LIVINGSTON COUNTY
ADMINISTRATIVE PROCEDURE
HIPAA-2

RESOLUTION #2013-04-107 **LIVINGSTON COUNTY, MICHIGAN** **APPROVED: APRIL 9, 2013**

SUBJECT: SECURITY OF ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

PURPOSE: TO OUTLINE SECURITY MEASURES TO PROTECT AGAINST ANY REASONABLY ANTICIPATED THREATS OR HAZARDS TO THE SECURITY OR INTEGRITY OF EPHI AND AGAINST ANY REASONABLY ANTICIPATED USES OR DISCLOSURES OF EPHI THAT ARE NOT PERMITTED BY LAW. THESE PROCEDURES APPLY TO ALL EMPLOYEES.

DEPARTMENT RESPONSIBLE: INFORMATION TECHNOLOGY SECURITY OFFICER

DATE: APRIL 9, 2013

DEPARTMENTS AFFECTED: ALL DEPARTMENTS/OFFICES

LEGAL CITATION/ REFERENCE: RESOLUTION #2013-04-107 ADOPTING LIVINGSTON COUNTY HIPAA SECURITY POLICIES AND DIRECTING THE APPOINTMENT OF INFORMATION TECHNOLOGY SECURITY OFFICER

OTHER FORMS:

- ATTACHMENT A: EMAIL CONSENT
- ATTACHMENT B: BUSINESS ASSOCIATE COMPLIANCE REQUIREMENTS
- ATTACHMENT C: EXTERNAL BUSINESS PARTNERS NETWORK ACCESS REQUEST
- ATTACHMENT D: BUSINESS PARTNER HIPAA COMPLIANCE AGREEMENT
- ATTACHMENT E: HIPAA TRAINING ELEMENTS

TABLE OF CONTENTS

A. DEFINITIONS

Access-controlled areas: Sections of buildings or entire buildings which have areas secured by locks that require an electronic or physical key to enter. These areas are considered access-controlled whenever the locks are engaged. These areas are not generally accessible by the public and often contain sensitive data.

Best Practice: A technique or methodology that, through experience and research, has proven to reliably lead to a desired result. Most HIPAA Best Practices were discerned by researching the information security practices of major Healthcare providers in response to the HIPAA Security Rule. In general, when the policy refers to Best Practices they are recommendations, not requirements, unless their status as requirements is specifically stated.

Critical Record: Records without which an individual work section or unit would be unable to do its work.

Derivative Record: All records not classified as source records. These records can be reconstructed in their entirety from other systems or records.

Electronic media: Any electronic storage media including memory devices, tape, magnetic or optical disk. Transmission media includes the Internet, extranet, leased lines, dial-up, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including that of paper, fax, voice, and telephone ARE NOT considered to be electronic.

Electronic Protected Health Information (*ePHI*): Individually identifiable health information (past, present or future physical or mental health or condition, or provision of health care) including demographic data that can identify an individual, maintained or transmitted using electronic media. PHI (Protected Health Information) excludes employment records held by the County in its role as employer.

Encryption: The conversion of data into a form which cannot be easily understood by unauthorized people.

External Business Partner: A non-County entity or individual providing contracted services to Livingston County at a static location (either co-located in a County facility or located in a facility independent of any Livingston County organization) with access to the County WAN. Employees of other jurisdictions connecting to the County WAN from a trusted network (e.g., local police and fire agencues) or from outside the WAN (such as over the Internet) are not included in the definition of External Business Partner.

Flash Drive: see JumpDrive.

Health Insurance Portability and *Accountability Act (HIPAA):* An act passed by Congress in 1996 which mandated all health care involved entities to observe specific data format, privacy, security, and identification rules. This procedure is intended to inform Livingston County's implementation of the security rules under HIPAA.

HIPAA Privacy and Security *Training:* Training which includes the elements detailed in the attached HIPAA Training Elements (Attachment E:) shall be deemed to qualify as HIPAA Privacy and Security Training.

ID: When the term appears alone, it refers to the identification cards issued to County workers; when it appears with Log in, Log on, Login, or Logon, it refers to an alpha-numeric code given to each worker with access to the WAN which uniquely identifies them to the network.

Information Resources: Any and all online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablet devices, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Security Event: An unplanned and unexpected information resources access occurrence that does not qualify as an information security incident and where no data exposure occurred. When the status of data exposure is unknown, the occurrence will be classified as an incident and not an event.

Information Security Incident: The word "incident" includes emergencies, attacks, and unauthorized disclosures of information, as well as disasters. It includes unauthorized physical entry into the County's IT Facilities, or attempted unauthorized physical entry to such facilities as well as unauthorized electronic entry or attempted unauthorized electronic entry, into information processing systems, networks, or information storage, or information transmission resources. It includes situations which appear to have risked unauthorized disclosure of information as well as confirmed disclosure. Any violation of a County Security Policy shall be, by itself, considered a Security Incident subject to the reporting and documentation requirements. Note that incidents of computer virus infection are security events requiring reporting but not security incidents unless they involve the disclosure, suspected disclosure, or potential disclosure of data.

Information Technology Security Officer (Security Officer): One or more Security Officers, either the County's Chief Information Officer or appointed by and reporting to the County's Chief Information Officer. Responsible for administering the information security functions within Livingston County. The Security Officer is the County's internal and external point of contact for all information security matters.

Information Technology Department (IT Department*):* The name of the Department responsible for computers, networking and data management for all staff in covered units.

JumpDrive: A device that allows the storage, transfer, and portability of files. Allows the ability to move files from one computer to another with cross platform capabilities via the USB (Universal Serial Bus) port on a computer with no driver installation required.

LAN (Local Area Network): A group of computers and communication devices located together inside of the Livingston County firewalls. In addition to obtaining access to the Livingston County wide area network (WAN), external business partners may be sharing County LANs or using and managing their own LAN.

Log in: See ID.

Mission Critical Record: Records whose loss would result in large numbers of County employees being unable to do their work, or where highly critical and urgent services required by the public would not be able to be performed.

Owner of Record: For files, spreadsheets, documents, etc. that do not constitute applications, the owner is the user logged on when the record was created. For applications, the owner is the employee designated the owner pursuant to the County Information Security Policy.

Password: Any combination of letters, numbers and characters which are entered to gain access to IT systems.

Passphrase: A combination of multiple words, numbers, characters and spaces which are entered to gain access to IT systems

Personal Computer (PC): A computing device, either designed for desktop or portable use, which is designed to provide computing resources to one user at a time.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from Information Resources. These include, but are not limited to, notebook computers, laptop computers, handheld computers, tablet device, and cell phones.

Publicly Accessible Areas: Those areas of County buildings and leased facilities where the general public is permitted full access during normal working hours with no formal escort or supervision.

Public Access PC's: Those PC's the County purposely makes available to the general public or the clientele of County programs or Departments for their use.

Sharing: The provision of information to, or the receiving of information from, another entity, employee, or workgroup, regardless of the purpose for such provision.

Source Record: Source systems or files contain one or more data items that are original input and not contained in other systems or files within the County. Source data is often entered via a keyboard by a system or file user.

Termination: The cessation, or reasonably anticipated cessation, of all work for the County, regardless of cause.

Violation: Any act that is inconsistent with the County's policies or procedures established pursuant to the implementation of the Security Rule provisions of HIPAA, including any attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Visitors: Those persons in work locations with no ongoing permission to be present. Specifically not included are employees, students, volunteers, business associates, or contractors who are permitted access to the location.

VPN (Virtual Private Network): A method of access to the Livingston County WAN via an encrypted tunnel over the Internet. Some external business partners may access the County by VPN services provided by and controlled by Livingston County.

WAN (Wide Area Network): A collection of LAN's connected over a geographically disbursed area.

Windows Account: An account which has permission to log in to the Livingston County Network.

B. POLICIES AND PROCEDURES

1. DATA CLASSIFICATION, STORAGE, BACKUP AND RECOVERY

a. The owner of record must classify record data as:
   - Containing or not containing ePHI;
   - Source or derivative;
   - Not critical nor mission critical or critical or mission critical.

b. Records containing ePHI must be stored securely to prevent unauthorized access to them. Normally this means they will be stored on a server and not on a computing device in the work area.

c. Records containing ePHI that are also source records must be backed up in a manner that will allow them to be restored if they are lost or damaged.

2. NETWORK COMMUNICATION ENCRYPTION

a. To protect external ePHI transmissions, all covered components must:
   - Encrypt the file, document, or folder containing ePHI before transmission or, as an alternative, an encryption mechanism such as an encrypted data stream may be used.
   - Take reasonable precautions to authenticate the receiving party and ensure there is a business need for the requested ePHI. Transmissions of ePHI should include only the minimum amount of PHI necessary to accomplish the business need.

b. Requirements:
   - All encryption mechanisms must support a minimum of, but not limited to, 256-bit encryption.
   - When transmitting ePHI electronically, regardless of the transmission system being used, workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a business need for the ePHI requested.
   - To transmit data securely an application that is able to encrypt data will need to be purchased. Workforce members needing to encrypt data for transmission who lack the software to prepare and securely transmit the data should contact the County's Help Desk for assistance.

c. To protect internal ePHI transmissions, Livingston County will encrypt all internal wireless data transmissions.

3. PASSWORDS

a. Generally:
   - All customer-level (all those without administrative authority) passwords controlling access to WAN level resources (e.g., email, web, desktop computer, etc.) shall be changed every 90 days.
   - All customer-level passwords controlling access to applications containing ePHI which are hosted by the County shall be changed at least every 90 days if the application can support this requirement.

- Passwords must not be inserted into email messages or other forms of electronic communication.
- A generic user identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to ePHI. An additional unique user identification and password must be supplied to access applications and database systems containing ePHI or they must be isolated in network areas off limits to generic passwords.
- Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

b. Password Construction Guidelines:

Everyone shall select a strong password for network access and for all applications which support the enforcement of strong passwords and can otherwise support this requirement. Supporting the requirement means that the application supports password controlled access, supports end user updateable passwords, and supports aging passwords with the ability to notify end users upon password expiration. All applications containing ePHI which are added to the County's hosted applications on or after the effective date of this procedure shall support this requirement.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have numbers and punctuation characters as well as letters e.g., 0-9, -!@#$%A&*O+I_~=\~{}[]:hI;I<>?, .1)
- Are at least eight characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Every user should try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2RP" or "Tmb1W>r~-" or some other variation.

NOTE: Do not use either of these examples as passwords!

c. Passphrases:

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks," where hackers try every word in a dictionary to try to find a password that works.

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOn59Was*&#!#This Morning"

All of the rules above that apply to passwords apply to passphrases. Note that passphrases can also be the sentence itself, though password or passphrase length is limited on most applications. On the Windows log in screen, you can use up to 128 characters.

d. Password Protection Standards:

- Don't use the same password for Livingston County accounts as for other non-Livingston County access (e.g., personal ISP (Internet Service Provider) account, option trading, benefits, etc.). Where possible, don't use the same password for various Livingston County access needs. For example, select one password for the department systems and a separate password for IT systems. Also, select a separate password to be used for Windows account. Don't share Livingston County passwords with ANYONE, including family members, your supervisor, co-workers, administrative assistants or secretaries. All passwords are to be treated as sensitive and confidential Livingston County information.
- Don't write passwords down. Employees can download a password keeper on their PC or phone from a list of providers approved by IT. Do not store passwords in a file on any computer system (including handheld/tablet devices or similar devices) without encryption.
- Don't reveal a password over the phone to anyone.
- Don't reveal a password in an email message.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, or Google Chrome) and don't create batch log in files containing passwords to automate the log in process to on line environments.
- If someone demands a password, refer them to this document or have them call the County's Information Technology Security Officer.
- If an account or password is suspected to have been compromised, report the incident to your manager and the County's Help Desk and change all passwords.

e. Use of Passwords and Passphrases for Remote Access Users:

Access-to the Livingston County WAN via remote access, other than webmail, is to be controlled using either a one-time password authentication or a VPN Fob or RSA token or other hardware or software device provided by the Livingston County IT Department.

4. EMPLOYMENT TERMINATION

a. Covered components must notify the County's Help Desk with respect to a terminating employee (including a volunteer or the separation for an indefinite period for an on-call employee) within two working days of their knowledge of an impending departure and shall immediately notify the Help Desk of an actual departure when no prior notice has been given. Covered components will provide the Help Desk with an accounting of all IT systems with log ins to which the departing workforce member has access.

b. All terminating workforce members not subject to the exception for email below shall have their access to the County WAN eliminated immediately upon termination. Normally, this will coincide with the end of their shift on their final working day.

Human Resources or Program Managers may also notify the Help Desk of anticipated terminations at any time to request that a workforce member's accesses be

eliminated earlier than would otherwise occur under this procedure, for example, at the instant of termination or before, at a time specified by Human Resources.

Managers may seek permission from the Department Director or designee to allow continuing access to the County's email resources for a reasonable time (less than 60 days) following termination. Such exceptions to this procedure shall be in writing to the County's Help Desk and shall specify the time limit on access with that access to be terminated upon expiration of that time. Absent such granted exceptions, the intent of this procedure shall be carried out. The terminating employee's access to all other County computing resources shall still be removed within the time limits set in this procedure.

5. PORTABLE DEVICES

a. Only Livingston County IT Department approved portable computing devices (which would include cellular telephones, tablets or future technology which is able to connect to the County Network or receive email) may be used to access Livingston County Information Resources. All portable computing devices that will access Livingston County Information Resources must be approved by the IT Department. Contact the County Help Desk and request approval. If the IT Department is providing the device no additional approval is required.

b. Portable computing devices and all removable media that contain ePHI must be password protected and hard drive encrypted with remote wipe capabilities. Refer to the documentation that comes with each device or contact the County's Help Desk to request assistance in password protecting your device.

c. Best practices dictate that ePHI should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all Livingston County ePHI data must be encrypted using approved encryption techniques. Contact the County's Help Desk for instructions on approved encryption techniques.

d. Livingston County ePHI data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are used. If transmission of ePHI is necessary via-wireless, contact the County's Help Desk for approved wireless transmission protocols and approved encryption techniques.

e. Non-Livingston County portable devices that require network connectivity must connect only through the wireless guest network and are not allowed to connect to the County's secure network.

f. Unattended portable computing devices must be physically secure. If not in an access control area they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system. For more information please refer to Section 14, the Access Control Procedure.

6. SECURITY SANCTIONS

a. Employees whose actions are determined to be a violation of the HIPAA Security Policies are subject to disciplinary sanctions proportional to the severity of the violation and determined in the same manner and by the same authorities as other personnel rule violations.

b. Non-Employee sanctions (including volunteers, external business partners and contractors) for a violation are specified by contract or if not specified may include restricted or terminated access to County facilities and/or the WAN as determined by the Security Officer in consultation with the Director of the Department in which the violation occurred. The severity of the consequences to the non-employee workforce member must be proportional to the severity of the violation.

7. EXTERNAL BUSINESS PARTNER ACCESS

a. Requests for external business partner access to County WAN Staff must be in writing, from a sponsoring Department, with justification for the access, and sent to the Security Officer. See attached request (Attachment C:) and compliance forms (Attachment D:) required for external business partner access. Any existing agreements or contracts between the sponsoring department and the external business partner should be included with the request. Any request for exceptions to this procedure must be in writing to and granted or denied in writing by the Security Officer.

b. The sponsoring department must require external business partners to:

- Undergo and pass the same (or enhanced) procedures used (including the requirements of this procedure for passwords and log in id's) to ensure network and information security as is practiced for the sponsoring department's employees. These may include but are not limited to criminal history or Michigan Law Enforcement Information Network (LEIN) / National Crime Information Center (NCIC) background checks and signing of confidentiality or non-disclosure agreements.
- Run anti-virus software on all desktop or laptop computers that have Livingston County WAN connectivity.
- Comply with County policy for appropriate use of information technology, complete the sponsoring department's HIPAA training requirements; and comply with all policies and procedures (including those that apply specifically to HIPAA regulations, if applicable) and procedures developed to ensure the security and integrity of the County's network, applications, and information.
- Immediately notify the sponsoring department when network login IDs are no longer in use or required; and sponsoring departments must immediately notify the County's Help Desk.

c. PCs or laptops used by the external business partners must not have connections to any other network. This hardware, and the software loaded thereon, is subject to approval by the IT Department's Security Officer. Contact the County's Help Desk for more information on this requirement if elaboration is needed.

d. When a request is approved, sponsoring departments are to fund any required devices to support the WAN connectivity.

All devices must be provided by County IT staff. County staff will also be solely responsible for management of these devices.

e. Compliance with these security policies and procedures will be monitored by IT and appropriate action taken when non-compliance is identified, up to and including termination of all County network access.

8. BUSINESS ASSOCIATE AGREEMENTS

The Security Official for covered components desirous of sharing ePHI with external entities who are not themselves covered entities must prepare and assure execution of the required business associates agreement, or may contact Human Resources for guidance in the preparation and execution of the required business associate agreements (see attached form, Attachment B:). If non-County entities are connected to the County's WAN, they must comply with section 7 of this procedure, the External Business Partners procedure and its corresponding policy.

9. INFORMATION SECURITY PROGRAM

a. The HIPAA Security Officer has the authority to manage all aspects of the County's HIPAA Security Rule Compliance Program. The Information Technology Security Officer and the HIPAA Security Officer may be the same employee.

b. The HIPAA Security Officer shall convene an Information Security Management Committee whose members shall be designated by the directors of each covered entity County department. This committee will work under, and report to, the County's Chief Information Officer. The committee shall meet at least quarterly to review the current status of the County's information security, to review and advise the Security Officer on any security issues which arise, and to review any information security projects. Designated Departmental members of the Information Security Management Committee shall be known as the Security Officials for their Department. The County's Chief Information Officer shall provide a report to the Livingston County Board of Commissioner's Technology Committee at least on a quarterly basis.

c. All applications in the County other than standard desktop office automation aids (e.g. Microsoft Office, Adobe Acrobat, etc.) shall have an owner designated by the Departmental senior manager assigned to implement HIPAA for the Department where the application originated, was purchased, or within which the application is primarily used. The application owner shall be responsible for authorizing all access to the application and for performing the assessments or reassessments required by this policy for all applications containing ePHI. Each new application in the County shall require this designation and subsequent classification should it include ePHI.

d. All applications containing ePHI are eligible to be selected for random security auditing.

e. All information security incidents shall be handled with the involvement and cooperation of the Information Technology Security Officer.

f. Any exceptions to the security policies or procedures adopted by, or pursuant, to this rule shall be granted solely in writing and shall be documented and signed by the Security Officer. Exceptions must be sought from the Security Officer who shall consult with the Chief Information Officer, if not the same individual, prior to making the determination as to whether or not to approve the exception.

10. EMAIL ENCRYPTION

a. Transmission of ePHI from Livingston County to a patient via an email or messaging system is permitted if the sender has ensured that the following conditions are met:
   - The client or personal representative has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.

- The client or personal representative has authorized Livingston County in writing to use an email or messaging system to transmit ePHI to them. This authorization shall be stored in the patient's record. Departments shall create a form for this purpose substantially similar to the attached (Attachment A:) sample form from the Health Department.
- The email or message contains only the minimum ePHI necessary to accomplish the business purpose of the email.
- The sender and receiver are able to implement a compatible encryption mechanism.

b. The transmission of ePHI from Livingston County to an outside entity other than a client or personal representative via an email or messaging system is permitted if the sender has ensured that the following conditions are met:
   - The receiving entity has been authenticated.
   - The receiving entity is aware of the transmission and is ready to receive said transmission.
   - The sender and receiver are able to implement a compatible encryption mechanism.

c. Best practices suggest that emails containing ePHI not be "broadcast" to email groups and that cc:'s be avoided in order to prevent unintended spread of the information they contain.

d. The transmission of ePHI within Livingston County via an email or messaging system is permitted without additional security measures or safeguards.

11. INFORMATION SECURITY INCIDENT RESPONSE

a. First Actions When Unauthorized Access Problems Occur:
   - Whenever non-IT Department workforce members suspect or learn that unauthorized system access has occurred, they must immediately report such events to their supervisor who will report the incident to the Security Official or the Privacy Official for their Department. The identity of the incident reporter shall be safeguarded at the reporter's request to the extent possible without jeopardizing the County's interests as an employer.
   - Such events that also may have resulted in an unanticipated and unintended release of ePHI or other confidential County data, or where such release is not possible to determine, shall also be reported by that Security Official to the County's Information Technology Security Official.
   - All incidents which investigation discovers may be due to deliberate actions of County workforce members shall, at the CIO's discretion, be referred to the Human Resources Director or their designee to determine appropriate discipline.

b. Inclusion of Information Security Official Information On Web Site: The home page of all County external web sites for Departments shall include contact information (email address and / or phone number) for the Information Technology Security Official.

c. Interference With Reporting Of Information Security Problems: Any attempt to interfere with, prevent, obstruct, or dissuade a staff member in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited and cause for disciplinary action.

d. Immediate Reporting Of Suspected Computer Virus Infection: Computer viruses and other sorts of malicious computer activity constitute an information security event and workforce members shall report such events immediately to the County's Help Desk and to the workforce member's supervisor who will report the incident to the Security Official and Privacy Official for their Department. Such events which also may have resulted, or did result, in an unanticipated and unintended release of ePHI or other confidential County data, or where such release is not possible to determine, shall also constitute reportable information security incidents and be reported by that Security Officer or Privacy Officer.

12. POLICIES AND PROCEDURES; DOCUMENTATION AND REVIEW

See the HIPAA Security Policies and the IT Department Staff Specific HIPAA Procedures (HIPAA-3) for these requirements. There are no procedures relevant to all County staff.

13. WORKSTATION AND DISPOSAL OF INFORMATION

All County Personal Computers (PCs), laptops and handheld/tablet devices will comply with the security measures described in this procedure and general usage guidelines contained in the Information Technology Usage policy. All ePHI shall be disposed of in a manner consistent with record retention requirements and the procedures set forth below.

a. Physical security measures: Note that Public Access PC's are exempt from the requirements of this subsection, 13.a. Where all machines subject to these procedures cannot be made to comply with them prior to 30 days following Board approval of this policy, those machines with access to ePHI shall be made to comply first.

- All PCs located in publicly accessible areas will be secured by attaching a locking cable to the PC and a non-movable fixture.
- Reasonable safeguards must be in place to prohibit unauthorized persons from viewing confidential information such as logins, passwords, or ePHI. This may be accomplished by positioning the monitor such that they cannot view the screen or by installation of a privacy screen.
- Workforce members shall lock out access to their workstation when leaving the area.
- PCs will have a screen saver enabled that will be activated after at most 10 minutes of inactivity.
- The screensaver will require the workforce member's password to unlock it.

b. Authentication requirements:

- All PCs, servers and laptops will be required to have a password authentication mechanism enabled to gain access.
- Each workforce member will have a personally unique login ID to systems containing ePHI and active directory will control access to all directories containing ePHI based on these login IDs.
- Each member will be given the minimum rights to applications, files and directories to perform their job functions.

- Access to applications, files and directories will be tracked to individual logins, and workforce members are responsible for keeping their ID and password private.

c. ePHI on Portable Devices: ePHI shall not be stored permanently on any portable device or media.

d. Authorized storage for ePHI data:

- ePHI shall be stored on Livingston County servers or the servers of County contractors or business associates where formal, HIPAA compliant agreements exist which allow this.
- ePHI shall not be stored on County or Personal PCs, laptops or handheld/tablet devices.
- ePHI must not be permanently stored on portable electronic media, such as floppy disks, zip disks, CD-ROMs or-DVD-ROMs, unless it is for the purpose of archiving the information or used for routine backups. It shall be stored in a lockable, secure area at all times.
- The IT Department shall be informed of all applications and/or files containing ePHI to ensure proper backup and disaster recovery planning can be provided.
- Livingston County prohibits the removal of all devices and media containing ePHI from County facilities without proper authorization from the-manager in charge of the facility.

e. Responsibilities reserved to IT Department staff:

- Unless an exception is granted by the Security Officer, only workforce members who are County IT Department staff or specifically authorized by Chief Information Officer (or his or her designee) are authorized to install software on County owned PCs, laptops and handheld/tablet devices.
- Workforce members that use Livingston County information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, Livingston County may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted.

f. Disposal guidelines:

- Prior to destroying or disposing of any storage device (whether inside or outside of a processing device or a copy machine) or removable media, care must be taken to ensure that any data stored on the device or media be disposed of properly, particularly ePHI. In addition to complying with the requirements in these procedures, all applicable County retention schedules shall be complied with.
- If the device or media contains data which is required or needed, a retrievable copy of the data, particularly ePHI, must be made prior to disposal. Care shall be taken to ensure an accurate and permanent copy is made and that all County retention schedules are complied with.
- If the device or media contains ePHI that is no longer required or needed a data destruction tool shall be used to destroy the data on the device or media prior to disposal. Contact the County's Help Desk for assistance if needed.
- Any form of portable electronic media that once contained ePHI and reaches end of useful life must be destroyed when that information is no longer needed, prior

to placing it in the trash. This should be done by following the methodology set forth in 13.f., 3rd bullet, above.

Prior to the sale or return of any device capable of electronic storage of PHI, including computers, copy machines, cell phones and tablets, IT must be notified by the Security Official so that proper data disposal or destruction may be considered.

- Any of the requirements of this subsection 13.f. must be met by any business associate or contractor of the County providing a contract exists wherein the contractor agrees to be bound by the terms of the State's Records Disposition and Destruction requirements. - See the IT Department Staff-specific procedure (HIPAA-3) for details. Wherever practical, such destruction or data obliteration should be witnessed by a County employee.

14. ACCESS CONTROL AND PHYSICAL SECURITY

a. Identification: Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information nor are they permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information. All workforce members are responsible and accountable for all accesses under their personal identifiers.

b. Physical and Visitor Requirements:

- Workstations shall invoke password-enabled screen savers after a time interval of inactivity to be defined in the workstation procedure.
- Devices connecting to the County's networks shall receive and display an initial message that indicates the user is entering a private network and that unauthorized users should disconnect or log off immediately.
- When leaving a workstation users are required to secure the workstation or properly log out of all applications and networks.
- All site administrators are to ensure that physical security systems comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Visitors must be escorted in access-controlled areas of Livingston County facilities.
- All Livingston County facilities that allow access to controlled areas for visitors will track visitor access with a sign in/out log which will be kept for routine review for one year. When visitors are clients or others who have appointments to visit the areas which are tracked in automated appointment systems, the records in those systems shall suffice as a log. Those records should be maintained according to the design and configuration of those systems. The recommended practice is that such systems should be configured to retain their records for at least a year. These recommended retention times are minimums. Records shall be maintained longer when required by formal record retention schedules.

c. IT Controls

- Electronic access is controlled through authentication. Each session will be uniquely identified and passwords will be used to authenticate identity.

- All files containing protected health information shall have appropriate access controls.

d. Access Authorization:

- Physical and electronic access to protected health information shall be controlled through established rules for granting access, determining initial right of access and modifying the right to access. The appropriate level of control shall be proportionate to user need and the level of risk and exposure to loss or compromise. These rules are to be written and shall be established by the System owners for electronic access to multi-Departmental systems and by the Departments for Departmental systems and Departmentally- controlled facilities for physical access.
- Managers or supervisors are to immediately notify the appropriate authority, i.e. the application administrator, to report all system access need changes based on changes in user duties or employment status.
- Access to specific data elements, files, functions, menus, commands and networks shall be to the minimum necessary to perform the user's responsibilities or job functions.
- Those responsible for managing areas where ePHI is accessible shall assure adequate supervision of non-County employed maintenance personnel and shall establish personnel clearance procedures.
- Managers shall determine the proper access level to be granted to individuals working with protected health information.

15. HIPAA PRIVACY AND SECURITY AWARENESS AND TRAINING

a. County Training Plan:

- All employees in the Hybrid Covered Entity will get the same minimum level of training as set forth in the attached HIPAA Training Elements (Attachment E:). The IT Department provided HIPAA training software will be the prominent training method (with a supplement that covers County-specific policies and procedures). Alternatively, departments will have the flexibility to develop their own training, as long as it covers the elements enumerated on Attachment E:. Such curricula must be reviewed and approved by the County Privacy Officer and Security Officer. For new employees within the Covered Entity, all required HIPAA training shall be completed within 60 days of hire.
- For existing employees, their department's Privacy Official will be responsible for determining their HIPAA security training compliance. If the Privacy Official deems the employees have met the training requirements based on the attached Elements, they will credit the employee as having received training.
- In addition, but not specifically part of the County's compliance effort, Human Resources will include a 10 to 20 minute module on HIPAA in their New Employee Orientations. The New Employee Orientation presentation will cover both privacy and security, and will be presented for general awareness of HIPAA to all employees. This module will also be made available on Sharepoint. All employees new to the County's-Hybrid Covered Entity and all others regularly exposed to ePHI, on, or following Board approval of this policy, shall be enrolled in the IT Department provided training software. This information shall be entered as part of their LAN log-on provisioning and be done by the central account

administration staff. Hiring supervisors or managers submit a form Human Resources who will forward the form to Information Technology to request network access for their staff members. They shall mark the area on that form to indicate the need for HIPAA training.

- Actions to be taken for continued failure to meet the requirement may include removing an employee's access to the County's wide area network and computing resources, removing their access to PHI altogether, or some other combination.

b. Training Documentation Required:

- Employees' required to complete this training and the satisfaction of these requirements shall be tracked by Human Resources. This process shall be automated to the maximum feasible extent. The tracking of all HIPAA training is the responsibility of the HIPAA Privacy Official for each County department in the Hybrid Covered Entity.
- The Privacy Official shall notify the Privacy Officer, in writing,
- in the event an employee has not satisfied the HIPAA training requirements within the required timelines.. The departmental individuals are jointly charged with notifying the employees' managers to remedy the training lack.

16. PROCEDURE AND ABILITY OF COVERED ENTITY DEPARTMENTS TO ESTABLISH SECURITY PROTOCOLS AND PROCEDURES MORE STRINGENT THAN THOSE SET FORTH HEREIN.

- Department Security Officials may, after review and approval of the Security Officer, institute policies, procedures, protocols or other improvements to safeguard the security of PHI so long as such policies, procedures, protocols or other improvements are not less stringent or secure than those set forth herein. However, any such policies, procedures, protocols or other improvements must be reviewed and approved by the Security Officer.

RESOLUTION #2013-04-107	APPROVED: APRIL 9, 2013

S:\WP\Policies\HR Manual\HIPAA - Administrative Procedure 2.doc

ATTACHMENT A: # EMAIL CONSENT FORM

CLIENT NAME: _____ **DOB:** _____ **ID#:** _____

RISK OF USING EMAIL

Transmitting client information by email has a number of risks that clients should consider. These include, but are not limited to the following risks:

Email can be circulated, forwarded and stored electronically and on paper.

Email can be immediately broadcast worldwide and be received by unintended recipients.

Email senders can easily misaddress an email.

Backup copies of email may exist even after the sender or the recipient has deleted his or her copy.

Employers and on-line services have a right to archive and inspect emails transmitted through their systems.

Email can be intercepted, altered, forwarded, or used without authorization or detection.

Email can be used to introduce viruses into computer systems.

Email can be used as evidence in court.

CONDITIONS FOR THE USE OF EMAIL

Livingston County cannot guarantee the security and confidentiality of email communication, and will not be liable for improper use and/or disclosure of confidential information that is not caused by Livingston County's intentional misconduct. Clients must consent to the following conditions:

Email is not appropriate for emergency situations.

All emails containing protected health information to or from a client will be printed out and made part of the client's record.

Livingston County staff may receive and read your email messages.

The client is responsible for protecting his/her password or other means of access to email.

Livingston County is not liable for breaches of confidentiality caused by the client or any third party.

It is the client's responsibility to follow-up and/or schedule an appointment if warranted.

The client shall avoid use of his/her employer's computer to send/receive emails to Livingston County.

The client shall inform Livingston County in writing of changes in his/her email address.

The client shall notify Livingston County in writing when he/she no longer wants to receive email from Livingston County.

CLIENT ACKNOWLEDGEMENT AND AGREEMENT

I acknowledge that I have read and fully understand the information Livingston County has provided me regarding the risks of using email. I consent to the conditions outlined above, and understand that Livingston County may impose other conditions regarding email usage in the future.

CLIENT SIGNATURE: _____ Date: _____

Email address: _____

Attachment B: Health Insurance Portability And Accountability Act of 1966 (HIPAA)

BUSINESS ASSOCIATE COMPLIANCE REQUIREMENTS

A. GENERAL: For purposes of this Contract, Contractor is County's business associate and will comply with the obligations set forth below. Contractor and County agree to amend this section if necessary to allow either party to comply with the Privacy or Security Rule.

B. DEFINITIONS: Terms used, but not otherwise defined in this section, will have the same meaning as those terms in the Privacy Rule and Security Rule.

Designated record set: as defined in 45 CFR 164.501.

Individual: as defined in 45 CFR 164.501 and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule: the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and part 164, subpart A and E.

Protected Health Information: as defined in 45 CFR 164.501, limited to the information created or received by Contractor on behalf of County.

Required by Law: as defined in 45 CFR 164.501.

Secretary: the Secretary of the Department of Health and Human Services or designee.

Security Rule: the Standards for Security of Individually Identifiable Health Information at 45 CFR Part 160 and part 164, subpart A and C.

C. CONTRACTOR'S OBLIGATIONS:

1. Contractor agrees to not use or disclose Protected Health Information (PHI) other than as permitted or required by this Contract or as required by law. Contractor further agrees to use or disclose Protected Health Information only on behalf of, or to provide services to, the Covered Entity in fulfilling Contractor's obligations under this contract, and to not make uses or disclosures that would violate the Privacy Rule if done by County or violate County's Minimum Disclosure policy.
2. When using, disclosing, or requesting PHI, Contractor agrees to make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request, with the following exceptions:
    a. Disclosures to or requests by a health care provider for treatment
    b. Disclosures made to the individual about his or her own protected health information
    c. Uses or disclosures authorized by the individual
    d. Disclosures made to the Secretary of Health and Human Services in accordance with the HIPAA Privacy Rule

e. Uses or disclosures that are required by law

f. Uses or disclosure that are required for compliance with the HIPAA Transaction Rule

3. Contractor agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

4. Contractor agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by 45 CFR 164 Subpart C.

5. Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use of Protected Health Information by Contractor in violation of the requirements of this Contract.

6. Contractor agrees to report to County any security incident, including use or disclosure of the Protected Health Information not provided for by this Contract of which it becomes aware.

7. Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Contractor on behalf of County, agrees to the same restrictions and conditions that apply through this Contract to Contractor with respect to such information.

8. Contractor agrees to provide access within 5 working days of County's request to Protected Health Information about an individual contained in a designated record set. If an individual requests access to information directly from Contractor, Contractor agrees to forward the request to County within 2 working days of receipt. County will be responsible for any denials of requested Protected Health Information.

9. Contractor agrees to make any amendments to Protected Health Information in a Designated Record Set that the County directs or agrees to pursuant to 45 CFR.164.526 within 10 working days of County's request.

10. Contractor agrees to make internal practices, books and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Contractor, on behalf of, County available to County or Secretary upon request of County or Secretary, for purposes of the Secretary determining County's Compliance with the Privacy Rule or the Security Rule.

11. Contractor agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for County to respond to a request by an individual for an accounting of disclosure of Protected Health Information in accordance with 45 CFR 164.528. Contractor will make available, at a minimum, the following information: (i) the date of the disclosure, (ii) the name of the entity or person who received the Protected Health Information, and if known, the address of such entity or person, (iii) a brief description of the Protected Health Information disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. Contractor hereby agrees to implement an appropriate record keeping process to comply with this section

12. Contractor agrees to provide County or an Individual, within 10 working days of the request from County or individual, information collected under Item 9 of this section, to permit County to respond to a request by an Individual for an accounting of disclosure of Protected Health Information in accordance with 45 CFR 164.528.

D. TERMINATION

1. Notwithstanding any other termination provisions in this Contract, County may terminate this contract in whole or in part upon 5 working days written notice to Contractor if the Contractor breaches any provision contained in this section, HIPAA Compliance, and fails to cure the breach within the 5 working day period; provided, however, that in the event termination is not feasible County may report the breach to the Secretary.

2. Upon termination of this Contract for any reason, Contractor will extend the protections of this section, HIPAA Compliance, to any records containing PHI that contractor is required to retain under any provision of this Contract.

ATTACHMENT C: IT / INFRASTRUCTURE

ATTACHMENT D: EXTERNAL BUSINESS PARTNER HIPAA COMPLIANCE AGREEMENT

[Department] is a covered entity as that term is defined in the Health Information Portability and Accountability Act (HIPAA). [Contractor] is an External Business Partner of County providing contracted services to [Department] at [location] with access to the Livingston County wide area network (WAN). Contractor and/or its employee(s) is therefore a member of County's "workforce" as that term is defined in HIPAA, for HIPAA purposes only, and must comply with the County's rules regarding protection of personal health information (PHI) and electronic personal health information (ePHI).

Contractor agrees as follows:

Contractor and each of its employee(s) to be granted access have read each of the following County Policies and Procedures related to protection of PHI:

Livingston County HIPAA Privacy Policies: Resolution #2013-04-107

Livingston County HIPAA Security Policies: [Citation to be added later when policies are formally adopted]

Livingston County Personnel Rule: The Acceptable Use of Information Technology: Personnel Rule-_____.

Contractor and its employee(s) agree to abide by all policies and procedures listed above.

Contractor and its employee(s) agree not to use or disclose PHI or ePHI other than as permitted or required by this Contract or as required by law.

Contractor further agrees to use or disclose PHI or ePHI only on behalf of or to provide services to the County in fulfilling Contractor's obligations under this contract, and not to make uses or disclosures that would violate HIPAA if done by County, or violate County's Minimum Disclosure policy.

Contractor agrees to immediately report to County any incident involving use or disclosure of PHI or ePHI not provided for by this contract of which it becomes aware.

Employee departures shall be reported immediately to the County's liaison for your agency.

_____ _____

Signature Date

Please indicate if signing as an individual (X) or officially for your agency (X):

_____ Individual _____ Agency

ATTACHMENT E: HIPAA TRAINING ELEMENTS

PRIVACY

1) What is privacy?
2) Why does privacy matter?
    a. Legal
    b. Ethical
    c. Employee Sanctions
3) Definition of PHI
4) Disclosure of PHI
    a. Treatment, Payment Health Care Operations
    b. Permitted or required by law
    c. Authorization
5) Minimum Necessary
6) Individuals (Clients) Rights
    a. Right to inspect and copy
    b. Right to request amendments
    c. Right to know what disclosures have been made
    d. Right to request restrictions on us and disclosure
    e. Right to request confidential communications
    f. Right to know our privacy practices
7) De-identified data and limited data sets
8) Transaction and Code Sets
9) Business Associates

SECURITY

10) What is information security; what is ePHI?
11) Why does security matter?
12) Passwords
13) Email
14) Faxing
15) Mobile Working
    a. Password protect all devices
    b. Physically secure all devices
    c. No PHI stored on lap tops, handheld/tablet devices
    d. No transmission of E-phi via wireless unless encrypted

16) Secure Storage (Clear Desk)
    a. Paper documents
    b. No PHI stored on PC
    c. Secure workstation when leave

17) Secure Disposal

18) System Integrity - e.g. County approved hardware and software

19) Virus Control

20) Entry Control

21) Internet Usage

22) Log in monitoring

23) Immediate reporting of security incidents

RESOLUTION #2013-04-107	APPROVED: APRIL 9, 2013

S:\WP\Policies\HR Manual\HIPAA - Administrative Procedure 2.doc