POLICY & PROCEDURES

Purpose: This policy lays out standards for the use of confidential data, and outlines specific security controls to protect this data.

Scope: The scope of this policy covers all county-confidential data, regardless of location. Also covered by the policy are hardcopies of county data, such as printouts, faxes, notes, etc.

Definitions
Authentication: A security method used to verify the identity of a user and authorize access to a system or network.

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device: A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Policy
Treatment of Confidential Data: For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

Storage: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

Destruction: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Storage media (CD's, DVD's): physical destruction is required and can be completed by the employee supervisor.

- Hard Drives/Systems/Mobile Storage Media: physical destruction is required. This process will conducted by the HIPAA security officer or designee.

Use of Confidential Data: A successful confidential data policy is dependent on the users knowing and adhering to the county's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

- Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."

- Users must only access confidential data to perform his/her job function.

- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.

- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.

- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.

- If confidential information is shared with third parties, such as contractors or vendors, a Business Associate Agreements must govern the third parties' use of confidential information. Refer to the county's outsourcing policy and Business Associate Agreements for additional guidance.

- If confidential information is shared with a third party, the county must indicate to the third party how the data should be used, secured, and, destroyed. Refer to the Business Associate Agreements for additional guidance.

Security Controls for Confidential Data: Confidential data requires additional security controls in order to ensure its integrity. The county requires that the following guidelines are followed:

- Authentication. Must be used for access to confidential data

- Physical Security. Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.

- Printing. When printing confidential data the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.

- Faxing. When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.

- Emailing. Confidential data must not be emailed outside the county without the use of strong encryption.

- Confidential data must never be stored on non-county-provided machines (i.e., home computers).

Examples of Confidential Data: The following list is not intended to be exhaustive, but should provide the county with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee or customer social security numbers or personal information

- Medical and healthcare information

- Electronic Protected Health Information (EPHI)

- Network diagrams and security configurations

- Passwords

- Bank account information and routing numbers

- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

Emergency Access to Data: In the event that access in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems. You are to contact a member of the MIS staff to gain access to the needed information. The procedure should answer the following questions:

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

IV. COUNTY OF VENANGO HIPAA SECURITY POLICY DATA CLASSIFICATION POLICY & PROCEDURES

Overview
Information assets are assets to the county just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to county operations and the confidentiality of its contents. Once this has been determined, the county can take steps to ensure that data is treated appropriately.

Purpose
The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

Scope
The scope of this policy covers all county data stored on county-owned, county-leased, and otherwise county-provided systems and media, regardless of location. Also covered by the policy are hardcopies of county data, such as printouts, faxes, notes, etc.

Definitions
Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Backup To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Data Device A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Policy
Data Classification: Data residing on county systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.

3. Operational: includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

Data Storage: The following guidelines apply to storage of the different types of county data.

Personal: There are no requirements for personal information.

Public: There are no requirements for public information.

Operational: Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

Critical: Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

Confidential: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

Data Transmission: The following guidelines apply to transmission of the different types of county data.

Personal: There are no requirements for personal information.

Public: There are no requirements for public information.

Operational: No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

Critical: There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

Confidential: Strong encryption must be used when transmitting confidential data, outside the county's network. Confidential data must not be left on voicemail systems, either inside or outside the county's network, or otherwise recorded.

Data Destruction: The following guidelines apply to the destruction of the different types of county data.

Personal: There are no requirements for personal information.

Public: There are no requirements for public information.

Operational : Cross-cut shredding is required for documents. Storage media should be appropriately sanitized/wiped or destroyed.

Critical: There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

Confidential: Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding or professional shredding service is required.

- Storage media (CD's, DVD's): physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media: physical destruction is required and conducted by the HOPAA Security Officer or designee.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

V. COUNTY OF VENANGO HIPAA SECURITY POLICY
E-MAIL POLICY & PROCEDURES

Refer to Hipaa Confidentiality E-Mail Policy XVI on Page 83

Emailing Confidential Data: Email is an insecure means of communication. The County of Venango requires that any email containing confidential information sent external to the county be encrypted using commercial-grade, strong encryption.

Encryption is encouraged, but not required, for emails containing confidential information sent internal to the county. When in doubt, encryption should be used.

Further guidance on the treatment of confidential information exists in the county's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county **will** report such activities to the applicable authorities.

VI. COUNTY OF VENANGO HIPAA SECURITY POLICY
GUEST ACCESS POLICY & PROCEDURES

Overview
Guest access to the county's network is often necessary for customers, consultants, or vendors who are visiting the county's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on the county's network. Guest access to the county's network must be tightly controlled.

Purpose
The county may wish to provide network access as a courtesy to guests wishing to access the Internet, or by necessity to visitors with a business need to access the county's resources. This policy outlines the county's procedures for securing guest access.

Scope
The scope of this policy includes any visitor to the county wishing to access the network or Internet through the county's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse the county's network.

Definitions
Account: A combination of username and password that allows access to computer or network resources.

Guest: A visitor to the county premises who is not an employee.

Policy
Granting Guest Access: Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network, or access the Internet from the county network.

AUP Acceptance: Acceptance of the county's Acceptable Use Policy (AUP) is not required for guest access.

Approval: Guest need for access will be evaluated and provided on a case-by-case basis. This should involve management approval if the request is non-standard.

Account Use: The county may provide a generic guest account that can be re-used by different guests. If these accounts are offered, they are only to be used by guests. Users with network accounts must use their accounts for network access.

Security of Guest Machines: Guests are expected to be responsible for maintaining the security of his or her machine, and to ensure that it is free of viruses, Trojans, malware, etc. The county reserves the right to inspect the machine if a security problem is suspected, but will not inspect each guest's system prior to accessing the network.

Guest Access Infrastructure Requirements: Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network, since guests have typically not undergone the same amount of scrutiny as the county's employees. This must be weighed, however, with the costs and technical issues that come with providing such separation. At this time the county does not provide any specific requirements for guest access infrastructure. Guest access should be provided prudently and monitored for appropriateness of use.

Restrictions on Guest Access: Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The county will evaluate the need of each guest and provide further access if there is a business need to do so.

Monitoring of Guest Access: The county's policy is that if it is granting access to a guest, that guest is a trusted user. As such, the county does not wish to monitor guest access.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe

penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

VII. COUNTY OF VENANGO HIPAA SECURITY POLICY INCIDENT RESPONSE POLICY & PROCEDURES

Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the county's information assets, and outlines steps to take in the event of such an incident.

Purpose

This policy is intended to ensure that the county is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from a security practices perspective.

Scope

The scope of this policy covers all information assets owned or provided by the county, whether they reside on the corporate network or elsewhere.

Definitions

Encryption; The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Malware; Short for "malicious software." A software application designed with malicious intent. Viruses and Trojans are common examples of malware.

Mobile Device: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Smartphone/ Tablet: A mobile telephone that offers additional applications, such as PDA functions and email.

Trojan: Also called a "Trojan Horse." An application that is disguised as something innocuous or legitimate, but harbors a malicious payload. Trojans can be used to covertly and remotely gain access to a computer, log keystrokes, or perform other malicious or destructive acts.

Virus: Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

WEP: Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WPA: Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

Policy
Types of Incidents: A security incident, as it relates to the county's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

• Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.

• Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, camera, Smartphone/ Tablet, portable storage device, or other digital apparatus that may contain county information.

Preparation: Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.

Confidentiality: All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers.

Electronic Incidents: When an electronic incident is suspected, the county's goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

2. Disable the compromised account(s) as appropriate.

3. Report the incident to the HIPAA Security Officer.

4. Backup all data and logs on the machine, or copy/image the machine to another system.

5. Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?

6. Notify county management/executives as appropriate.

7. Contact an IT Security consultant as needed.

8. Determine how the attacker gained access and disable this access.

9. Rebuild the system, including a complete operating system reinstall.

10. Restore any needed data from the last known good backup and put the system back online.

11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.

12. Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done differently?

13. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

Physical Incidents: Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable polices, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft of inadvertent loss by a user, but they must be treated as if they were targeted at the county.

The county must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

Response: Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
    a. If not, refer to "Loss Contained" below.
    b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
    a. If strong encryption was used, refer to "Loss Contained" below.
    b. If not, refer to "Data Loss Suspected" below.

Loss Contained: First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the HIPAA Security Officer. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

Data Loss Suspected: First, notify the HIPAA Privacy Officer if confidential data may have been breached, HIPAA Security Officer, IT Team & legal counsel, so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

Notification: If an electronic or physical security incident is suspected to have resulted in the loss of third-party/customer data, notification of the affected public or agencies must occur. (See Breach Notification Policy in the HIPAA Confidentiality Policy Section XX on page 96)

The first step must be discussions with the HIPAA Privacy and Security Officers and legal counsel to determine an appropriate course of action. Notification should occur in a prompt, organized and consistent manner.

Managing Risk: Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to the county.

Risk Assessment: A formal risk assessment is a good way to manage risk of a security incident. A proactive risk assessment may be performed at the discretion of the HIPAA Security and Privacy Officers. If an assessment is performed, it should be an accurate and thorough assessment of the potential risks (man-made and natural) and any vulnerability to the confidentiality, integrity, and availability of the county's critical or confidential information.

Risk Management Program: A risk management program may be adopted if deemed appropriate by the HIPAA Security Officer. If implemented, the program should cover any risks known to the county (possibly identified by a risk assessment), and insure that reasonable security measures are in place to mitigate those risks to an acceptable level.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

VIII. COUNTY OF VENANGO HIPAA SECURITY POLICY
MOBILE DEVICE POLICY & PROCEDURES

Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

Purpose

The purpose of this policy is to specify county standards for the use and security of mobile devices.

Scope

This policy applies to county data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with county data.

Definitions

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media: A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password: A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Portable Media Player: A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Cell/ Smartphone: A mobile telephone that offers additional applications, such as PDA functions and email.

Policy

Physical Security: By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The county shall carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Mobile devices should be kept out of sight when not in use.

- Care should be given when using or transporting mobile devices in busy areas.

- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove

box.

Data Security: If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting county data. The following sections specify the county's requirements for data security as it relates to mobile devices.

Laptops: Laptops require a username and password login. Laptops that contain confidential data will be secured with a Hard Drive password if available, if not then an encrypted partition will be setup on the laptop for storing any confidential data.

Tablets/Cell Phones: If data stored on the device is especially sensitive or contains individually identifiable health information of any client, the cell phone or device must be password protected.

USB Flash Drive: Storage of county data on such devices is permitted and encryption is required. The USB Drive used must be capable of Password protection and AES hardware encryption. These drives will be issued by the MIS Department. Any USB Drives that are not capable of encryption will be removed from service. Privately owned devices may not be used to store any county data.

Portable Media Players: No county data can be stored on personal media players.

Other Mobile Devices: Unless specifically addressed by this policy, storing county data on other mobile devices, or connecting such devices to county systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the HIPAA Security Officer.

Connecting to Unsecured Networks: Users must not connect to any outside network without a secure, up-to-date software firewall and virus software configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the county.

General Guidelines: The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a county-provided mobile device must be reported immediately.

- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.

- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

- Storing confidential data on non-county-provided mobile devices is expressly prohibited.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

IX. COUNTY OF VENANGO HIPAA SECURITY POLICY NETWORK ACCESS AND AUTHENTICATION POLICY & PROCEDURES

Overview

Consistent standards for network access and authentication are critical to the county's information security and are often required by regulations or third-party agreements. Any user accessing the county's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with county standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

Scope

The scope of this policy includes all users who have access to county-owned or county-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the county's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

Definitions

Antivirus Software: An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Authentication: A security method used to verify the identity of a user and authorize access to a system or network.

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Password: A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Policy
Account Setup: During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted least amount of network access required to perform his or her job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

Account Use: Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (firstinitial-lastname)
- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must not be given administrator access unless this is necessary to perform his or her job function.
- Occasionally guests will have a legitimate business need for access to the county network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

Account Termination: When managing network and user accounts, it is important to stay in communication with the departments so that when an employee no longer works at the county, that employee's account can be disabled. Venango County Human Resources shall promptly report terminations or transfers to the MIS department for user account maintenance. Terminations will be reported immediately and transfers within 48 hours.

Authentication: User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

Use of Passwords: When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the county's Password Policy.

Remote Network Access: Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the county requires additional scrutiny of users remotely accessing the network. The county's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

Screensaver Passwords: Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are encouraged to be activated after 15 minutes of inactivity.

Failed Logons: Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the county must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the HIPAA Security Officer.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

X. COUNTY OF VENANGO HIPAA SECURITY POLICY NETWORK SECURITY POLICY & PROCEDURES

Overview
The county wishes to provide a secure network infrastructure in order to protect the integrity of county data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

Purpose
The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the county's comprehensive set of IT and HIPAA security policies. However, this policy purposely

avoids being overly-specific in order to provide some latitude in implementation and management strategies.

Scope
This policy covers all IT systems and devices that comprise the county network or that are otherwise controlled by the county.

Definitions
ACL: A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Antivirus Software: An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Firewall: A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

IDS: Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

IPS: Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

Password: A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

RAID: Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

Switch: A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.

VLAN: Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Virus: Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

Policy
Network Device Passwords: A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

Password Construction: The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 6 characters
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

Failed Logons: Repeated logon failures can indicate an attempt to `crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the county must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the HIPAA Security Officer.

Change Requirements: Passwords must be changed according to the county's Password Policy. Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a county network or system administrator leaves the county, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.

Administrative Password Guidelines: As a general rule, access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security

Firewalls: Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the county network through the use of a firewall.

Configuration: The following statements apply to the county's implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- No unnecessary services or applications should be enabled on firewalls. The county should use `hardened' systems for firewall platforms, or appliances.

- Clocks on firewalls should be synchronized with the county's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- The firewall must log dropped or rejected packets.

Disposal of Information Technology Assets: IT assets, such as network servers and routers, often contain sensitive data about the county's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the county must be removed before disposal.

- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

- Physical destruction of the device's data storage mechanism (such as its hard drive or solid state memory) is required. If physical destruction is not possible, the HIPAA Security Officer must be notified.

Network Documentation: Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the county's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

Network documentation should include:

- Network diagram(s)

- System configurations

- Firewall ruleset

- IP Addresses

- Access Control Lists

The county encourages network documentation, but does not require it.

Antivirus/Anti-Malware: Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire county. The county provides the following guidelines on the use of antivirus/anti-malware software:

- All county-provided user workstations must have antivirus/anti-malware software installed.

- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.

- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually

- In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

- For no reason should Antivirus/Anti-Malware software be disabled on the computer unless done so by MIS staff.

Software Use Policy: Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The county provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the county's software must be stored in a secure location.

- Open source and/or public domain software can only be used with the permission of the HIPAA Security Officer.

- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.

- Vulnerability alerts should be monitored for all software products that the county uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

XI. COUNTY OF VENANGO HIPAA SECURITY POLICY COUNTY PASSWORD POLICY & PROCEDURES

Overview
A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

Purpose
The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them

create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

Scope
This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

Definitions
Authentication: A security method used to verify the identity of a user and authorize access to a system or network.

Password: A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Policy
Construction: The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 6 characters

- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Confidentiality: Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone

- Users must not share their passwords with others (co-workers, supervisors, family, etc.)

- Users must not write down their passwords and leave them unsecured

- Users must not check the "save password" box when authenticating to applications

- Users must not use the same password for different systems and/or accounts

- Users must not send passwords via email

Change Frequency: In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The organization

may use software that enforces this policy by expiring users' passwords after this time period.

Incident Reporting: Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the HIPAA Security Officer. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the HIPAA Security Officer will request that the user, or users, change all his or her passwords.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

XII. COUNTY OF VENANGO HIPAA SECURITY POLICY
COUNTY PHYSICAL SECURITY POLICY & PROCEDURES

Overview
Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the county's physical network infrastructure. In order to secure the county data, thought must be given to the security of the county's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

Purpose
The purpose of this policy is to protect the county's physical information systems by setting standards for secure operations.

Scope
This policy applies to the physical security of the county's information systems, including, but not limited to, all county-owned or county-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the county's office is covered by this policy.

Please note that this policy covers the physical security of the county's Information Technology infrastructure, and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must taken to ensure that this policy is consistent with any existing physical security policies.

Definitions

Biometrics: The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Datacenter: A location used to house a county's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Keycard: A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Mobile Device: A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Tablet / cell -Smartphone: A mobile telephone that offers additional applications, such as PDA functions and email.

Uninterruptible Power Supplies (UPSs): A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

Policy
Security: At a minimum, the county will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the county's assets.

Physical Data Security: Certain physical precautions must be taken to ensure the integrity of the county's data. At a minimum, the following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.

- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.

- Users must log off, lock or shut down their workstations when leaving for an extended time period, or at the end of the workday.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

XIII. COUNTY OF VENANGO HIPAA SECURITY POLICY
REMOTE ACCESS POLICY & PROCEDURES

Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the county's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

Purpose

This policy is provided to define standards for accessing county information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

Scope

The scope of this policy covers all employees, contractors, and external parties that access county resources over a third-party network, whether such access is performed with county-provided or non-county-provided equipment.

Definitions

Modem: A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access: The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Policy

Prohibited Actions: Remote access to corporate systems is only to be offered through a county-provided means of remote access in a secure fashion. The following are: specifically prohibited:

- Installing a modem, router, or other remote access device on a county system without the approval of the HIPAA Security Officer.
- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the HIPAA Security Officer.
- Use of non-county-provided remote access software.

Use of non-county-provided Machines: Accessing the county network through home or public machines can present a security risk, as the county cannot completely control the security of the system accessing the network. Use of non-county-provided machines to access the county network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed
- Its software patch levels are current
- It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

Client Software: The county will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

Network Access: There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

Applicability of Other Policies: This document is part of the county's cohesive set of HIPAA security and confidentiality policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement: This policy will be enforced by the HIPAA Security Officer, Privacy Officer and/or Human Resources Office. Violations may result in disciplinary action by the County Commissioners, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of county property (physical or intellectual) are suspected, the county will report such activities to the applicable authorities.

Glossary of Terms

Access: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource. 45 CFR § 164.304

Authorization: A document signed and dated by the individual who authorizes use and disclosure of protected health information for reasons other than treatment, payment or health care operations. An authorization must contain a description of the protected health information, the names or class of persons permitted to make a disclosure, the names and class of persons to whom the covered entity may disclose, an expiration date or event, an explanation of the individual's right to revoke and how to revoke, and a statement about potential re-disclosures.

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, 'compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at § 164.514(e) (2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) 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 in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a CE or BA 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. ARRA/HITECH Title XIII Section 13400; §164.402,

Business Associate: (1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

Business Associate Agreement: A contract between a covered entity and a business associate

Caseworker: This term shall include county or contract employees otherwise identified as: Case Managers, Care Managers, Intensive Case Managers, Service Coordinators, Supports Coordinators or other equivalent position including their immediate supervisors.

CMS: Centers for Medicare & Medicaid Services within the United States Department of Health and Human Services.

Consent: A document signed and dated by the individual that a covered entity must obtain prior to using or disclosing protected health information to carry out treatment, payment or health care operations. A consent must be in plain language, inform the individual that protected health information may be used to carry out treatment, payment and health care operation, refer to the notice of privacy practices, state that the individual has a right to request restriction on how protected health information is used or disclosed, and state that the individual has the right to the revoke the consent.

Correctional Institution: Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody.
Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

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 this subchapter.

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.

HHS: The United States Department of Health and Human Services

Designated Record Set: The medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or medical records and billing records used by or for the covered entity to make decisions about individuals.

Disclosure: The release, transfer, provision of access to, or divulging of information outside the entity holding the information.

Electronic Health Record: An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Electronic Media: This term is broadly defined and includes both (1) electronic storage and (2) electronic transmission media. That said, the following language within this definition excludes certain transmission: Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Health Care: Care, services or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, palliative care and counseling, service, assessment or procedure with respect to the physical or mental condition or functional status, of an individual or that affects the structure or function of the body; and

2. Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health Care Clearinghouse: A public or private entity that does either of the following:

1. Processes health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations: Has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations [CFR]: "Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g)[1] are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

i) Management activities relating to implementation of and compliance with requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514,[2] creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity."

[1] "(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use of disclose such protected health information for any other purpose, except, as may be required by law."

[2] "Other requirements relating to uses and disclosures of protected health information."

Health Care Provider: A provider of services 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:

1. 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
2. Relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual.

Health Maintenance Organization (HMO): A federally qualified HMO, and any organization recognized as an HMO under State law.

Health Oversight Agency: An agency or authority of the United States, Pennsylvania or a political subdivision of a state, or a person or entity acting under a grant of authority from such public agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan: An individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act).

Hybrid Entity: A single legal entity that is a covered entity and whose covered functions are not its primary functions.

Indirect treatment relationship: A relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and

2. The health care provider typically provides services or products or reports, the diagnosis or results associated with the health care directly to another health care provider, who provides the services or products or reports directly to the individual.

Individual: The person who is the subject of protected health information.

Individually Identifiable Health Information: That 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; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 CFR § 164.503.

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

Law Enforcement Official: Any officer or employee of an 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 45 CFR § 164.103

Marketing: To make a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

1. Marketing does not include communications that are made by a covered entity for the purpose of describing the entities participating in a health care provider network or health plan network or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or that are tailored to the circumstances of a particular individual and the communications

are made by a health care provider to an individual as part of the treatment of the individual and for the purpose of furthering the treatment of that individual; or made by a health care provider or health plan to an individual in the course of managing the treatment of that individual; or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers or settings of care.

2. A communication described above is not included in marketing if the communication is made orally, or the communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

Notice of Privacy Practices: A notice to the individual of the uses and disclosures of protected health information and the individual's rights and the covered entity's legal duties with respect to protected health information.

Organized Health Care Arrangement: A clinically integrated care setting in which individuals typically receive health care from more than one health care provider or an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities.

Payment: The activities undertaken by:

1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

2. A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

The activities in paragraphs (1) & (2) of this definition relate to the individual to whom health care is provided.

Personal Representative: An executor or administrator authorized by law to act on behalf of an individual's estate is a personal representative. The representative will be treated as the individual for purposes of disclosure of protected health information.

Plan Administration Functions: Administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Privacy Rule: The final privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which created national standards to protect medical records and other protected health information. The final rule went into effect September, 23, 2013.

Protected Health Information (PHI): Individually identifiable health information that is maintained or transmitted in any form or medium. This information can identify an individual's past, present or future medical or mental condition. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act.

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.

Public Health Authority: An agency or authority of the United States, Pennsylvania, a political subdivision of a State or a person or entity acting under a grant of authority from or contract with such public agency that is responsible for public health matters as part of its official mandate.

Required by Law: A mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders, and court-ordered warrants; subpoenas, or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government providing public benefits.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.

Secretary: Secretary of [U.S. Department of] Health and Human Services.

Security: Has the meaning given such term in section 164.304 of title 45, Code of Federal Regulations [CFR].
"*Security* or *Security measures* encompass all of the administrative, physical, and technical safeguards in an information system."

State: Each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

Summary Health Information: Information that may be individually identifiable health information and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the individually identifiable information has been deleted, except that the geographic information can be aggregated to the level of a five digit zip code.

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:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefit

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that may be prescribed by regulation.

Treatment: The provision, coordination or management of health care 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 an individual or the referral of an individual for health care from one health care provider to another.

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS web site.

1. 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 the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt) 45 CFR Parts 160 and 164; Final Rules Issued *8/19109.* The following encryption processes meet this standard.

A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with 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 Federal Information Processing Standards FIPS 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in the following ways:

A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special

Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. HHS issued guidance on protecting personally identifiable healthcare information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMS (Issued *4/17/09).*

Use: With respect to individually identifiable health information, 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 such covered entity.