LIVINGSTON COUNTY
ADMINISTRATIVE PROCEDURE
HIPAA-3

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 DIRECTLY TO INFORMATION TECHNOLOGY PERSONNEL.**

DEPARTMENT RESPONSIBLE: **INFORMATION TECHNOLOGY**

DATE: **APRIL 9, 2013**

DEPARTMENTS AFFECTED: **INFORMATION TECHNOLOGY**

LEGAL CITATION: **RESOLUTION 2013-04-107 LIVINGSTON COUNTY HIPAA SECURITY**

REFERENCE: **POLICIES AND DIRECTING THE APPOINTMENT OF SECURITY OFFICER**

TABLE OF CONTENTS

A. DEFINITIONS

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.

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 departments) 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, handheld/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 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.

IT (Information Technology) Facilities: Livingston County occupied buildings which contain servers located in a secured data room.

Jump Drive: 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, typically within one physical facility, 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.

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 devices, jump or thumb drives, pagers, and cell phones.

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

Simple Network Management Protocol (SNMP): A language used to communicate between PC's and other network devices which allows them to be configured from a central location over a wide area network.

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.

Supports Scrutiny: This term applies to information system applications which contain functionality to track user activities, including view, add, change, and delete transactions. Before and after images, time, date, and user involved all must be tracked in order for an application to "support scrutiny."

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.

VLAN: Virtual Local Area Network.

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.

B. POLICIES AND PROCEDURES

1. DATA CLASSIFICATION, STORAGE, BACKUP AND RECOVERY

a. 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.

b. 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.

c. Source records that are critical or mission critical records must also be the objects of a disaster recovery plan.

d. Source records that are mission critical records will be scheduled for restoration before critical records.

2. NETWORK COMMUNICATION ENCRYPTION

To transmit ePHI data securely an application that is able to communicate using encrypted FTP (File Transfer Protocol) 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

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

3. PASSWORDS

a. Generally:

- 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. 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.
- Current applications containing ePHI with no password support must be isolated in network areas off limits to employees with no job related need to access the data contained there.
- 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 OPHI 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. IT Department Staff procedures

- All production system-level passwords must be part of an IT Department administered password management database e.g. Active Directory (AD) when available and applicable.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., the SNMP product, version 2).
- Customer accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- IT Department shared administrative passwords will be changed immediately when a team member leaves.

- When design considerations require a password to be included in a batch computing process, that password shall be a strong password whenever the application involved can support one. Such passwords are exempt from the expiration requirements which would otherwise apply.
- Passwords shall not be embedded in automated scripts solely for logging in to on-line processes.

c. Application Development Standards: Application developers must ensure their programs contain the following security precautions. Applications:

- Shall use the Active Directory if available and applicable.
- Shall support authentication of individual users, not groups.
- Shall not store passwords in clear text or in any easily reversible form.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Shall support TACACS+, RADIUS and/or X.509 with LDAP, lightweight directory access protocol, security retrieval, wherever possible.
- Shall support the requirements in this procedure if developed subsequent to the effective date of this procedure.

4. EMPLOYMENT TERMINATION

No less often than quarterly, the IT Department shall also verify the continued need to access the WAN of all active log in ID's in active directory via a cross check of active employees in HR/Payroll and a contact with the Officials of all others with active log on ID's. Those users with accounts still active in HR/Payroll shall be construed as still requiring their access to the WAN while those in HR/Payroll but inactive will have their access to the WAN removed unless they are on an exception list, based on 4.b. in the HIPAA-2 procedure, maintained in the account administration team.

5. PORTABLE DEVICES

a. Only Livingston County IT Department approved portable computing devices 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. 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 or utilize other security mechanisms to protect the data which is approved by the Security Officer. 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. As of this publication date, WPA and WPA2 are approved encryption techniques. WEP should not be used. If transmission of ePHI is

necessary via wireless, contact the County's Help Desk for approved wireless transmission protocols and approved encryption techniques.

6. SECURITY SANCTIONS

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. Also, see the all-employees procedure for this item.

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. Also see the all-employees procedure for this item.

b. PCs or laptops used by the external business partners must not have connections to any other network unless through the central County firewall or through a local firewall, router or VPN device managed by WAN Staff of the IT Department. This hardware, and the software loaded thereon, is subject to approval by the Security Officer.

c. When a request is approved, sponsoring departments are to fund any required devices to support appropriate isolation of external partner's IP data traffic using recommended network segmentation techniques. County IT Department WAN Staff are to design and recommend solutions that will provide the ability to appropriately segment the traffic. This may include physically segmenting traffic, using switched VLANs, and/or configuring router access lists.

   All devices, switches, routers, and all other non-desktop hardware required to support the connectivity of external business partners and the traffic segmentation thereof, must be provided by County IT Department WAN Staff. County IT Department WAN Staff will also be solely responsible for management of these devices.

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

8. BUSINESS ASSOCIATE AGREEMENTS

Covered components desirous of sharing ePHI with external entities who are not themselves covered entities must contact their designated Contract Officers for guidance in the preparation and execution of the required business associate agreements. (see the form attached to the all employee procedure.) 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. All applications containing ePHI which support such scrutiny are eligible to be selected for random security auditing. Priority for selection shall be given to the most mission critical systems in each of the major Departments in the HCE (Health, Human Services, and Justice). These audits shall be analyzed for any unauthorized activity and appropriate action taken, coordinated by the Security Officer. These audits shall occur no less frequently than yearly for each source system which supports such scrutiny and

which has been identified as priority one in the Data Classification Categories identification process.

b. No less frequently than once in three years, the Security Officer shall arrange for a County-wide Information Security risk assessment to be conducted. The report resulting from this assessment shall include a detailed description of the information security risks currently facing the organization as well as specific recommendations for mitigating those risks. The assessment shall include any necessary updates to the County's Information processing emergency procedures, backup and recovery, and disaster plans. As part of the risk assessment, the County's HIPAA training programs will be reviewed for completeness and continuing relevance and modified as required. Substantive and substantial changes shall require employees who work with ePHI to be trained on the new curricula. This risk assessment shall include a re-evaluation of ePHI applications to determine if they are appropriately classified.

c. Systems designers and developers must include the Security Officer in project planning. All problems or issues associated with information systems being designed, modified, or developed with the potential to impact information security shall be discussed with the Security Officer.

10. EMAIL ENCRYPTION

See the all-employees HIPAA Security Procedure, HIPAA-2 for this item.

11. INFORMATION SECURITY INCIDENT RESPONSE

a. First Actions When Unauthorized Access Problems Occur:

- Whenever IT Department workforce members suspect or learn that unauthorized system access has occurred, they must immediately report such events directly to the Security Officer and then to their Privacy Officer.
- At the Security Officer's direction, IT Department staff must take immediate action to terminate the access in accordance with operational guidelines to be established pursuant to this procedure by the Security Officer. That Officer will establish an Information Security Incident Response Team based on an incident commander model and including representation from the various major sections under his or her direction. The guidelines shall include an escalating reaction to events based on the apparent threat level of those information security incidents.
- The Security Officer must report all such incidents as quickly as possible in person or by phone to the Chief Information Officer (CIO), if not the same individual.
- The CIO shall immediately report such incidents which 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, to the County Attorney, the County Administrator and to the County Board Chair.
- 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 consistent with the Security Sanctions Policy.

b. Logging Incidents: All Information Security Incidents shall be logged in the issues and incidents log kept by the IT Security Officer, along with their resolution.

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. External Reporting of Information Security Violations or Incidents: If required by law or state or federal regulation, County shall promptly report information security violations to the appropriate external authorities. If no such requirements exist, the County Administrator, the County Attorney, the Security Officer, the Chief Information Officer, the County's Privacy Officer, the HIPAA Privacy and Security Officials of the affected Departments, and the County Chair, shall determine when, and whether, to make external disclosure of these violations. Similarly, if required by law, state, or federal regulations, such violations shall also be reported to those individuals whose information has been compromised or potentially compromised.

   All external communications to the general public or the media shall be directed by, and be at the option of the County's Administrator's office.

e. 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 Official or Privacy Official to the Security Officer and the County Privacy Officer.

f. Required Investigation Following All Information Security Incidents: Whenever evidence clearly shows the County has experienced an information security incident, the Security Officer must perform a thorough, post-incident, investigation and review. This investigation must provide sufficient information to improve processes so similar incidents are not likely to recur. The investigation outcome must be documented as required by the information security documentation policy and procedure.

12. POLICIES AND PROCEDURES; DOCUMENTATION AND REVIEW

The Security Officer will maintain at least five types of documentation in order to implement this procedure as follows:

a. An accounting of the forty-eight required and addressable directives contained in the HIPAA Security Rule along with the County's response.

b. Documentation of the County's response to the HIPAA Security Rule from the County's Implementation Project's inception to the Security Rule's effective date.

c. A chronological documentation of information security issues and incidents which arise and their resolution. Items in the log will be identified as involving ePHI or not involving ePHI. Any formal opinions or advice issued by the Security Officer will also be documented.

d. Any formal reports prepared subsequent to needs assessments, compliance reviews, or security audits.

e. A compilation of any reports on the Livingston County Information Security Program prepared for the CIO by the Security Officer. These reports will be circulated as directed by the CIO.

13. WORKSTATION AND DISPOSAL OF INFORMATION

a. Patching and prevention of malicious activity:

- Anti-virus software will be installed on all applicable devices.
- All anti-virus software will be updated on a weekly basis whenever an update is available, or in the case of laptops the next time they are connected to the County's network.
- IT Department technical staff will be responsible for managing the central deployment and verification of successful anti-virus updates to all devices.
- IT Department technical staff will deploy all applicable security patches (security-motivated, vendor-issued software modifications) for the operating system, office applications suite and individualized applications after testing on a representative sample of the County's PCs, laptops and servers.
- Deployment of the patches will be applied based on the severity of the vulnerability corrected.

b. IT Department Staff responsibilities:

- Only workforce members who are County IT Department staff or specifically authorized by the Security Officer (or his or her designee) are authorized to install software on County owned PCs, laptops and handheld/tablet devices.
- IT Department staff will configure the PCs to enable the greatest level of security while enabling the customer to fully perform all necessary job requirements.
- IT Department Staff will disable any unnecessary services or applications on PCs and laptops.
- 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.
- Any IT administrative functions on a PC or laptop will be password protected.

c. Disposal guidelines:

- Any Livingston County computer or computer equipment, including storage devices, that is being surplused or otherwise passed outside the County, must undergo a hard drive reformatting process that includes multiple passes of writing all zeroes or other arbitrary characters to the hard drive or the hard drive must be removed from the computer and destroyed, prior to sending that computer to surplus.
- 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 following the method set forth in 13.c., 3Id bullet.
- Any hard drive which is found to be defective shall be destroyed unless reformatted as described in this procedure at 13.c., 3rd bullet, above. If the drive is damaged

beyond being able to be formatted, it shall be physically destroyed before being discarded. Exception: if on warranty, it may be sent to a vendor with whom we have a data destruction agreement for credit.

- Any of the requirements of this subsection 1 3.c. 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 as set forth in State of Michigan Administrative Rule. 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:

- 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.
- Lost or stolen access cards and/or keys for all IT facilities must be reported to the person responsible for the Information Technology facility immediately.

c. IT Controls

- Means of physical access to all Information Technology facilities which are restricted shall be controlled, logged, managed and protected in proportion to the criticality or importance of their function at Livingston County. All maintenance operations in primary IT facilities will be logged and monitored.
- Public entrances to all IT facilities shall be locked when no personnel are available to staff the reception area. A sign must be posted directing the visitor to another Livingston County receptionist for assistance and an estimated time of return. All exterior entry points to primary IT facilities will be monitored by receptionists or remotely by employees who have line of sight or electronic image view of the entry point. Best practice is to have a two way intercom to the entry point from the control point.

d. Access Authorization:

- System access will not be granted to any user without approval from the data system owner designated pursuant to the County Information Security Policy; a record of all authorizations will be kept.
- The process for granting card and/or key access to any IT facility shall include the approval of the person responsible for that facility.
- No individual shall be granted continuing access rights to an IT facility where ePHI is stored or accessible until they receive HIPAA training and sign any appropriate

access and non-disclosure agreements even if not employed in the hybrid covered entity.

15. HIPAA PRIVACY AND SECURITY AWARENESS AND TRAINING

See the all-employees HIPAA Security Procedure, HIPAA-2 for this item.

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

S:\WP\Policies\HR Manual\HIPAA - Administrative Procedure 3.doc