INFORMATION TECHNOLOGY, GENERAL OPERATIONS AND SECURITY POLICY

This policy establishes that the Erie County Board of Developmental Disabilities shall have consistent standards for network access and authentication to assure safe and HIPAA compliant operation. To ensure that Protected Health Information (PHI) and Confidential Information, as defined below, in all its forms: written, spoken, recorded electronically or printed; will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate and reasonable level of security over the Board's facilities, media, equipment and software used to process, store, and transmit that information.

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the Board's network are authenticated in an appropriate manner, in compliance with Board standards, and are given the least amount of access required to perform their job function. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the Board's network. Public accesses to the Board's externally-reachable systems, such as its website or public web applications, are specifically excluded from this policy.

The Superintendent shall establish, revise and keep current the procedures to be utilized in the implementation of this policy. The Superintendent/ designee shall ensure compliance with these procedures. All revisions and changes will be shared with the Board when made.

Superintendent Signature: Carrie Beier Date: 8/17/17

Implemented: 7/21/2011

Board Approval: 7/21/2011, 9/17/2015, 8/17/17

Revised: 8/2015, 5/8/17

Reviewed: 8/2015, 5/8/2017

CROSS REFERENCE:
Ohio Revised Code 149.43, 5123.61, 5123.89
45 CFR Part 160 and 164 generally
45 CFR 164.504(g) for entities with multiple functions
ORC § 5126.044 Ohio law on confidentiality
OAC § 5123:2-1-02(I)(7) General DD Board confidentiality requirements
OAC § 5123:2-4-01(C)(2)(b) General requirements for DD Board confidentiality policies
OAC § 5123:2-12-02(J)(2) Supported Living requirements for confidentiality policies and standards
OAC § 5123:2-15-01 (C)(6) Habilitation Center/TCM requirements for confidentiality policies and standards
45 CFR 164.302 Applicability
45 CFR 164.304 Definitions

45 CFR 164.306 Security Standards: General Rules
45 CFR 164.308 Administrative Safeguards
45 CFR 164.310 Physical Safeguards
45 CFR 164.312 Technical Safeguards
45 CFR 164.314 Organizational Requirements
45 CFR 164.316 Policies and Procedures and Documentation Requirements
45 CFR 164. 318 Compliance Dates for the Initial Implementation of the Security Standards
45 CFR 164. 402-.410 Breach/Notice of Breach to Individuals
45 CFR 164.502(b)(1) minimum necessary standard
45 CFR 164.502(a)(1)(iii) incidental uses and disclosures
45 CFR 164.514 (a-e), 45 CFR 164.502 (d)
NIST SP 800-14
NIST SP 800-18
NIST SP 800-30
NIST SP 800-53
NIST SP 800-66
NIST SP 800-88

POLICY: Confidentiality of Protected Health Information Held by the Board, Administrative Resolution of Complaints for Individuals, Document Management, Emergency Operation Procedures, Retention and Destruction of Administrative Records Policy.

PROCEDURES: Information Technology, General Operations and Security Procedures

ERIE COUNTY BOARD OF DEVELOPMENTAL DISABILITES
INFORMATION TECHNOLOGY, GENERAL OPERATIONS AND SECURITY PROCEDURE

I. DEFINITIONS

A. Business Associate (BA): A person or entity which creates, uses, receives or discloses PHI held by a covered entity to perform functions or activities on behalf of the covered entity. (45 CFR 160.103)

B. Confidential Information: shall mean private or otherwise sensitive information (not classified as protected health information (PHI)) that must be restricted to those with a legitimate business need. Examples of Confidential Information includes: personnel information, system access passwords, file encryption keys, etc.

C. Covered Entity: A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form.

D. Encryption: Is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. (Microsoft.com)

E. Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

F. HIPAA: The Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 – 1320d-8.

G. Information Security Officer: An employee who serves as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of individuals, providers, employees, and business information in compliance with organization policies and standards.

H. Media Access Control Address (MAC Address): Is a unique identifier assigned to a network interface for communications on the physical network.

I. Media Access Control Filtering (MAC Filtering): Refers to a security access control method whereby the MAC Address assigned to each network interface is used to determine access to the network.

J. Personal Mobile Devices (PMD): Shall mean any devices not owned by the Board, and able to store, communicate, record or transport electronic Protected Health Information (ePHI) or Confidential Data. PMD may include laptops, cell phones, smartphones, tablets, any data video and voice recording devices, external drives including USB Flash drives and memory cards etc.

K. Protected Health Information (PHI): Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is:

1. Created or received by a health care provider, health plan, employer, or health care clearinghouse;
2. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual;
3. Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (a)(4)(B)(iv); and (iii) Employment records held by the Board in its role as employer.

L. Redundant Array of Independent Disks (RAID): is a technology that provides increased storage functions and reliability through redundancy. This is achieved by combining multiple disk drive components into a logical unit, where data is distributed across multiple drives.

M. Security Officer: An individual appointed by the Superintendent responsible for

assuring the Board's compliance with HIPAA Security Standards. These responsibilities will include risk management plan implantation, monitoring, policies interpretation, review and medications as needed.

N. Security Rule: Is the final rule adopting standards for the security of electronic protected health information as required by the Administrative Simplification title of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR Part 160 and Part 164, Subparts A and C as amended.

O. Service Set Identifier (SSID): Is a name that identifies a particular wireless network or wireless access point (WAP).

P. Virtual Private Network (VPN): A network that is constructed by using the internet to connect a device to the Board's in house network. The system uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Q. Wired Equivalent Privacy (WEP): is a security algorithm for wireless networks.

R. Wired Network: A computer network that is constructed using wired cables to communicate from one device to another.

S. Wireless Network: A computer network that is constructed using radio frequencies (or wireless) distribution method to communicate from one device to another through access points.

T. Workforce: shall mean every worker at the Board without regard to their status. This includes Board Employees, contracted employees, business associates, consultants, temporaries, volunteers, interns, etc.

II. SECURITY MANAGEMENT PROCESS

All administrative safeguards requirements apply to a business associates in the same way they apply to covered entities.

A. Assign Security Responsibility

The Board will identify and assign security responsibilities to designated individual(s) responsible for Security Safeguards and rule compliance. The individual's position description should be updated to reflect assigned duties. Specific responsibilities of the Security Officer shall include:

1. Ensuring security policies, procedures, and standards are in place and adhered to by the Board;
2. Providing basic security support for all systems and users;
3. Providing on-going employee security education;
4. Performing periodic contingency plans, data classification and systems' audits/log review;
5. Managing system(s) users and overseeing information use;
6. Reviewing, approving, revoking and tracking requests for use of Personal Mobile Devices (PMD), Monitoring PMD use;
7. Reporting regularly to the Superintendent/Board on the Board's status regarding HIPAA Security Compliance.

B. Risk Analysis

The Information Security Officer/Systems Manager, at minimum, annually create a Risk Management Report and submit it to the Superintendent. These reports shall be maintained in an easily accessible shared folder titled "Risk Management". The Assessment Report shall contain the following:

1. Vulnerability Scan;
2. Business Associates and Contractor reviews;

3. User Lists reviews of Active Directory and all applications;
4. Device configuration benchmarks against current practices;
5. Training documentation.

C. Risk Management

The Security Officer will be responsible for implementation of the Risk Management Plan. The Board's Risk Management activities will include the following elements:

1. Development of the Risk Management Plan and Strategies based on the comprehensive Risk Analysis, the plan development can be completed in-house or it can be outsourced. The Risk Management Plan will include risks and mitigation strategies prioritization, and implementation plan for selected security measures;
2. The most recent risk assessment shall be used to develop or modify the risk management plan;
3. The plan shall include implementation specifics and timelines for selected risk mitigation strategies (security measures) identified in risk assessment final report, and shall describe processes for regular organizational review of activity on its information systems containing ePHI.

D. Sanctions/Disciplinary Actions

1. Employee violations of the Board's HIPAA policies and procedures will be documented and reviewed. Appropriate actions will be taken against employees who do not comply with the Board's security policies and procedures. These actions range from verbal warning to contract/employment termination. Possible disciplinary action must be instituted for, but are not limited to the following policy violations:
   a) Unauthorized disclosure of PHI or Confidential Information including information sharing through social media, email, photo sites, phone etc;
   b) Unauthorized PHI or Confidential Information access (snooping);
   c) Unauthorized disclosure of a User ID or password, attempting to obtain or using User ID or password that belongs to another person;
   d) Unauthorized use of an authorized password to invade client privacy by examining records or information for which there has been no request for review;
   e) Installing or using software on computers without the Systems Manager or Security Officer's permission;
2. The intentional, unauthorized destruction of information. Upon Discovery of the policy violation the Security Officer will notify the Superintendent and will investigate and verify the violation. The Security Officer shall use the Security Incident Response Report (Attachment A) to document the incident, findings and evidence.
3. Upon determination/confirmation of the policy violation the Security Officer shall complete the Sanction Severity Determination Form (Attachment B) categorizing the violation, documenting factors increasing or decreasing sanctions severity and suggesting appropriate sanctions.
4. Final determination of the appropriate sanctions will be made with Board leadership.

E. Information System Activity Review

System capabilities for maintaining audit trails of system use will be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews will be conducted to identify inappropriate activity so that appropriate corrective action is possible.

1. System Activity Logs: Activity Logs will be enabled at the following levels:
   a) Operating System software or Window OS: audit policy will be set to log logon events, account management events, policy changes, and system events.
   b) Firewall Hardware and Software: Logs will be enabled to track inbound and outbound activity, including internet access by an individual.
   c) Application Software Logging: All software which stores data on individuals served shall have audit trail capabilities. Logs will be enabled in application software such as clinical records software, billing software, or individual information systems.
2. Security on Logs: Appropriate security features and passwords will be used at all levels above to permit log file access only by the Information Security Officer and/or Systems Manager.

   Audit of PHI Access: There are system administration tools in place for on-going monitoring and auditing of system accesses by the Information Security Officer and IT staff. In the event, there is a suspicion of inappropriate activity the department director or designee may request a more in-depth audit of employee activity. These audit activities may include but are not limited to:
   a) Access by individuals at unusual hours;
   b) Higher access/usage levels than normal;
   c) Access to records of relatives of celebrities or employees;
   d) Unauthorized changes to security settings;
   e) Web sites viewed by employees to verify that they are work related;
   f) Outside probe attempts and/or accesses via the internet connection;
   g) Other unusual patterns of activity.
3. System Activity Review: In a manner determined by the Information Security Officer/Systems Manager will monitor system activity to detect suspicious or unusual system activity.
4. Corrective Action: The Information Security Officer/Systems Manager will initiate corrective action, in conjunction with HR policies, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
5. Purge of Log Files: System Log files which grow large may be purged under the direction of the Information Security Officer/Systems Manager.
6. Annual Policy Review: Annual attention will be given to this procedure regarding audit controls, as the threat level varies and the cost of monitoring tools changes.
7. Preventative Measures: The Information Security Officer/Systems Manager shall, on an ongoing basis, evaluate the activities that are critical to Board operations and implement preventative measures to reduce the

likelihood of system failure. These would include technical measures such as RAID arrays, backup power supplies, fire suppression systems, security systems, and database transaction logging.

III. WORKFORCE SECURITY AND INFORMATION ACCESS MANAGEMENT

The purpose of this section is to ensure that all members of the Board's workforce have the appropriate access to ePHI, access is authorized, supervised, modified and properly terminated as needed.

A. Personal Mobile Devices

The Board's Workforce will NOT use unauthorized Personal Mobile Devices (laptops, smartphones, external drives, etc.) to store, access, send or process ePHI or Confidential Data under any circumstances. Specifically, the use of Personal Mobile Devices to photograph, video or voice record ePHI and Confidential Data is prohibited.

The use of Personal Mobile Devices with Board systems and data may be permitted by Security Official under specific circumstances described below.

1. A workforce individual can request permission for the use of a Personal Mobile Device for work purposes. The individual must complete the Bring Your Own Device Release Form (Attachment C) and submit it to the Security Officer for review. This agreement will govern the use of such devices when the request is approved. The agreement will address specific administrative and technical requirements, end user obligations and employer rights.
2. The agreement must be signed/approved before devices can be connected to or access Board Systems.
3. Security Officer will review the request and inspect the device (as needed) within 2 weeks.
4. Security Officer will keep track of the Personal Mobile Devices permitted to access the Board's systems and can revoke such permissions at any time.
5. In case Personal Mobile Devices are permitted to be used with the Board's systems and data, all Information Technology General Operations and Security Policies and Procedures will apply to these devices.

B. Email, text, web, social media and oral communications and use Workforce shall always be aware of their surroundings when discussing PHI and Confidential Information or communicating through email, text or social media to avoid shoulder browsing.

1. Oral/Phone Communications

   Workforce shall not discuss PHI or Confidential Information in public areas of the information can be overheard. This includes the use of cellular telephones in public areas. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.
2. Email

   Email is often used for spam and phishing, which aids hackers in obtaining your passwords, for example to banking sites or allows them to download malware/spyware to your computer, to steal information (e.g.

passwords) or gain control of your computer and use it for illegal purposes or deny access to your computer.

a) All emails that contain PHI or confidential information should only be sent to those recipients with whom the Board has a Business Associates Agreement or a Consent to Release form with.

b) All email communications containing ePHI or confidential information must be encrypted using the Board's current email encryption service. Emails that do not contain ePHI do not have to be encrypted.

c) PHI or confidential information shall not be typed into the subject line, as the subject line cannot be encrypted.

d) All e-mails that contain PHI shall be sent with the following Confidentiality Notice at the bottom of the e-mail.

e) Confidentiality Notice: All or part of this electronic mail transmission may contain private health information (PHI). You are obligated to maintain it in a safe, secure and confidential manner. Any re-disclosure without the individual's consent may subject you to federal and/or state penalties. If you are not the intended recipient, you are hereby notified that any retention or dissemination of this information is strictly prohibited. If you have received this e-mail in error, please call 419-626-0208 immediately and delete the e-mail from your system.

f) Senders shall pay special attention when completing the address lines of an email, and making sure they are addressed to the intended recipients.

3. Text (SMS) Messages

Board allows the use of Text Messaging to families/individuals, and co-workers, but at no time shall ePHI be transmitted via a text message. Although we cannot help what is sent to us, you should respond using email, oral or other secured method.

4. Web

While using web interfaces to submit ePHI, or other confidential information make sure the connection is secure.

a) When login is necessary make sure you verify the web address before entering user and password data. The secure connection is indicated by "https" and a padlock in web browser address bar.

b) Make sure you are using approve and updated web browser.

5. Social Media

Workforce shall pay special attention to privacy and personally identifiable information when using social media. Sharing individual's photos without their written permission is violation of the HIPAA Privacy Rule.

C. Access Authorization and Account Setup

1. Account Setup

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

a) Positive ID and coordination with Human Resources is required.

b) Users will be granted least amount of network access required to perform his or her job function.

c) Users will be granted access only if he or she accepts the

Acceptable Use Policy.

d) Access to the network will be granted in accordance with the Acceptable Use Policy.

2. Account Use

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

a) Accounts must be created using a standard format (i.e., firstinitiallastname; "jdoe").

b) Accounts must be password protected (refer to the Password section for more detailed information).

c) Accounts must be for individuals only. Group accounts are to be used sparingly in a case by case bias as a last resort.

d) User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

e) Occasionally guests will have a legitimate business need for access to the Board's 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.

f) Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Systems Manager or Management Team, or as required by applicable regulations or third-party agreements.

g) Vendors/Contractors, who need access into our network to perform maintenance or other work, will be granted access to just those areas that pertains to their function. Once their contract has ended their accounts will be disabled. When possible the Board will ask that the company notify the Systems Manager when they have employees leave their company, in order that passwords are changed.

3. Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee leaves the agency, that employee's account can be disabled. Human Resources will notify the Systems Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.) through the various HR check lists. Access termination timeline shall be no less than one day of termination. There are cases when the supervisors still need to have access to the email for brief period of time. At the very least their password should be changed within one day of termination and access to all internal databases shall be revoked. Once the supervisor no longer needs access to their email, their email mailbox shall be deactivated and their account deleted from the active directory.

IV. SECURITY AWARENESS AND TRAINING

The purpose of this section is to maintain, document and improve workforce use of security related best practices to safeguard the Board's information and information systems.

A. The Board's workforce will be provided with quarterly reminders/updates highlighting information security best practices including protection from malicious software, log-in and password management. The Board shall provide and requires completion of an annual HIPAA Privacy and Security refresher training. The completion of the training shall be documented with H.R. in the annual training and certificate database.

B. The quarterly reminders shall include examples of common privacy and security pitfalls leading to data breaches, federal investigations and or penalties.

V. PHYSICAL SAFEGUARDS

A. Facility Access Controls

The purpose of this section is to limit physical access to the Board's electronic information systems and the facility in which they are housed, while ensuring that properly authorized access is allowed.

1. To safeguard server and network equipment from unauthorized physical access, tampering, and theft all server rooms and network closets will be locked with limited employee access.
2. All employees will be aware of facility security and access policies to ensure that only authorized personnel have physical access to the facility and its equipment.
3. Physical Security Planning: The Information Security Officer will periodically evaluate the physical security vulnerabilities, identify corrective measures, and develop a written facility security plan. The plan will focus on security of:
   a) Computer Servers;
   b) Telephone and Networking equipment;
   c) IT staff offices;
   d) Workstation locations.
4. Attention will be given to areas with public access; whether workstations are protected from public access or viewing; the security of entrances and exits; and the use of normal physical protections to secure records and server rooms.
5. The server room shall be equipped with its own separate air conditioning unit, and fire suppressant system.
   a) The server room shall be monitored for high temperature warning. To ensure the equipment is kept at a constant temperature of 68°F.
   b) The server room shall be equipped with a separate fire suppression system from the rest of the building. This suppression system will be safe for computer equipment. A hand-held extinguisher containing the same suppression chemical shall be placed outside of the server room.
6. Everyone shall pay attention to locking cabinets/file rooms with ePHI or Confidential Information, locking office doors and windows after hours.
7. Workforce shall maintain a clean desk policy and not to store sensitive

files in the open; shall tidy up their desk at the end of the working day. All un-needed paper that contains PHI shall be placed into the secure shredding bins at the end of the day.

8. All non-monitored entrance doors to the facility shall always be locked so they are only opened from the inside or with a proper door access badge. Unless a special activity in the facility requires the doors to be unlocked.
9. All visitors and non-workforce individuals shall sign-in at the front desk and receive a visitor's badge, or contractor's ID badge. All visitors shall be accompanied, as appropriate and necessary, by staff when entering the facility beyond waiting area.

B. Access Control and Validation

Access to the Board's facilities and systems will be controlled so only authorized individuals will be granted access. Workforce members will have access to facility based on their roles and functions.

1. Only Security Officer/Systems Manager can grant access to the Board's systems or to software programs for testing and revision. Workforce needs to check with Security Officer/Systems Manager for explicit permission before allowing individual's access to their PCs or software.
2. Workforce access to facility areas containing protected or confidential information or sensitive/critical equipment (e.g. server room, records room, HR office) is restricted to respective staff members. Access restriction shall be enforced by locking doors.
3. All repairs and modifications to the physical components of the Board's facility which are related to security (e.g. hardware, walls, doors, and locks) will be documented through contracts with vendors. These documents will be housed in the Board's electronic file system.
   a) Repairs and modifications documentation related to information systems will be reviewed and retained by the Security Officer
   b) Contractor's access will be documented through sign-in sheet when individuals enter the facility.

VI. WORKSTATION SECURITY

The purpose of this section is to safeguard protected information and information infrastructure through secure configuration of the Board's information systems and devices.

A. 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.

B. 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 required to be activated after a maximum of 15 minutes of inactivity.

C. All Board terminal servers will be set to disconnect idle users after 15 minutes of inactivity. Disconnected users will automatically be logged off of the terminal server after 90 minutes of being disconnected.

D. All Board servers must be secured with a strong password and setup to automatically lock out user access after a maximum of 5 minutes of inactivity.

E. All Board issued hand held devices (i.e. smart phones) will be set to lock the

device after a maximum of 15 minutes of inactivity.

F. All Board issued mobile devices that contain PHI shall be encrypted. Current devices can now be encrypted with built in software. Starting with Windows 8 all Microsoft user devices have the ability to be encrypted with BitLocker.

G. User IDs and 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 Board's requirements on passwords in this Policy.

1. Passwords complexity shall be enabled for all applications that allow for this policy. It is recommended that when considering new applications that they meet these standards. This includes active directory and all applications that contain client information.
   a) Passwords shall not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
   b) Be at least eight (8) characters in length;
   c) Contain characters from three of the following four categories:
      i. English uppercase characters (A through Z)
      ii. English lowercase characters (a through z)
      iii. Base 10 Digits (0 through 9)
      iv. Non-alphabetic characters (for example, !, @, $, #, %).
2. Mobile hand held devices that connect to the Exchange server will have a minimum of 4 characters and will be set with a maximum of 8 attempts before the device's data is wiped.
3. Users are required to change all passwords at least every 90 days.
4. Minimum password age is 1 day.
5. The maximum number of passwords remembered is 9 (Meaning you cannot re-use the same password until 9 other different passwords have been used after it).
6. All network accounts will be locked out for 15 minutes after 3 invalid logon attempts. The account lockout counter will reset after 15 minutes.

VII. DEVICE AND MEDIA DISPOSAL AND RE-USE

Electronic storage media and devices will be cleaned of Protected Health Information and other confidential information prior to disposal and/or re-use.

A. Media Disposal will be handled by Systems Manager: Board employees are prohibited from storing PHI on the Board's removable media. In the event of a legitimate requirement to store data on a device such as a CD, the employee will be instructed to give it to the Information Security Officer for proper disposal when it is no longer needed.

B. Media Disposal and Re-use: Procedures vary based on type of storage media:
1. Tapes: Tapes will be destroyed by a service who will issue a certificate of destruction.
2. Hard Drives and Floppy Disks: Hard drives will be sanitized according to the current National Institute of Standards and Technology (NIST) "Guidelines for Media Sanitization", prior to re-use and will be stored on agency property. Hard drives will be destroyed by a service who will issue a certificate of destruction. Floppy Disks, CD-ROMS and DVDs will be destroyed in house by shredder.

3. Flash Drives: Flash Drives will be sanitized according to the current NIST Guidelines before re-use.
4. Multi-Purpose Business Machines: Hard drives will be wiped clean or destroyed before returning leased machines or selling/destroying Board owned machines.

C. Records: Records of media disposal will be maintained for at least one year.

D. Other Media: Appropriate data wiping and/or destruction procedures shall be employed with other media, such as memory sticks, or other devices which may be used at the Board in the future.

VIII. TECHNICAL SAFEGUARDS

Technical safeguards will be employed as necessary to maintain the integrity of data, and to insure the security of data during transmission.

A. Firewalls: Hardware and/or software firewalls shall be employed to protect against network intrusions. These will be configured to enforce board policies, such as blocking of internet e-mail sites, and other safeguards.

B. Virtual Private Network (VPN): Hardware and/or software will be used to create a VPN for staff and approved outside vendors/contractors to be able to securely access the network from outside of the network. The system is to be setup with different user access levels into the network.
   1. Only employees approved by their supervisor will have VPN access from home.

C. Wireless Networks: Wireless networks, when employed, will be implemented with the following security options:
   1. The beacon shall be disabled.
   2. The SSID should be changed from the default.
   3. WEP should be enabled.
   4. MAC filtering will be employed to allow access only to workstations owned by the Board and authorized to use the network.
   5. These security options will be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.

D. Secure Certificate on email server to secure the connection between the Exchange server and Outlook, Outlook Web Access, Smart Phones etc.

E. Appropriate Audit Controls in Board-Used Software: Software used by the Board will be evaluated for the appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements should be made as appropriate. Appropriate audit controls should be criteria for continued use of and/or procurement of any new operating or application software.
   1. PaperVision uses a featured called 'Enhanced Auditing' that forces a user when printing, emailing a document to state who the reason and who the recipient is. PaperVision has different reports that allows an administrator to run a report based on a users' document access. The report details the documents they looked at and any functions they might have performed, such as printing it off. Other reports include user accounts that are locked out, password resets, and other system operations reports.

2. Gatekeeper sends an email alert to the designated HIPAA Security officer to let them know of all failed login attempts by a user. Administrators of Gatekeeper have access to reports that log specific windows that have been viewed and the users that have accessed these windows during a specific time.
   a) Gatekeeper will log information for the following windows and will display specific information which includes User ID, Date of Disclosure, Window Name, Consumer's name and Consumer's DOB:
      i. People
      ii. Medical History
      iii. Prior Authorization of Services (PAS)/Prior Authorization of Waiver Services (PAWS)
      iv. Plan
      v. Enter/Review Mental Health Notes
      vi. Goals and Objectives

F. Automatic Log Off: Appropriate measures shall be taken, based on the technology available, to enable the automatic log-off provisions as determined by the risk assessment.

G. Integrity Checks: Automated integrity checks will be run on server data periodically. Any problems will be reported to the Information Security Officer for corrective action.

H. Copiers: All print jobs that are sent to a multi-function printer (copiers) shall be sent using the hold or lock job feature. This will prevent print jobs from being accidently picked up by someone else, and from accidental PHI exposure.

I. Malicious Software Protection

All Board owned computer systems will be protected by virus and malicious software protection capabilities.

1. The Information Security Officer and/or the Systems Manager will insure that all computers in the facility are protected with reputable software for protection against malicious software. This software will protect against the various categories of malicious software, including viruses, Trojans, malware, and spyware.
2. Appropriate configuration options will be established in the software to protect against malicious software contained in:
   a) Incoming e-mail and e-mail attachments
   b) Files saved to any hard disk
3. Necessary procedures will be implemented to update the virus protection software:
   a) Daily on a schedule
   b) At system boot
4. The Systems Manager will utilize Microsoft Update Services Server or similar software to ensure each user's computer and all servers are updated with the latest Microsoft operating system updates.
5. An annual review of the malicious software protection procedure will be conducted to ensure that the products, services, and configuration, and policies appropriately manage risk for this rapidly evolving threat.

IX. SECURITY INCIDENT RESPONSE AND REPORTING

The purpose of this section is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Board and document security incidents and their outcomes. All workforce members are required to promptly report suspected or known security incidents to the Security Officer and their immediate supervisor. Examples of security incidents include: data/equipment theft or loss, unauthorized access or use, inadvertent email distribution, policy violation, virus, malware or spyware infection, hacking incident, inappropriate use of media/social media.

A. Data Breach is generally, an impermissible use or disclosure under the Privacy Rule (see the Breach section in the Board Policy "Confidentiality of Protected Health Information Held by the Board") that compromises the security or privacy of the protected health information, unless the Board's or business associate can demonstrate that there is a low probability that the protected health information has been compromised, or one of the exactions to the data breach definition applies. Part 164 Section §164.402- §164.410 address data breach and notification requirements.

1. Breach definition includes the following exceptions:
   a) Unintentional acquisition, access or use by employee (acting under authority);
   b) Accidental disclosure between authorized employees;
   c) When there is a good faith belief that information could not have been retained by unauthorized individual, to whom impermissible disclosure was made.
2. While the above definition of PHI data breach comes from the HIPAA Omnibus rule, the same concepts can be applied to confidential information or personally identifiable information (PII).

B. Security Incident/Data Breach Response

This procedure describes event triggers and steps to be taken in case of security incident. Security Officer will be responsible for implementation of this procedure.

1. The most serious security incidents are those resulting in data breach. Factors to consider in assessing the probability of PHI being compromised include:
   a) What type of data has been compromised, what are the data elements involved and how likely can data be re-identified;
   b) Who is the unauthorized person who used the protected health information or to whom the disclosure was made;
   c) Was the protected health information actually acquired or viewed only; and
   d) The extent to which the risk to the protected health information has been mitigated (what were the immediate mitigation steps).
2. Security Incident Risk Assessment, considering the above factors will help identify the high or low probability of data being compromised, and will determine need for data breach notification. It is necessary to retain the copy of the security incident report and risk assessment in all situations, even when level of information compromise is low and no breach notification is necessary.

a) Security Officer, Supervisor shall be notified immediately when security incident is suspected. Upon notification, the Security Officer shall:

i. Immediately investigate the issue and complete the Security Incident Response Report to evaluate the situation and document the investigation. The form contains additional guidance and information about data breaches.

ii. When incidents involve equipment (e.g. PC, laptop, and storage device) the Security Officer needs to take immediate ownership of the equipment suspected in security incident to facilitate its inspection and completion of the investigation. The equipment, including personal owned devices needs to be secured and not accessible to others to avoid possibilities of tampering with evidence. As needed a specialized data forensic services may need to be employed.

iii. Notify the Superintendent upon confirmation of incident or when suspected incident may result in a data breach.

iv. The Superintendent along with the Security Official shall determine additional steps to verify potential for data breach and need for breach notification. The investigation steps will be unique to each situation but may include: interviews with workforce, review of EHR system audit trail reports, forensic review of computers and records, inventory review, staff and patients' attendance (time cards/sign in sheets), review of janitorial/maintenance schedules etc. Isolating affected equipment for computer forensics shall also be considered especially in case of suspected data breach.

v. Data breaches by Business Associates are quite common. Proper Business Associate (BA) agreement is a key in mitigating the Board's risk exposure. In case of the data breach caused by BA, a review of BA contract, their records and establishing good communications and collaboration in the investigation process is essential.

vi. If it is clear that the security incident does not result in data breach, sanction policy and other corrective actions may still have to be applied. The workforce Sanction Procedure shall be used to determine sanction steps.

vii. If it is clear that the security incident likely resulted in data breach the Security Incident Response report should help identify actions necessary to mitigate data breach results, actions necessary to comply with HIPAA rules, and individuals to be included in addressing the incident. The Board shall consider at least including Legal Counsel and Privacy and Security expert in developing plan to address data breach.

3. Before issuing any data breach notification and following HHS Breach Notification rule described at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html the Covered Entity leadership and Security Official shall conduct thorough investigation verifying that data breach in fact occurred, and account for number of individuals affected by data breach, as reporting responsibilities differ based on number of individuals affected (500+). Ask for second opinion.

C. Contingency Plan

1. Data Backup Plan

The data backup plan must assure availability of retrievable exact copies of critical information created and maintained by the Board (including PHI). The backup plan must be documented and routinely updated; backup data must be stored off-site for a specific period of time, must be protected from physical damage, and must be afforded the same level of protection as the original data.

a) Data Criticality Analysis: Data identified as either Critical or Important, as described below, shall be backed up each evening:
   i. Critical Data:
      (a) Gatekeeper
      (b) PaperVision
      (c) TC-1
   ii. Important Data:
      (a) E-Mail
      (b) Other Administrative Data
      (c) User Directories (word processing documents, spreadsheets, other data)
   iii. Non-unique Data – Is backed up nightly
      (a) Operating system, other system software and applications software

b) Backup Software: Appropriate backup software shall be maintained, with appropriate scripting.

c) Drive Storage/Off Site Storage: Daily backup removable media will be stored in the vault at the County Auditor's office.

d) Responsibility: The Security Officer will designate the employee with primary responsibility to personally handle the backup. In the event that he/she is absent from work, an alternate individual will be responsible. All individuals responsible for this critical function will be trained and familiar with how to review the log file in the backup software to verify the proper operation of the backup.

e) Removable Backup Media Security: Removable Backup Media will be kept in a secure area with access limited to those individuals named in this procedure.

f) Removable Backup Media Replacement: Removable Backup Media will be replaced at the frequency recommended by the manufacturer. Old media will be disposed as specified by Board policy.

g) Testing and Plan Revision: Review and update of the data backup plan will be conducted with any significant update of the

technical environment. On at least a quarterly basis, a trial restore will be performed from a backup tape to verify the proper function of the backup process. Based on the results of this test, and any other environmental changes, the Data Backup Policy and Disaster Recovery Plan will be updated. The results of this process will be documented and maintained for one (1) year.

h) Data Recovery Plan: The Security Officer and/or Systems Manager will maintain a written plan for restoration of data in the event of various system failures.

2. Disaster Recovery Plan
In case of disaster or incident destroying PHI, please refer to the Board's Emergency Operation Procedures section IV – IT Recovery Plan.

3. Testing and Revision Procedures
The contingency plan testing will be conducted at least once a year. The Security Officer will be responsible for implementation of the testing procedure.
The testing will consist of testing the information systems as a result of loss of data. The Security Officer/Systems Manager will conduct a process/workflow review of responding to this scenario: identifying equipment, reinstalling systems/software and restoring data from encrypted offsite storage.

4. Evaluation
The Board's information systems both technical and non-technical will be periodically evaluated. These evaluations will include vulnerability testing, port scanning and penetration testing. The comprehensive evaluation of the Board's systems will be conducted annually during completion of the Risk Analysis and development of the Risk Management Plan.

X. BUSINESS ASSOCIATE CONTRACTS AND OTHER AGREEMENTS

The Board will incorporate written business associate agreements with all contractors and individuals creating, receiving, maintaining or transmitting PHI for or on behalf of Covered Entity, to safeguard protected and confidential information. Covered entity does not need to enter into business associate agreements with subcontractors of their business associate - business associates need to do so.
The following procedure will be used to determine the need and establish business associate contracts. Security Officer will be responsible for implementation of the Business Associate Contract Procedure.

A. Business associates are directly liable under the HIPAA Rules:
   1. For impermissible uses and disclosures;
   2. For a failure to provide breach notification to the Board;
   3. For a failure to provide access to a copy of electronic protected health information to either the Board, the individual, or the individual's designee (whichever is specified in the business associate agreement);
   4. For a failure to disclose protected health information where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules;
   5. For a failure to provide an accounting of disclosures;
   6. For a failure to comply with the requirements of the Security Rule;

7. For applying minimum necessary standard when disclosing PHI;
8. For assuring that their subcontractors comply with the same restrictions and condition;
9. For reporting breaches of unsecured PHI to covered entity;
10. For civil monetary penalties;
11. In general business associates are not required to designate privacy official or provide notice of privacy practices unless such responsibility is delegated to business associate as a contractual requirement (see below);
12. Business associates remain contractually liable for other requirements of the business associate agreement.

B. Security Officer will use the Business Associate Decision Chart (Attachment D) to determine vendor's business associate status. Many of the verification steps can/should be used for any contractor.

C. The Board shall verify prospective contractor or business associate status by requesting Certificate of Good Standing issued by the Ohio Secretary of State certifying good standing of the prospective partner.

D. The Board shall request a proof of professional liability insurance (not just general slip and fall insurance) and proof of worker's compensation coverage for its employees (when applicable).

E. The Board shall request clear statement from vendor describing PHI access needs and how the PHI will be handled.

F. The Board shall request written Statement of Compliance with HIPAA Privacy and Security regulations from business associate, signed by organization CEO/President. Asking that the Business Associate CEO/President personally signs the business associate agreements helps assure that the safeguards are in place.

G. In some instances (e.g. high value/impact agreements, resources available) the Board may want to review the potential business associate Risk Analysis summary report before signing contract and make sure that the PHI is adequately protected. When reviewing the vendor Risk Analysis report special attention shall be placed on:
1. How current the Risk Analysis is (no more than 12 months old), and if it was performed by HIMSS/AHIMA credentialed vendor (3rd party versus internal self-assessment);
2. How current is the vendor's associates HIPAA awareness training, is it documented;
3. Does the vendor have a Risk Management Plan in place, does it address the risks identified in the Risk Analysis;
4. How high vulnerability risks are being addressed before Business Associate agreement is signed.
5. Consider incorporating the BA monitoring process (if needed) by requesting monthly BA_DEVICE_REPORT (Attachment E) updates identifying ePHI in BA possession, where they reside and how are they protected.

H. The business associate written agreements shall incorporate the HHS guidance, yet should be customized to reflect particular Board and vendor specific relationship. The obligations and activities of the business associate, and the use of PHI by business associate, shall reflect the specific vendor need as it relates

to service to be provided. Incorporating the 'right to audit' the business associate is strongly recommended.

I. The Board shall use the BA_AGREEMENT_TEMPLATE (Attachment F) to draft respective agreements with business associates, incorporate 'chain of command' for breach notification by business associates and their subcontractors, and specify expense responsibilities.

J. When vendor drafted business associate agreement is used, the Board will thoroughly review the agreement and will follow recommendations from item (X.G.) of this procedure to limit and/or avoid 'boiler plate' language related to use of PHI not applicable to particular business relationship.

Security Incident Response Report
Attachment A

INCIDENT IDENTIFICATION INFORMATION

INCIDENT DETECTOR's INFORMATION:

NAME:		DATE/TIME DTECTED:	
TITLE:		LOCATION:	
PHONE/CONTACT:		SYSTEM/APPLICATION:	

INCIDENT SUMMARY

TYPE OF INCIDENT DETECTED:

	DATA/EQUIPMENT THEFT/LOSS		MALICIOUS CODE/VIRUS/HACKING INTRUSION
	UNAUTHORIZED ACCESS/USE		INAPPROPRIATE USE /SOCIAL MEDIA
	INADVERTENT EMAIL DISTRIBUTION		IDENTITY THEFT
	POLICY VIOLATION		OTHER:

DESCRIPTION OF INCIDENT:

LIST COMPROMISED DATA ELEMENTS POTENTIALLY RESULTING IN SIGNIFICANT HARM TO AFFECETED INDIVIDUALS:

TBD

NEED FOR BREACH NOTIFICATION

	LESS THAN 500 INDIVIDUALS AFFECTED		MORE THAN 500 INDIVIDUALS AFFECTED
	INDIVIDUAL NOTICE		INDIVIDUAL NOTICE
			MEDIA NOTICE
	HHS SECRETARY (ANNUAL)		HHS SECRETARY (60 DAYS)

INCIDENT NOTIFICATION (who needs to be involved in addressing the incident)

	OWNER		CO-OWNER/PARTNER
	OFFICE MANAGER		BUSINESS ASSOCIATE/CONSULTANT
	PRIVACY/SECURITY OFFICER		SYSTEM/APPLICATION VENDOR
	OTHER:		LEGAL COUNSEL

ACTIONS

IDENTIFICATION MEASURES(INCIDENT VERIFIED, ASSESSED, OPTIONS EVALUATED):

CONTAINMENT MEASURES:

EVIDENCE COLLECTED (SYSTEM AUDIT LOGS, AUDIT REPORTS etc.)

ERRADICATION MEASURES:

RECOVERY MEASURES/EFFORTS:

EVALUATION

HOW WELL DID THE STAFF RESPOND?

WERE THE DOCUMENTED PROCEDURES FOLLOWED? WERE THEY ADEQUATE?

WHAT INFORMATION WAS NEEDED SOONER?

WERE ANY STEPS OR ACTIONS TAKEN THAT MIGHT HAVE INHIBITED RECOVERY?

WHAT COULD THE STAFF DO DIFFERENTLY THE NEXT TIME AN INCIDENT OCCURS?

WHAT CORRECTIVE ACTIONS CAN PREVENT SIMILAR INCIDENTS IN THE FUTURE?

WHAT ADDITIONAL RESOURCES ARE NEEDED TO DETECT, ANALYZE, AND MITIGATE FUTURE INCIDENTS?

OTHER CONCLUSIONS/RECOMMENDATIONS:

FOLLOW UP

REVIEW BY:			
	PRIVACY/SECURITY OFFICER		BUSINESS ASSOCIATE/CONSULTANT
	OTHER:		SYSTEM/APPLICATION VENDOR

BREACH NOTIFICATION COMPLETED

	LESS THAN 500 INDIVIDUALS AFFECTED		MORE THAN 500 INDIVIDUALS AFFECTED
	INDIVIDUAL NOTICE		INDIVIDUAL NOTICE
			MEDIA NOTICE
	HHS SECRETARY (ANNUAL)		HHS SECRETARY (60 DAYS)

RECOMMENDED ACTIONS CARRIED OUT:

INITIAL REPORT PREPARED BY:	
DATE:	

FOLLOW UP COMPLETED BY:	
DATE:	

MEDICAL IDENTITY THEFT FOR INDIVIDUALS

IN CASE OF IDENTITY THEFT WITHIN THE PRACTICE MANAGER/SECURITY OFFICIAL SHOULD:
- ASSIST AFFECTED INDIVIDUALS IN ANSWERING QUESTIONS, PROVIDING GUIDANCE
- ADVISE INDIVIDUALs TO CONTACT ENTITIES LISTED BELOW

CREDIT REPORT ORGANIZATIONS
ATTORNEY GENERAL OFFICE - FILE COMPLAINT
POLICE - FILE REPORT
STATE INSURANCE DEPARTMENT - FILE COMPLAINT
IDENTITY THEFT DATA CLEARINGHOUSE (FTC) - FILE COMPLAINT
INTERNET CRIME COMPLAINT CENTER (FTC) - FILE COMPLAINT
HHS OIG (IF MEDICARE/MEDICAID FRAUD SUSPECTED) - FILE COMPLAINT

SANCTION SEVERITY DETERMINATION FORM
Attachment B

NAME OF INVESTIGATED INDIVIDUAL:		DATE OF COMPLETION:	
PERSON (s) COMPLETING THE REPORT			

PERSONNEL CATEGORY: *Discretion or adaptive use of this form may be necessary in circumstances of labor unions.

	CLINICAL STAFF		VOLUNTEER		BUSINESS ASSOCIATE
	PHYSICIAN SELF-EMPL		SUPPORT STAFF		CONTRACTOR
	OTHER - DESCRIBE =>				

DATE(s) OF INCIDENT(s)		DATE DISCOVERED	

METHOD OF DISCOVERY:

	MEDIA		FOUND ON AUDIT		PATIENT COMPLAINT
	INTERNAL STAFF		OTHER- DESCRIBE =>		

DESCRIPTION OF INCIDENT (ATTACH ADDITIONAL DOCUMENTATION AS NEEDED)

SANCTIONS APPLIED	

The organization takes corrective action and bases remediation on the highest level of category indicated. If a violation falls into one or more risk areas on the chart, the corrective action is based on the highest category level of risk.

CATEGORY	EXPOSURE	NUMBER OF INDIVIDUALS AFFECTED	PURPOSE	SPECIAL PROTECTION	INTENT and PHI DISCLOSURE
1	Low external exposure to the organization	Involves a single patient	Carelessness, lack of education/training or poor judgment	No additional state or federal protection	Unintentional and unauthorized, PHI disclosure occurred
2	No external exposure to the organization	Involves 1 - 5 patients	Snooping or curiosity	Employees, VIP	Deliberate and unauthorized, no PHI disclosure
3	Medium external exposure to the organization	Involves 1 - 99 patients	Snooping or curiosity	Employees, VIP	Deliberate and unauthorized, PHI disclosure occurred
4	High external exposure to the organization	Involves 100+ patients	Malice, sale or personal gain	HIV, mental health, adoption, substance abuse, genetic data	Deliberate and unauthorized, PHI disclosure occurred

SANCTION SEVERITY _ _TERMINATION FORM
Attachment B

FACTORS INCREASING SANCTION SEVERITY

Multiple offense	High exposure to organization
Harm incurred to victim(s)	Hampered investigation
High volume of victims or data	Large expense incurred (e.g. cost of breach)
Breach of specially protected information	Negative influence of actions on others

FACTORS DECREASING SANCTION SEVERITY

Occurred with good intentions (i.e., patient care, assist operations)	Showed remorse
No harm to victim(s)	Acted under direction of authority
Volunteered /reported breach	Low cost to organization
Confessed/ cooperated with investigation	Inadequate training

CHOICE OF SANCTIONS APPLIED (CAN BE CUSTOMIZED)

LESSER SANCTIONS

Verbal warning (documented)	Written warning	Probation

STRONGER SANCTIONS

Final warning w/suspension w/pay	Final warning w/suspension w/o pay	Loss of medical staff privileges	Contract severance	Employment termination

CATEGORY DETERMINATION

Category 1 Factors	Unintentional	Careless	Poor judgment	Lack of training/knowledge
Category 2 Factors	Deliberate	Unauthorized	No known Disclosure	Trained; understood policy
Category 3 Factors	Deliberate	Unauthorized	Disclosure occurred	Trained; understood policy
Category 4 Factors	Deliberate	Unauthorized	Disclosed for malice or personal gain	Understood policy

EXAMPLES

Category 1: Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
Category 2: Deliberate unauthorized access to PHI without PHI disclosure. Examples: snoopers accessing confidential information of a VIP, coworker, or neighbor without legitimate business reason; failure to follow policy without legitimate reason, such as password sharing.
Category 3: Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Examples: snooper access and disclosure to the news media; unauthorized modification of an electronic document to expedite a process.

Category 4: Deliberate unauthorized disclosure of PHI for malice or personal gain. Examples: selling information to the tabloids or stealing individually identifiable health information to open credit card accounts.

Importance of Consistency for applying Privacy and Security Sanctions

The disparity among organizational responses to employee privacy and security violations has a far-reaching impact on the healthcare industry. Consequences include the following:

Inconsistent corrective disciplinary actions. Organizations have reported terminating some staff while issuing lesser reprimands or suspensions to higher-level staff for the same type of offense. Staff may interpret this to mean that it is acceptable to breach privacy or security rules as long as an individual holds a certain status in the organization. The healthcare industry should nurture an image of solidarity in enforcing the privacy and security of protected health information (PHI) in a standardized approach across the workforce, from file clerks to medical staff members.

Poor compliance. Staff in organizations with less stringent enforcement may weigh the level of risk to themselves against the potential advantages; for example, taking home PHI in order to catch up on work over the weekend. Staff perceived as lower risk may ignore security and privacy policies designed to protect PHI. Inequity in sanction application encourages poor compliance by individuals who know they will escape serious consequences for breaching privacy and security policies.

Delayed response in applying sanctions. A delayed response to a violation might imply a lack of commitment to protecting patient privacy. Delays in applying sanctions place the organization at risk, allowing security risks and violations to go unaddressed. Sanctions must be prompt and suitable to the severity of the violation so that employees understand the organization is serious about information privacy and security enforcement.

Erosion of public trust. Public trust is eroded when significant variation is blatantly apparent in how healthcare organizations prevent and manage privacy or security violations both within and across entities and systems. The public must feel assured their PHI has sufficient protections across the healthcare spectrum, particularly in this era of HIE.

Weakened position for dispute resolutions. Inequitable application of sanctions can affect the outcome of personnel actions at arbitration and grievance proceedings. Unequal penalties for similar offenses undermine the organization's ability to prevail in dispute resolutions.

Vulnerability to civil actions and lawsuits. Healthcare organizations leave themselves open to both individual and class action lawsuits when they do not have a strong, consistent privacy and security compliance program. Under HITECH, state attorneys general are now authorized to bring civil suits against covered entities on behalf of individuals. The Office for Civil Rights (OCR) has funded training for attorneys general on how to bring these suits forward. This new provision strengthens the capabilities of the states and empowers OCR's overall enforcement.

Vulnerability to penalties and fines. OCR will continue to increase its enforcement activities, and the federal judiciary is becoming engaged in enforcing privacy and security violations and imposing ever-increasing fines. Inconsistent application of sanctions at the organizational setting may affect how OCR and the federal judiciary view such issues.

More regulation. Poor and inconsistent implementation of privacy and security safeguards invites further state and federal intervention. States are beginning to impose more stringent reporting obligations and stiffer penalties on healthcare organizations, business associates, and individuals. Such laws place an additional administrative and financial burden on organizations. If the industry does not self-correct, then it leaves open the door to state and federal government intervention. HITECH has increased the likelihood of federal intervention by requiring regular privacy and security audits as a measure of OCR's enforcement.

"BRING YOUR OWN" DEVICE RELEASE FORM

I, _____ have been identified as an employee who is required to have a cellular phone with a data package as a working condition of my employment in accordance with Board's "Proper Use of Public Funds" Policy and I am electing to use my own personal cellular phone and receive a voice and data package stipend.

I, _____ have NOT been identified as an employee who is eligible to receive a data package stipend to use my own personal cellular phone, but I am requesting to use my own mobile device to connect to the Board's Exchange Server.

I have read and understand the Board's "Information Technology" and the "Confidentiality of Protected Health Information Held by the Board" Policies. I understand that I must password protect my device as per policy being forced down to my device from the Board's network. I understand that after 8 failed logon attempts my device will be wiped, as a security precaution. My device may also be remotely wiped by me or the Network Administrator at any time if my device is lost or stolen. I also understand that since I am using my personal mobile device to conduct Board business my device may be subject to a public records request. Upon my employment termination my access to the Board's network will be revoked and I will need to show proof that the account was removed from my mobile device.

Type of Device: _____

Associated Phone Number: _____

_____ _____

Signature Date

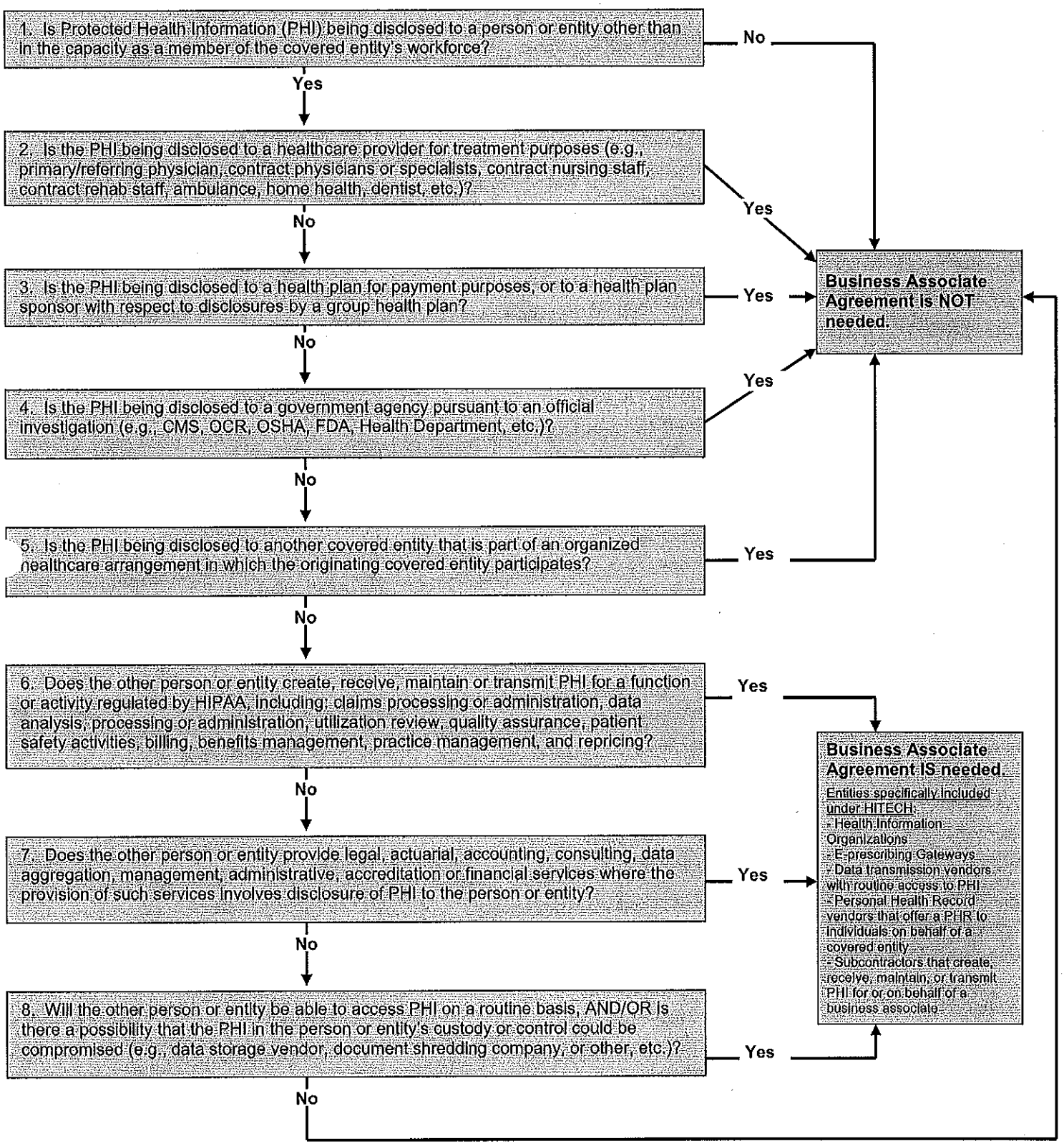
Removal Of Access

Date Removed: _____ Observed By: _____

Employee Signature: _____

Revised 9/2012

HIPAA/HITECH
Business Associate Decision Tree
Attachment D



BA_DEVICE_REPORT
Attachment E

BUSINESS ASSOCIATE NAME								
DATE	**DEVICE UNIQUE ID**	**DEVICE DECRIPTION**	**OWNER/ USER/ PERSON RESPONSIBLE (include BA subcontractors)**	**ePHI DESCRIPTION**	**PURPOSE FOR STORING ePHI on the device**	**DEVICE SAFEGUARD used to protect ePHI**	**ePHI DESTRUCTION DATE**	**ePHI DESTRUCTION METHOD**

This template can be used by Covered Entity (CE) and Business Associate (BA) to satisfy CE monitoring requirements of BA - Business Associate Contracts or Other Arrangements 164.314(a)(2)(ii). The template should be used when BA stores ePHI. CE should request that BA provides e.g. monthly updated report where the CE's ePHI is stored, who has access to ePHI and how it is protected. Applicable to e.g. IT partners implementing new EHR systems, billing solutions, system configuration changes, data base transitions or upgrades etc.
This information will be essential in case of security incident investigation (e.g. data breach) and with BA equipment inventory tracking.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (this "Agreement"), is made as of the ___ day of _____, 20_____ (the "Effective Date"), by and between ___BA_____ ("Business Associate") and ___PRACTICE NAME_____ ("Covered Entity") (collectively the "Parties").

1. Business Associate provides [NAME/TYPE OF SERVICES] services to Covered Entity pursuant to a separate contract agreement;
2. In relation to these services, Covered Entity may need to disclose to Business Associate certain Protected Health Information ("PHI") protected under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and other applicable laws. Like a covered entity, Business Associate may not use or disclose protected health information except as permitted or required by the Privacy Rule or the Enforcement Rule.
3. The purpose of this agreement is to comply with HIPAA requirements and assure that Business Associate meets HIPAA privacy and security standards with respect to PHIs received, created, maintained or transmitted in the course of providing services to or on behalf of Covered Entity.

In consideration of the mutual promises and agreements the Parties agree as follows:

I. Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

a. Business Associate. "Business Associate" shall mean [Insert Name of Business Associate].
b. Covered Entity. "Covered Entity" shall mean [Insert Name of Covered Entity].
c. Individual. "Individual" shall mean the person who is the subject of the Protected Health Information.
d. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E as amended.
e. Security Rule. "Security Rule" shall mean the final rule adopting standards for the security of electronic protected health information as required by the Administrative Simplification title of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 CFR Part 160 and Part 164, Subparts A and C as amended.
f. Protected Health Information. "Protected Health Information" shall mean individually identifiable health information that is held, transmitted or maintained in any form or media, whether electronic, paper or oral.
g. Required By Law. "Required by Law" shall mean a mandate contained in law that constrains a use or disclosure of PHI.
h. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.
i. Designated Record Set. "Designated Record Set" shall mean a group of records maintained by or for a covered entity, as defined by HIPAA, that is: (i) the medical records and billing records about Individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about Individuals. For purposes of this definition, the term "record" means any item, collection, or grouping of

information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

II. Obligations and Activities of Business Associate

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.
b. Business Associate agrees to implement and use appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of the Protected Health Information that is created, received, maintained or transmitted by Business Associated for or on behalf of Covered Entity.
c. Business Associate agrees to implement and use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
d. Business Associate agrees to mitigate, to the extent practicable, any known, harmful effect of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. [This provision may be included or further modified if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]
e. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, immediately upon the improper use or disclosure discovery.
f. Business Associate will notify Covered Entity immediately upon discovery of the suspected security incidents and will inform, and include (as needed) Covered Entity in investigation and final determination if data breach really occurred.
g. Business Associate will be responsible for costs associated with security incidents caused by Business Associates or its subcontractors. Specifically the Business Associate will cover cost of: forensic investigation, research/investigation confirming that the security incident really occurred including any legal and 3rd party consulting costs related to the security incident investigation, data analysis - cost of determining who needs to be notified if data breach is confirmed, communication (notice letters, printing, mail management, notice to AG, HHS, call centers), credit monitoring and identity protection for affected individuals for 1 year or cost of alternative harm mitigation strategies, fines and settlements, and other reasonable remediation costs of Covered Entity reputational harm (e.g. public relation costs).
h. In case of a confirmed data breach caused by Business Associate Covered Entity will be responsible for notify affected individuals, media and HHS (as needed) about data breach. Business Associate will reimburse Covered Entity for the cost of notification. [Consider size of BA and Practice when defining this point]
i. Business Associate will carry professional insurance during entire contract engagement with Covered Entity, providing Breach Notice Coverage which needs to include Forensic investigation, legal fees, data analysis, Communication (notice letters, printing, mail management, notice to AG, HHS, call centers), credit monitoring and identity protection, public relations, fines and settlements.
j. Business Associate will provide Covered Entity with following report on a monthly basis:
    a. Listing of all BA devices where Covered Entity ePHI data is stored, ePHI description and unique identifier, specific safeguards protecting ePHI, purpose of storing the ePHI on these devices and names of users/owners of these devices, ePHI destruction date and methodology used;
    b. The report must include information about ePHI stored on BA subcontractors' devices as well and must be in electronic format. Use BA_DEVICE_REPORT Excel template.

k. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from or created by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate.
Business Associate shall enter into a Business Associate agreement with its agent or subcontractor to whom PHI is provided or disclosed.

l. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. [Not necessary if business associate does not have protected health information in a designated record set.]

m. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms]. [Not necessary if business associate does not have protected health information in a designated record set.]

n. Business Associate agrees to make internal practices, books, and records, including policies and procedures related to the use and disclosure of Protected Health Information received from, created, maintained or transmitted on behalf of Covered Entity, available to the Covered Entity, and/or to the Secretary, in a time and manner [Insert negotiated terms] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rule.

o. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

p. Business Associate agrees to provide to Covered Entity or an Individual with information to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

q. Business Associate agrees to notify Covered Entity immediately about any HIPAA related audits and investigations the Business Associate is subjected to.

r. Business Associate agrees to provide Covered Entity with a summary report of a Risk Analysis before contract renewal. The Risk Analysis shall not be older than 12 months.

III. Purposes for which PHI May Be Disclosed to Business Associate

a. Purpose: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:
[List Purposes e.g. providing legal counsel, defending or prosecuting litigation on behalf of Covered Entity, assisting with regulatory requirements, accreditation, certification licensure, or operational issues, and any other legal services provided to Covered Entity.].
Red font indicates sections to be deleted, they are part of HHS template, but may not be needed and should ONLY be included in the BA agreements when specific need exists.
- Use or disclosure of PHIs for proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate – be specific about management

functions, who data will be disclosed too – if BA cannot provide specific do not include it.
- Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted – will BA be providing any data aggregation? If not do not included it.

b. Refer to underlying service agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of Services Agreement], provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity. [business associate agreement may be part of the service contract or an addendum]

IV. Obligations of Covered Entity

a. Covered Entity shall provide the Business Associate a copy of its Notice of Privacy Practices ("NPP") produced by Covered Entity in accordance with 45 C.F.R. 164.520 as well as any changes to such notice, and notify Business Associate of any NPP limitation(s) that may affect Business Associate's use or disclosure of Protected Health Information.
b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.
d. Covered Entity shall notify Business Associate of any amendment to PHI to which Covered Entity has agreed that affects a Designated Record Set maintained by Business Associate.

V. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. [Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].

VI. Term and Termination

a. Term. The Term of this Agreement shall be effective as of Effective Date and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is returned to Covered Entity. If return of PHIs is not feasible the PHI shall be destroyed by Business Associate in accordance with 45 CFR 164.310(d)(2)(i). Business Associate shall forward PHI disposal documentation to Covered Entity.

b. Termination for Cause. If Covered Entity determines that Business Associate has breached the requirements of this Agreement, by not meeting:
- [insert specific performance measures, thresholds or standards as needed]
- the security functional requirements/specifications,
- the security-related documentation requirements,
- the development and evaluation-related assurance requirements described in applicable laws,

regulations and guidance documents,
The Covered Entity may:

1. Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
2. Immediately terminate this Agreement [and the _____ Agreement/ sections ____ of the _____ Agreement] if Business Associate has breached a material term of this Agreement and cure is not possible; or
3. If termination or cure of the violation is not feasible, Covered Entity shall report the violation to the Secretary and/or to the Office of Civil Rights.

[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]

c. Effect of Termination.
   1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
   2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the reasons that make return or destruction infeasible. Upon Covered Entity written acceptance of the Business Associate reasoning that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

VII. Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
c. Survival. The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.
d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

Agreed to:

BUSINESS ASSOCIATE

By:_____
(Authorized Signature)

Name:_____
(Type or Print)

Title:_____

Date:_____

Agreed to:

COVERED ENTITY

By:_____
(Authorized Signature)

Name:_____
(Type or Print)

Title:_____

Date:_____