

HIPAA Policies and Procedures – Part II

For

Sound Inpatient Physicians, Inc.

TABLE OF CONTENTS

	Page
GENERAL SECURITY	1
DESIGNATION OF SECURITY OFFICER	3
SECURITY MANAGEMENT	4
SECURITY AWARENESS TRAINING	6
AUDITS AND EVALUATION	8
INFORMATION SYSTEMS INVENTORY	10
PHYSICAL SECURITY	11
CONTINGENCY PLAN	13
INFORMATION ACCESS MANAGEMENT	14
WORKFORCE SECURITY	16
TECHNICAL ACCESS CONTROLS	18
PASSWORDS	20
WORKSTATION USE	21
WORKSTATION SECURITY	23
INTEGRITY OF ELECTRONIC PHI	24
ANTI-VIRUS STANDARDS	25
MONITORING AND AUDIT CONTROLS	26
DEVICE AND MEDIA CONTROLS	27
ELECTRONIC COMMUNICATIONS	29
SECURITY INCIDENT MANAGEMENT	30

SOUND HIPAA POLICY AND PROCEDURE GENERAL SECURITY	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Part II of these HIPAA Policies and Procedures relate primarily to uses and controls for the security of the information systems and data of Sound Inpatient Physicians, Inc. and its subsidiaries and other affiliates (collectively, “Sound”) and specifically for the protection and security of electronic protected health information (“ePHI”) obtained and/or maintained by Sound.

I. General Policy of Compliance

- A. It is the policy of Sound to comply with all aspects of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the regulations promulgated thereunder. These regulations include the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E (the “HIPAA Privacy Rule”); the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C (the “HIPAA Security Rule”); and the standards relating to Notification in the Case of Breach of Unsecured Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and D (the “HIPAA Unsecured PHI Breach Notification Rule”).
- B. Part II of these HIPAA Policies and Procedures has been prepared to ensure Sound’s compliance with the HIPAA Security Rule. Part I of these HIPAA Policies and Procedures has been prepared to ensure Sound’s compliance with the HIPAA Privacy Rule and the HIPAA Unsecured PHI Breach Notification Rule. Nonetheless, certain policies and procedures in each Part could relate to topics primarily addressed in other Parts; therefore, the Parts shall be read and followed in conjunction with the other.
- C. As set forth in these HIPAA Policies and Procedures, Sound will promote a secure information systems environment through administrative, physical and technical safeguards to protect the privacy, integrity, and availability of ePHI while allowing its workforce (i.e., physicians, nonphysician practitioners, nurses and other clinical employees, its volunteers and other persons whose conduct, in the performance of work for Sound, is under the direct control of Sound, whether or not they are paid by Sound) (collectively, the “Sound Workforce”) reasonable access to systems and data necessary to carry out their duties for the safe and effective provision of medical care.

II. Security Responsibilities.

- A. The Sound Workforce has a general responsibility to adhere to administrative, technical, and procedural safeguards relating to security, as defined within these HIPAA Policies and Procedures.
- B. Sound Workforce members must comply with all HIPAA Policies and Procedures in the handling of ePHI.

- C. Managers and supervisors are expected to ensure all appropriate Sound Workforce members comply with these policies and procedures. They are also expected to create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all personnel and contractors observe these policies.
 - D. Each Sound Workforce member is individually responsible for seeking answers to questions and/or issues he or she does not understand in these policies and procedures, including bringing ambiguous, incomplete or erroneous policies, procedures and practices to the attention of Sound administration.
 - E. Sound administration, including the Sound Board of Directors (the “Board”), bears responsibility for creating and promoting a climate for maintaining the security of Sound’s information systems environment.
- III. Purpose. These HIPAA Policies and Procedures relating to information security are established to:
- A. Protect against unauthorized access or use of such records or information that would result in substantial harm or inconvenience to Sound’s patients;
 - B. Protect Sound’s information systems from threats that would result in unreasonable delay or inconvenience to our patients;
 - C. Protect Sound’s investment;
 - D. Safeguard the information contained within these systems in accordance with regulatory requirements;
 - E. Reduce business and legal risks; and
 - F. Protect Sound’s reputation and promote patient confidence.
- IV. Board Oversight. All HIPAA Policies and Procedures will be reviewed and approved by the Board, or an appropriate committee thereof, and the Board or such committee will have such other responsibilities as specified herein.
- V. Clarification of General Policy. This general policy is subject to clarification by more specific policies and/or procedures.

SOUND HIPAA POLICY AND PROCEDURE DESIGNATION OF SECURITY OFFICER	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will designate an appropriate person to fill the position of Security Officer.

- I. Designation. The Board will appoint a HIPAA Security Officer who is charged with the duties listed below. The following individual is designated as the Security Officer for Sound:

Zima Hartz
 Sound Inpatient Physicians, Inc.
 1123 Pacific Avenue
 Tacoma, WA 98422
 (253) 284-1874

- II. Duties. The duties of the Security Officer shall include, but not be limited to:
- A. Developing and implementing security policies and procedures in accordance with the HIPAA Security Rule and all other applicable laws;
 - B. Providing leadership and assume accountability for Sound’s compliance with the HIPAA Policies and Procedures related to security;
 - C. Coordinating risk assessment and risk management activities to ensure ongoing identification of threats to the confidentiality, integrity and availability of ePHI and selection of appropriate safeguards to manage and reduce risks;
 - D. Ensuring that operations comply with Sound’s policies and procedures related to security and that security policies, procedures, and practices are revised as needed;
 - E. Reviewing and investigating all security incidents and ensuring that response and reporting procedures are followed and that harm caused by security incidents is mitigated to the extent practicable;
 - F. Cooperating with oversight agencies in any investigations of security violations;
 - G. Developing and conducting training on and fostering awareness of security policies and procedures to ensure that all members of the Sound Workforce, including management, receive adequate and appropriate security training;
 - H. Ensuring that all documentation required by the HIPAA Security Rule is created and maintained for six years from the date it was created or was last in effect, whichever is later;

- I. Serving as an internal and external liaison and resource with outside entities (including business associates, technology vendors, trustees, and other parties) to ensure that Sound's security practices are implemented, consistent and coordinated; and
 - J. Performing other duties as assigned by Sound management and/or the Board.
- III. Term of Service of Security Officer. The Security Officer shall serve until removed by the Board, or until he or she resigns the position.

SOUND HIPAA POLICY AND PROCEDURE SECURITY MANAGEMENT	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will regularly evaluate potential risks to the confidentiality, integrity and availability of ePHI, quantify the level of risk and develop and implement a strategy for minimizing or eliminating the risk.

I. Risk Assessments.

- A. Sound has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Sound (a “Risk Assessment”). The Risk Assessment results are contained in a HIPAA Risk Analysis Report that evaluates potential security risks, quantifies the level of risk, and develops strategies for minimizing the risks.
- B. The existing Risk Analysis Report will be reviewed periodically in order to audit continued compliance with the HIPAA Security Rule and to evaluate Sound’s effectiveness in reducing security risks.
- C. Sound will perform a Risk Analysis [**biennially**], as provided below, but risks may also be identified through other means, such as during a more limited risk assessment, exams, audits and through daily operations.
 - 1. A limited risk assessment can be conducted on any division or section of Sound or any outside entities providing services to Sound, if consistent with the contract with that outside entity. A limited risk assessment can be conducted on any Sound information system, to include applications, servers, networks, and any process or procedure by which these systems are administered, maintained, and/or utilized.
 - 2. A full Risk Analysis will be performed [*at least biennially*] on Sound’s information systems environment to examine existing risks as well as address changes that may give rise to any new threats to ePHI. This Risk Analysis will consist of the following steps:
 - (a) A detailed inventory of Sound’s ePHI and information systems that contain ePHI.
 - (b) Identification of all potential threats to ePHI and related information systems.
 - (c) Analysis and documentation of the security controls that have been implemented to protect ePHI.
 - (d) Estimation of the likelihood that each identified threat will occur.

- (e) Determination of the impact that would result if a threat were to occur.
- (f) Use of the above information to identify the level of risk to specific ePHI and related information systems.
- (g) Proposing security controls that can mitigate or eliminate identified unacceptable risks to ePHI.

3. The results of the full Risk Analysis will be incorporated into an updated Risk Analysis Report, which shall be presented to Sound management and the Board, or an appropriate committee thereof.

D. The Risk Analysis Report will be retained for six years from the date it is completed or last updated, whichever is later.

II. Risk Management. As risks are identified through limited risk assessments, full Risk Analyses, exams, audits, and/or general operations, the Security Officer will develop strategies to address and prioritize the mitigation of the risks. All risks may not be mitigated. At Sound's discretion, certain risks may be deemed as acceptable due to the conditions and circumstances particular to Sound. The Security Officer will oversee implementation of the risk mitigation strategies.

SOUND HIPAA POLICY AND PROCEDURE SECURITY AWARENESS TRAINING	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will provide information security training to all Sound Workforce members, to include specific information about policies, procedures and practices for safeguarding the confidentiality, integrity and availability of ePHI and maintaining the security of Sound's information systems environment.

I. Required Training.

- A. These HIPAA Policies and Procedures set forth best practices, guidelines, and stipulations concerning the security of Sound's information systems environment with which all members of the Sound Workforce must comply.
- B. All Sound Workforce members will be educated on the relevant provisions of these HIPAA Policies and Procedures.
- C. All Sound Workforce members must attend information security training *at least annually*. Each new Sound Workforce member will receive Security Training appropriate to his or her position prior to accessing any network system or electronic data.
- D. Outside third parties who access Sound's information systems must do so in compliance with these HIPAA Policies and Procedures and will be provided access to the applicable portions of these HIPAA Policies and Procedures, as necessary.

II. Acknowledgment of HIPAA Policies and Procedures. Prior to accessing network systems and data, all Sound Workforce members must read and acknowledge their understanding of Sound's HIPAA Policies and Procedures relating to network security.

III. Updates and Security Reminders.

- A. The Security Officer will provide the Sound Workforce with periodic reminders concerning security risks, incidents and issues through various means such as interoffice memos, email, and staff meetings.
- B. Whenever a material change is made to these HIPAA Policies and Procedures or other security practices, all Sound Workforce members affected by the change shall be trained regarding the change within a reasonable period of time, as defined by the Security Officer.

IV. Documentation of Training.

- A. The completion of training required by this Policy and Procedure shall be documented by either the individual who offered the training or the Security Officer acting upon a credible report from the individual who offered the training.
- B. This documentation shall be retained for at least six years from the date of its creation.
- C. Security Training attendance shall be documented in each Sound employees' personnel file.

V. Oversight and Enforcement.

- A. The Security Officer shall implement and oversee all training required by this Policy and Procedure. To accomplish this task, the Security Officer shall have the authority to consult with and delegate authority, as well as appoint committees to develop and perform training activities.
- B. If a Sound Workforce member purposefully fails to attend or participate in the designated training required by this Policy and Procedure, the member shall be subject to sanctions under the Policy and Procedure entitled "**SANCTIONS FOR SECURITY VIOLATIONS**".

SOUND HIPAA POLICY AND PROCEDURE AUDITS AND EVALUATION	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will test the successful implementation of security controls by performing routine audits of these HIPAA Policies and Procedures and their supporting components. Testing and auditing of information system activity are necessary to ensure and enforce proper implementation of security practices. Through auditing, controls used and tests of these controls are evaluated for implementation and successful application.

I. Audits.

A. Audits may be conducted for any one or more of the following purposes:

1. Ensure integrity, confidentiality and availability of information and resources;
2. Investigate possible security incidents;
3. Ensure compliance with these HIPAA Policies and Procedures that are related to information system security;
4. Ensure compliance with any law or regulation applicable to Sound's operations; and
5. Monitor user or system activity where appropriate.

B. As required by the HIPAA Security Rule, information system activity review will be part of the audit process.

1. Sound will periodically review records of information system activity in order to prevent, detect, correct and contain any violations of the HIPAA Security Rule or these HIPAA Policies and Procedures.
2. Internal review of a random sample of records of information system activity will be conducted on a periodic basis as determined by the Security Officer. A random sample of access and activity logs and security incident logs will be reviewed. A more extensive internal audit may be conducted if the results of this periodic review indicate that it is necessary.
3. The Sound Workforce shall be periodically reminded that records of information system activity are reviewed on a regular basis.

C. As required by the HIPAA Security Rule, the audit process will include periodic evaluations to establish the extent to which these HIPAA Policies and Procedures comply with the requirements of the HIPAA Security Rule.

1. Sound shall perform periodic evaluations that consist of a review of the technical and non-technical components of Sound's security environment and Sound's compliance with the requirements of the HIPAA Security Rule.
 2. Additional evaluations shall be conducted whenever there are environmental or operational changes affecting the security of ePHI created, received, maintained or transmitted by Sound.
- D. During an audit, any access needed will be provided to the Security Officer, his or her designee, or an outside auditor, as appropriate for the performance of the audit. This access may include:
1. User level and/or system level access to any computing or communications device present on Sound's premises, but which may not be owned or operated by Sound.
 2. Access to information (electronic, hardcopy, *etc.*) that may be produced, transmitted, or stored on Sound's equipment or premises.
 3. Access to work areas (labs, offices, cubicles, storage areas, *etc.*).
 4. Access to interactively monitor and log traffic on Sound's networks.

II. Documentation.

- A. Records of information system activity shall be maintained as needed and appropriate to facilitate audits, risk assessments and analyses, evaluations, and investigations of suspected security incidents or violations.
- B. The audit program and schedule, all internal and external audit reports and documentation of any additional evaluations shall be maintained for at least six years from the date they were created or last updated.

SOUND HIPAA POLICY AND PROCEDURE INFORMATION SYSTEMS INVENTORY	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will develop and maintain an accurate and up-to-date information systems inventory and network diagram documenting the mapping of all network equipment.

Sound will maintain an accurate inventory of all company owned hardware and software.

The inventory shall document the movements of all hardware and software and any person responsible for that movement.

SOUND HIPAA POLICY AND PROCEDURE PHYSICAL SECURITY	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will provide for the protection of all information system equipment and data stored on the equipment from theft, fire, failure of supporting utilities, and structural damage or collapse. Although system availability may deteriorate during extreme situations, a recovery plan will be in place and be familiar to the recovery team in the event of a disaster.

I. Equipment Locations.

- A. A list of all critical information system equipment will be maintained by the Security Officer.
- B. Equipment used in support of Sound's information technology systems may not be removed from Sound's facilities without prior written authorization from the Security Officer or his/her designee.
- C. All removals of information technology systems equipment will be logged.

II. Physical Access. All physical access to information system equipment must be approved by the Security Officer.

- A. The Security Officer will maintain an access list indicating all personnel authorized to access critical equipment and server rooms and each person's level of access by job duties.
 - 1. Access will be evaluated on an individual basis depending upon the Sound Workforce member's job duties.
 - 2. Changes to an employee's job responsibilities require immediate review of physical access.
- B. To ensure that only authorized individuals have access to Sound's information systems and the facilities in which they are housed, access is controlled and validated by identification badges and magnetic card readers.
- C. A former Sound Workforce member may not have physical access to non-public areas of the building housing the systems or the data contained on the systems at any point after ending employment with Sound.
- D. No guests, including without limitation, service contractors, auditors, and maintenance personnel, may have unattended access to equipment without the approval of the Security Officer.

- III. Maintenance. The Security Officer will maintain a log documenting all repairs or modifications that are related to the security of information systems equipment.
- IV. Contingency Operations. Loss of physical access due to fire, natural disasters, and man made disasters, or failure of supporting utilities shall be addressed in the Disaster Recovery Plan maintained in Sound's IT Department.

SOUND HIPAA POLICY AND PROCEDURE CONTINGENCY PLAN	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound will establish a contingency plan to respond to emergencies, disasters or other occurrences that damage systems that contain ePHI. Systems include all hardware, software, and data required to support processes necessary for Sound operations. As a minimum standard, all critical system recovery should minimize downtime and allow key business functions to continue to operate. System backups and disaster recovery planning are required to facilitate recovery.

I. Plan Components. The contingency plan shall consist of three components:

A. Data Backup Plan. Sound's critical data will be backed up on a regular schedule that will provide a mechanism for data recovery in the event data is lost or damaged. Backup procedures will create and maintain retrievable exact copies of ePHI.

B. Disaster Recovery Plan.

1. A Disaster Recovery Plan will be developed to provide for the restoration of any data lost as a result of a system interruption caused by emergencies, disasters or other occurrences.
2. The Disaster Recovery Plan will coordinate with the Emergency Mode Operation Plan for maintaining critical services.

C. Emergency Mode Operation Plan.

1. The Emergency Mode Operation Plan shall contain processes to enable continuation of critical business processes in the event of a disaster or emergency that damages information systems containing ePHI.
2. The Emergency Mode Operation Plan will be activated when an emergency that may impact critical business processes is reasonably anticipated, as well as in an actual emergency.
3. The Emergency Mode Operation Plan will specifically address the restoration of Sound operations.

II. Testing and Revision. Each component of the contingency plan shall be tested as determined necessary by the Security Officer, but no less than biennially, with results of the tests sent to the Board, or an appropriate committee thereof, for review. The results of such testing shall be documented and retained for six years. Based upon the results of testing, the procedures set forth in each of the plan components shall be revised as needed.

III. Insurance. Coverage will be maintained on information systems and data to adequately protect Sound from severe financial loss due to malicious activity and natural disasters.

SOUND HIPAA POLICY AND PROCEDURE INFORMATION ACCESS MANAGEMENT	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound Workforce members' access to ePHI is authorized, established, maintained and modified based on the minimum amount of PHI necessary for individual Sound Workforce members to perform their jobs effectively.

I. Access Authorization. The Security Officer will determine and assign the appropriate access privileges to ePHI.

A. Access to ePHI is granted to Sound Workforce members in accordance with their job function, as set forth in the Policy and Procedure entitled "**MINIMUM NECESSARY USES AND DISCLOSURES**".

1. Any Sound Workforce member who is authorized under the Policy and Procedure entitled "**MINIMUM NECESSARY USES AND DISCLOSURES**" to access PHI for a particular purpose is authorized to access ePHI for that purpose. Other Sound Workforce members are not authorized to access ePHI.

2. Managers and supervisors shall supervise all Sound Workforce members who work with ePHI or in areas where it may be accessed to ensure that such persons are complying with this Policy and Procedure.

B. A vendor that has signed a Business Associate Agreement may, if appropriate, be granted access to ePHI. Any third party who works with ePHI or in areas where it may be accessed must receive appropriate authorization from the Security Officer and be supervised at all times while on-site.

II. Access Establishment.

A. After the Security Officer authorizes access privileges for a Sound Workforce member, a unique user account is established that enables a Sound Workforce member to access ePHI and Sound's information systems as appropriate to his or her job function. Each user account is defined by a User ID and password. Passwords must comply with the Policy and Procedure entitled "**PASSWORDS**".

B. If appropriate and approved in writing by the Security Officer, a unique user account may be established for a vendor. The vendor shall be allowed access only to such ePHI that is necessary for the vendor to perform its services for Sound.

C. The Security Officer will maintain a list of authorized users, user accounts and access privileges.

III. Review and Modification of Access Rights.

- A. The Security Officer will review, adjust and/or terminate Sound Workforce members' access to ePHI as appropriate.
 - 1. Access assignments will be reviewed periodically to ensure that each Sound Workforce member's access authorizations match the description of his or her position within Sound.
 - 2. When the position or assigned duties of a Sound Workforce member changes, the Security Officer will review and adjust, as appropriate, the Sound Workforce member's authorization to access ePHI.
 - 3. When a Sound Workforce member is no longer engaged by Sound, access privileges to ePHI and to Sound's information systems and the facilities in which they are located shall be terminated as soon as the Sound Workforce member's termination is effective, or sooner if circumstances warrant.
- B. The Security Officer will review any vendor accounts and access levels at least semi-annually and make any modifications to such access rights as are necessary. Vendor accounts shall be terminated immediately upon expiration of the contract or other business relationship with the vendor.

SOUND HIPAA POLICY AND PROCEDURE WORKFORCE SECURITY	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound Workforce members who require access to ePHI in order to perform their job duties shall have appropriate access to such data. Sound shall take measures to prevent those Sound Workforce members who are not authorized to access ePHI from obtaining such access.

I. Authorization and Supervision.

- A. Sound Workforce members who work with ePHI or in areas where it may be accessed shall have received appropriate authorization to do so and will be properly supervised pursuant to Sound's Policy and Procedure entitled "**INFORMATION ACCESS MANAGEMENT**".
- B. Management will immediately inform the Security Officer when the services of a Sound Workforce member are terminated or his or her job responsibilities are changed. The Security Officer will immediately disable the Sound Workforce member's User ID or make changes to the Sound Workforce member's access level, as appropriate.

II. Workforce Clearance Procedure. The hiring practices of Sound include reference and background checks and other appropriate mechanisms to ensure that appropriate access to ePHI is granted.

- A. The background of all Sound Workforce members shall be adequately reviewed during the hiring process.
- B. Verification checks must be made, as appropriate, based on the Sound Workforce member's probable access to Sound information systems containing ePHI and his or her expected ability to modify or change such ePHI and based upon Sound's risk analysis. Verification checks may include, without limitation: (i) character references; (ii) confirmation of claimed academic and professional qualifications; (iii) professional license validation; (iv) criminal background check; and (v) OIG database check.
- C. When job candidates are provided via an agency, Sound's contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.

III. Termination Procedures.

- A. When a Sound Workforce member no longer needs access to ePHI to perform his or her job effectively, the member's access to ePHI is terminated.
 - 1. The Sound Workforce member's password is revoked or changed, as appropriate.
 - 2. The Sound Workforce member's name and user account, as appropriate, will be deleted from the list of those authorized to access ePHI.

- B. When a Sound Workforce member is no longer employed by Sound, access privileges to ePHI, Sound's information systems and the facilities in which they are located is terminated.
1. The former member's user account and access privileges will be revoked, and his or her name will be deleted from the information systems access list(s).
 2. The former member's password is revoked.
 3. Sound's People Support will obtain the following items from the former member, as applicable: (i) ID badge; (ii) keys; and (iii) laptop. **[Adjust list as appropriate.]**
 4. Locks, combinations and/or codes allowing access to Sound's information systems and the facilities in which they are housed will be changed if the circumstances warrant this safeguard.

SOUND HIPAA POLICY AND PROCEDURE TECHNICAL ACCESS CONTROLS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound has implemented technical security measures for Sound’s electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

I. Unique User ID.

- A. Access to Sound’s information systems will be controlled by a unique User ID and password.
- B. All individual users are accountable for all activity and access that occurs under their logon.
- C. Sound’s People Support Department will immediately inform the Security Officer when the services of a Sound Workforce member are terminated or his or her job responsibilities are changed. The Security Officer will immediately disable the Sound Workforce member’s User ID or make changes to the Sound Workforce member’s access level, as appropriate.

II. Emergency Access Procedure. Procedures have been put in place to facilitate Sound Workforce members’ access to ePHI or Sound’s information systems in an emergency situation, to include procedures for obtaining, monitoring and terminating access to ePHI in an emergency.

III. Automatic Log Off/Lock Out Features.

- A. Users will lock or log off of workstations when left unattended and should close applications when not in use.
- B. SoundConnect, the software system that contains most of Sound’s ePHI, automatically converts to a blank screen after five minutes of inactivity. After a further ten minutes of inactivity, the SoundConnect software automatically shuts off and requires users to log-in to the software again. In addition, user accounts for the general Sound network will be automatically logged off or locked after [minutes] of inactivity to restrict access to the network if the user inadvertently leaves the computer logged on after hours or during extended time away from the workstation.
- C. Sound has implemented encryption tools for its SoundConnect software system, as well as an account lockout feature for its network, that prevents password penetration of Sound’s systems. Sound encrypts the passwords for its SoundConnect system to prevent unauthorized access to such passwords. In addition, the User IDs for Sound’s network will be locked out after three consecutive failed attempts to access the systems. The Security Officer has put into place procedures for re-establishing User ID access and re-setting passwords.

IV. Encryption. Sound has determined that it is not reasonable and appropriate to encrypt ePHI that is stored in Sound's information system in order to control access to such ePHI.

SOUND HIPAA POLICY AND PROCEDURE PASSWORDS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Passwords for access to Sound’s information systems shall comply with this Policy and Procedure.

- I. User Responsibility. Sound network users and SoundConnect users (including employees, contractors and vendors with access to Sound’s systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- II. Confidentiality.
 - A. Passwords shall be changed periodically, as provided below, and in the event of a security breach or other security incident.
 - B. Computer passwords shall remain strictly confidential and shall not be divulged, orally or in writing, by any Sound Workforce member. The password’s owner is responsible for the security of that password.
 - C. Passwords may not be written down, printed, or stored in unencrypted electronic format.
 - D. Sound Workforce members logging onto a computer workstation will ensure that no one observes the entry of his or her password.
 - E. Sound Workforce members will not log onto a computer workstation using another’s password nor permit another to log on with his or her password. The exception to this rule would be for information technology staff or vendors to use a password during maintenance or to provide assistance to a user.
 - F. After three consecutive failed attempts to log on to Sound’s network, the Sound systems will refuse to permit access.
 - G. The Security Officer has procedures in place to assign a new password should a user forget his or her existing password.
 - H. Passwords for the SoundConnect system are encrypted.
 - I. Sound requires passwords to its network to be changed every sixty days.

- III. Training. Sound shall include in its Security Training, education regarding creating passwords, the importance of regular password changes, password change intervals and safeguarding passwords.

Infectious Disease Associates HIPAA Policy and Procedure WORKSTATION USE	Policy No.:	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

In compliance with the HIPAA Security Rule, Sound has established guidelines for workstation use to promote reasonable security and safeguards in the handling of ePHI. These guidelines specify proper equipment operation procedures, functions to be performed, and the physical attributes of the surroundings of the workstation, focusing on reasonable controls for workstations that can access ePHI.

- I. Workstation Defined. A *workstation* is an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

- II. Guidelines for Proper Workstation Use.
 - A. All computer workstations that are plugged into an electrical power outlet shall use a surge protector.
 - B. Only computer terminals, laptops and other devices authorized by the Security Officer may be connected to Sound's information systems.
 - C. Only software or application programs authorized by the Security Officer may be installed or loaded onto Sound's information systems equipment, including without limitation, individual computer terminals.
 - D. System settings, which include hardware and software modification, shall not be reconfigured by any user using the control panel without the Security Officer's express permission. Users shall not disable virus protection software under any circumstances.
 - E. Data files or applications from Sound's network server should not be downloaded or copied to workstations, home computers, diskettes, CD ROM or other storage media without authorization.
 - F. Workstations shall not be shared by individuals that have different levels of confidential information clearance.
 - G. Each Sound Workforce member using a computer workstation is responsible for the content of any data he or she enters into the computer workstation or transmits through or outside Sound's system.
 - H. Sound Workforce members shall not store, access or transmit any confidential records of Sound, its patients, employees, or vendors without adequate authority to do so.

- I. No Sound Workforce member may disclose confidential information unless they are properly authorized and such disclosure is in compliance with the HIPAA Privacy Rule and these HIPAA Policies and Procedures.
- J. Email that contains ePHI must be encrypted before transmission, and all such e-mail must comply with the Policy and Procedure entitled “**TRANSMISSION OF PHI VIA ELECTRONIC MAIL**”.
- K. Sound Workforce members and other authorized users of Sound’s information system are strictly prohibited from (i) effecting security breaches or disruptions of network communication; (ii) circumventing user authentication or security of any host, network or account; or (iii) uploading, downloading, storing or otherwise knowingly accessing or transmitting in any fashion any virus, worm, Trojan horse, trap door, or any other malicious program code.

SOUND HIPAA POLICY AND PROCEDURE WORKSTATION SECURITY	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Only authorized users may access Sound's systems. Accordingly, Sound has implemented physical safeguards for all workstations that access ePHI to restrict access to authorized users.

I. Physical Safeguards.

- A. Sound Workforce members will monitor their workstations and take appropriate measures to protect workstations from potential threats. Sound Workforce members shall report potential threats to the computer equipment and/or to the integrity and confidentiality of data contained in the equipment to the Security Officer or his or her designee.
- B. Workstations should be secured to surfaces with cables or other locking mechanisms to prevent theft.
- C. Workstations (including home computers, if applicable) that access ePHI must be located in secure areas with minimal risk of unauthorized access.
- D. Computer monitors must be positioned in a manner that prevents unauthorized persons from viewing screen contents.
- E. SoundConnect will automatically convert to a blank screen after five minutes of inactivity. After a further ten minutes of inactivity, SoundConnect will automatically shut off and will require users to log-in to the SoundConnect system again. In addition, computer screens shall return to a password protected screensaver if the computer is left unattended for longer than [minutes] to avoid or minimize the likelihood of unauthorized persons viewing on-screen data.
- F. Workstations and terminals shall be logged off and/or locked up when Sound Workforce members operating such stations are on an extended break or have left for the day. Sound Workforce members should log off of the Sound system when they will be away from their computer workstation for more than 15 minutes.
- G. An account lockout feature will be implemented on the local network to prevent password penetration of Sound's systems. The User ID will be locked out after three consecutive failed attempts to access the systems. The Security Officer will have procedures in place for re-establishing User ID access and re-setting passwords.
- H. Sound Workforce members shall maintain their confidential passwords in compliance with the Policy and Procedure entitled "**PASSWORDS**".

SOUND HIPAA POLICY AND PROCEDURE INTEGRITY OF ELECTRONIC PHI	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound has implemented electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner during transmission or while being stored and used on Sound’s systems and to authenticate the identity of the person or entity seeking access to ePHI.

I. Data Integrity.

- A. Sound will use the methods set forth in the Policy and Procedure entitled “**ANTI-VIRUS STANDARDS**” to ensure that ePHI has not been altered or destroyed by a virus or other malicious code while it is stored in Sound’s information systems.
- B. All equipment used to access, transmit, receive or store ePHI shall be appropriately secured in accordance with the Policy and Procedure entitled “**PHYSICAL SECURITY**”.

II. Transmission Integrity.

- A. All transmissions from the Sound network to an outside party or network must utilize an encryption mechanism between the sending and receiving entities. For transmissions via e-mail, Sound Workforce members also shall follow the Policy and Procedure entitled “**TRANSMISSION OF PHI VIA ELECTRONIC MAIL**”.
- B. Transmission of ePHI within Sound’s system is permitted without additional security measures or safeguards so long as only a minimal amount of ePHI is being transmitted and all other applicable Policies and Procedures are followed.

III. Encryption. When files or data are encrypted, only those methods that have received substantial public review and have been proven to work effectively shall be used. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.

IV. Person or Entity Authentication. As described in the Policy and Procedure entitled “**TECHNICAL ACCESS CONTROLS**”, a unique User ID and authentication through a strictly controlled password is required to access any system that maintains or accesses ePHI, and automatic log-off and account lockout features have been implemented on Sound’s information systems that contain ePHI.

SOUND HIPAA POLICY AND PROCEDURE ANTI-VIRUS STANDARDS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

All Sound computers must have Sound's standard, supported antivirus software installed.

I. Responsibility. Sound's IT Department is responsible for creating procedures to verify that antivirus software is updated and systems are scanned at regular intervals.

II. Virus Protections.

A. Antivirus software has been installed on all Sound information systems.

1. The Security Officer shall ensure that vendor information on the availability of updates for antivirus software is monitored regularly.

2. The Security Officer shall oversee the installation of all updates to antivirus software and maintain audit documentation indicating the time and name of the person who updated the software.

B. Virus-infected computers must be removed from the network until they are verified as virus-free.

C. Any activities with the intention to create and/or distribute malicious programs into Sound's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited, in accordance with the Policy and Procedure entitled "**WORKSTATION USE**".

III. Information and Training.

A. On a regular basis, Sound shall notify Sound Workforce members and other authorized users of its information systems of new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents.

B. Each authorized user shall be informed as to appropriate actions to protect systems from such risks and the timeline for antivirus software updates.

C. Sound shall include in its Security Training material information discussing the harms that can be caused by malicious codes and computer viruses, the methods of infection, safe computing practices, and what to do when a computer becomes infected.

SOUND HIPAA POLICY AND PROCEDURE MONITORING AND AUDIT CONTROLS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately secured, Sound has implemented the following procedures for monitoring activity in information systems that contain ePHI.

- I. Monitoring. Sound reserves the right to monitor system access and activity of all authorized users of Sound information systems. Accordingly, each Sound information system containing ePHI must utilize a mechanism to log and store system activity.

- II. Log-In Monitoring. A mechanism to log and document log-in attempts and activities has been implemented on each system that contains ePHI.
 - A. All failed log-in attempts of a suspicious nature, such as continuous failed attempts, must be investigated by the Security Officer.
 - B. Sound shall include in its Security Training information on the existence of log-in monitoring mechanisms and their importance.

- III. Audit Log.
 - A. Sound shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
 - B. Sound shall maintain audit logs regarding system activity logs for each system that contains or uses ePHI. All access to and changes made to ePHI shall be logged.

- IV. Review and Audit.
 - A. Audit logs shall be examined periodically in order to identify questionable data access activities, investigate breaches, access the security program, and aid in responding to potential weaknesses. In addition, audit logs shall be reviewed pursuant to the Policy and Procedure entitled “**AUDITS AND EVALUATION**”.
 - B. Reviews of audit logs must be documented and maintained for six years.

SOUND HIPAA POLICY AND PROCEDURE DEVICE AND MEDIA CONTROLS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Sound shall manage the receipt and removal of hardware and electronic media that contain ePHI into and out of Sound’s facilities and the movement of these items within Sound’s facilities.

- I. Purpose. Device and media controls are designed to facilitate the control of the flow of ePHI onto and from the premises. The control of the flow of information is enhanced by following carefully designed steps when disposing of media, when re-using media, by documenting how, when, and where hardware and software is accounted for, and backing-up ePHI and storing ePHI within acceptable practices.

- II. Disposal.
 - A. The Sound Workforce shall comply with the Policy and Procedure entitled “**DISPOSAL OF PHI**” governing the proper disposal of all PHI regardless of format (e.g., paper, magnetic tape, disk).
 - B. The Security Officer will oversee the shredding of all documents and reports that contain security and system configuration information.
 - C. Any information should be reviewed prior to destruction to ensure compliance with Sound’s record retention policies and with applicable legal and regulatory requirements.

- III. Accountability.
 - A. Pursuant to the Policy and Procedure entitled “**INFORMATION SYSTEMS INVENTORY**”, a complete inventory of hardware and software, their movements, and any person responsible for those movements is maintained.
 - B. If a Sound Workforce member or another person wishes to remove ePHI from the premises of Sound, prior approval by the Security Officer is required, and the removal and subsequent return of any electronic media containing ePHI shall be logged. The log shall be maintained by the Security Officer.

- IV. Removable Media Controls.
 - A. In general, the use of removable media is discouraged. Sound provides a network that provides for transmission of information between company computers requiring minimal need for the use of removable media for transport.
 - B. Information stored on removable media must be protected to the same degree as information stored on Sound information systems. Such media must be appropriately labeled so as to identify it as PHI, and it must never be left unattended in unsecured areas.

- C. Confidential data stored on removable media must not be transported outside of Sound facilities unless approved by the Security Officer. If transported off the premises, ePHI must be logged and must be either in direct control of an authorized Sound Workforce member or under physical lock granting access to only an authorized Sound Workforce member.
 - D. If ePHI is stored on a mobile computing device, and there is a breach of confidentiality of the ePHI, Sound will follow the Policy and Procedure entitled “**NOTIFICATION OF BREACH OF UNSECURED PHI**”.
- V. Mobile Computing Devices.
- A. PHI must never be stored on mobile computing devices unless the devices have the following minimum security requirements implemented:
 - 1. The device must be running an operating system that requires secure login via a password.
 - 2. The files stored on the device must be subject to safeguards that have been approved by the Security Officer.
 - 3. The device must have other security requirements, as required by the Security Officer in his or her sole discretion.
 - B. Mobile computing devices must never be left unattended in unsecured areas.
 - C. If ePHI is stored on a mobile computing device, and there is a breach of confidentiality of the ePHI, Sound will follow the Policy and Procedure entitled “**NOTIFICATION OF BREACH OF UNSECURED PHI**”.
- VI. Media Re-Use. The Security Officer shall ensure that the hard drives of computers, other media of computer equipment, and all removable storage media are appropriately wiped clean of ePHI prior to any re-use of the same.
- A. ePHI is removed from hard drives or electronic media prior to re-use by the IT Department.
 - B. The effective removal of ePHI from hardware or electronic media is verified prior to allowing re-use.
- VII. Data Backup and Storage. Sound shall create a retrievable, exact copy of any ePHI, when needed, before the movement of any equipment.

SOUND HIPAA POLICY AND PROCEDURE ELECTRONIC COMMUNICATIONS	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

Communications travel into and out of Sound’s environment through a variety of technologies. The purpose of this policy is not to define all possible technologies and security procedures, but to identify communication methods and set guidelines for their security. Electronic communication systems are provided to increase the efficiency and communications of Sound operations.

- I. Network. The internal network is provided for communication between Sound information systems for business purposes. Users are strictly prohibited from connecting non-company systems to the Sound network except with Security Officer approval.
- II. Internet. Access to the Internet is provided by Sound for business purpose and all activity must comply with Sound’s Policy and Procedure entitled “**WORKSTATION USE**”.
- III. Fax Machines. Fax machines are provided for business use. All fax machine locations must be approved by the Privacy Officer. Facsimile transmissions will comply with all other Sound policies and procedures, including without limitation, the Policy and Procedure entitled “**TRANSMISSION OF HEALTH INFORMATION VIA FACSIMILE**”.
- IV. Wireless Communication. Access to Sound networks via wireless communication mechanisms may only be done through secure network connections.

SOUND HIPAA POLICY AND PROCEDURE SECURITY INCIDENT MANAGEMENT	Legal Policy Number 4-II	
	Origination Date: 06/11/2010	Review/Revision Date: 06/30/2013

It is the policy of Sound to facilitate the reporting of and response to security incidents that have the potential to allow unauthorized access, disruption, damage, or theft of information resources. Incident response shall provide reasonable methods for limiting the impact on Sound's information systems due to an incident and for facilitating the progressive and successful investigation of an incident.

I. Security Incident Defined.

- A. A *security incident* is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
 - 1. Security incidents may be caused by failure of a security mechanism or an attempted or threatened breach of these mechanisms is considered a security incident.
 - 2. Security incidents may be recognized by individuals observing the incident, learning of the incident at a later time, finding the results of an incident, or by software monitoring and alerting.
- B. Examples of information security incidents include, but are not limited to (i) unauthorized disclosure, whether intentional or inadvertent, of ePHI; (ii) unauthorized use, alteration, reproduction, or destruction of ePHI; (iii) unauthorized use of user IDs, passwords, or access codes; (iv) failure to protect User IDs, passwords, or access codes (i.e., sharing codes, posting at workstation, *etc.*); (v) unauthorized access to the computer room or to a workstation; (vi) indications of a computer virus; or (vii) theft or tampering of computer equipment.

II. Reporting.

- A. Breaches in information security will be reported in writing to the Security Officer. Reports may be made in writing directly to the Security Officer or through a secure and confidential incident reporting method established for reporting such incidents (*e.g.*, drop box, hotline, email address designated for incident reporting).
 - 1. If a Sound Workforce member is uncertain as to whether or not an incident is a risk to information security, he or she should report the incident.
 - 2. Security risks may not be intentionally covered up or hidden by anyone aware of the risk.
- B. All employees will be provided with the name of the Security Officer and any delegates along with a method of contact. A notice will be placed in common areas of the building

identifying the Security Officer and methods of contact. The Security Officer will ensure the availability of any forms needed to report security incidents.

- C. No punitive or retaliatory action may be taken against any individual as a result of incident reporting.

III. Incident Management.

- A. Responsibilities of the Security Officer with regard to incident management include:

1. Confirming that an incident has occurred or is occurring.
2. Performing an investigation and documenting the results appropriately. Sound Workforce members shall cooperate with the Security Officer during the investigation.
3. Advising senior management of incidents, progress, and results on a monthly basis.
4. Implementing the appropriate course of action, including further investigation if merited and mitigation of the harmful effects of the incident.
 - (a) If the information security incident involves suspected malicious, fraudulent, or criminal activity, the Security Officer will implement mitigation efforts and consult with Sound management as to other appropriate actions.
 - (b) If the incident involves compromise of Sound's computer systems (such as a computer virus or a suspected penetration of the computer systems), the Security Officer will consult IT personnel, the computer maintenance provider, or the appropriate service provider to determine the appropriate course of action in order to mitigate the harmful effects of such incident.
 - (c) If the information systems incident is of a minor nature, the Security Officer will decide upon an appropriate course of action with regard to protecting the information systems and mitigating any harmful effects.
 - (d) If the incident involves a violation of these HIPAA Policies and Procedures, the Security Officer shall, in consultation with the Privacy Officer, impose appropriate sanctions. **All unauthorized disclosures of ePHI must be reported to the Privacy Officer so that an appropriate accounting can be kept of such disclosures, as required by the HIPAA Privacy Rule.**
5. Assessing, on a case-by-case basis, appropriate actions to mitigate the harmful effects of a security incident in compliance with the Policy and Procedure entitled "MITIGATION".
6. Reviewing the incident to determine if changes need to be made in the HIPAA Policies and Procedures to remove or reduce the vulnerability in the future and presenting those findings to the Board, or an appropriate committee thereof.

7. Adhering to strict confidentiality of all information collected surrounding the incident and disclosing information to only those parties that have a legitimate need to know.
 8. Maintaining all written complaints, investigation documentation, and any corrective or disciplinary action taken for a minimum of six years.
- B. Each incident will be fully documented by the Security Officer, to include:
1. Dates and times when the incident occurred, as well as when and by whom it was discovered or reported.
 2. The investigation process and results.
 3. The names of other persons consulted and the course of action that was established.
 4. A description and dates of the implementation of the course of action.