ABACUS

Company Policies

Policies for HIPAA Compliance, Technical Support, Human Resources and Software Development

Updated August 4, 2017

Policies for Compliance with HIPAA, 21 CFR Part 1311, and ENHAC Electronic Prescriptions for Controlled Substances Certification Program for Pharmacy Vendors (EPCSCP-Pharmacy).

Table of Contents

MODIFICATION GUIDELINES, ASSUMPTIONS and NOTES

This document was created using Microsoft Word. When updating, note the following conventions:

1) Policy titles and headings are created using styles Heading 1, Heading 2 and Heading 3
2) The Table of Contents is a field and can be updated based on revised policy titles and headings by pressing the F9 key.
3) Bookmarks are used in front of Policy titles and are used for hyperlinks.
4) Microsoft Word can create an HTML version of this document for use on your internal system to facilitate ready access by your employees.
5) Update Change Log below to document changes made

Change Log

Date	Policy	Description
6/15/2017	Entire	Complete re-write of previous company policies
7/24/2017	1300	Added policy for compliance with ENHAC certification criteria

ABACUS POLICIES
POLICIES FOR ALL STAFF
1000 Definitions for HIPAA Regulations and HIPAA Policies

POLICY
The following definitions shall apply to all Confidentiality and Computer Security Policies, numbered 1000 through 4000.

AUDIENCE
All Staff

REFERENCE
The definitions below are adapted from the federal HIPAA regulations. The HIPAA Privacy regulations are at 45 CFR Part 160 and 45 CFR Part 164 Subpart E. The HIPAA Security regulations are at 45 CFR Part 160 and 45 CFR Part 164 Subparts C and D. Subpart D is the Breach Notification rule created by the HITECH Act. See:
45 CFR 164.103 Definitions
45 CFR 164.304 Definitions
45 CFR 164.402 Definitions
45 CFR 164.501 Definitions

DEFINITIONS
1) **Access** -- means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition of "access" applies to the HIPAA Security rule only, not to the HIPAA Privacy Rule.)
2) **Administrative safeguards --** administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
3) **Authentication** -- means the corroboration that a person is the one claimed.
4) **Availability** -- means the property that data or information is accessible and useable upon demand by an authorized person.
5) **Breach –** the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy rules which compromises the security or privacy of the protected health information. Breach *excludes*:
   A) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA privacy rules.
   B) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy rules.
   C) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

   Except for the two exclusions above, any unintentional acquisition, access, use or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:
   A) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
   B) The unauthorized person who used the PHI or to whom the disclosure was made;

C) Whether the PHI was actually acquired or viewed; and
D) The extent to which the risk to the PHI has been mitigated.

6) **Business Associate (BA)** - basically, is 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. The complete definition and other information is included in Appendix A - Identifying Business Associates..
7) **Confidentiality** -- means the property that data or information is not made available or disclosed to unauthorized persons or processes.
8) **Covered Entity** -- means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA privacy rules.
9) **Destruction** - means physical destruction of a record or removal of personal identifiers from information so that the information is no longer personally identifiable.
10) **Designated Record Set** – means a group of records maintained by or for a covered entity that is:
    A) The medical records and billing records about individuals maintained by or for a covered health care provider;
    B) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
    C) Used, in whole or in part, by or for the covered entity to make decisions about patients.

    For purposes of this definition, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
11) **Disclosure** -- means the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the entity holding the information.
12) **Employee** –means any person employed by the company, volunteers, board members and other persons whose conduct, in the performance of work for ABACUS, is under the direct control of ABACUS, whether or not they are paid ABACUS.
13) **Encryption** -- means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
14) **ePHI** – means PHI in electronic format.
15) **Facility** -- means the physical premises and the interior and exterior of a building(s).
16) **HIPAA** -- means the Health Insurance Portability and Accountability Act of 1996, codified in 42 USC §§ 1320 - 1320d-8.
17) **Individually identifiable health information** – means the subset of health information, including demographic information collected from an individual, and
    A) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
    B) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
        i) That identifies the individual; or
        ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
18) **Information system** -- means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
19) **Integrity** -- means the property that data or information have not been altered or destroyed in an unauthorized manner.
20) **Malicious software** -- means software, for example, a virus, designed to damage or disrupt a system.
21) **Password** -- means confidential authentication information composed of a string of characters.
22) **PHI** – PHI, short for "Protected Health Information" means individually identifiable information that is: (i) transmitted by electronic media; (ii) Maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. PHI does not include (i) information in employment records held by a covered entity in its role as an employer or (ii) Records of individuals deceased for more than 50 years.
23) **Physical safeguards** -- means physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
24) **Protected Health Information** – See PHI above.

25) **Provider** – means a person or entity which is licensed or certified to provide services, including but not limited to health care services. This includes physicians, hospitals, home health agencies, ambulance companies, physical therapists, nurses, and any other licensed patient or entity who provides "health care". A Covered Provider is a Health Care Provider who transmits any health information in electronic form.
26) **Security** or **Security measures** -- encompass all of the administrative, physical, and technical safeguards in an information system.
27) **Security incident** -- means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
28) **Social Engineering** -- "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). . . ..social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
29) **Subcontractor** – means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
30) **Technical safeguards** -- means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
31) **Unsecured protected health information** – protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology in guidance specified by the Secretary of the Department of HHS in guidance published on the HHS Web site.
32) **Use** - means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
33) **User** -- means a person or entity with authorized access.
34) **Violation**. There are different types of violations, with different contexts:
    A) **Privacy Violation** means making a use or disclosure of PHI not permitted by HIPAA regulations, the violation of a patient right established by HIPAA, or the failure to perform an administrative procedure required by the HIPAA regulations.
    B) **Employee Security Procedure Violation** means the failure of an employee to comply with one or more of the policies and procedures described in the HIPAA Security Policies section of the policies and procedures manual.
35) **Workforce Member** - means the same as employee. See definition above.
36) **Workstation** -- means 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.

1010 Confidentiality and Security – General Rules

POLICY

Client data, which contains PHI that is maintained or encountered by employees of ABACUS, including patient demographic information, diagnoses, and treatment details are Protected Health Information (PHI) which must be safeguarded per the HIPAA regulations.

ABACUS complies with all regulations regarding HIPAA. Employees of ABACUS shall not view, use or disclose PHI except in accordance with these policies. All confidentiality and computer security measures detailed in these policies will be followed by employees to protect this PHI.

AUDIENCE

All Staff

REFERENCE

45 CFR Part 160 and 164
45 CFR 164.502 General Rules for allowed uses and disclosures
45 CFR 164.504(e)(2)(i)(A) Permitted disclosures for Business Associates
EHNAC II. A.2, II. A.3, V. B.3

PROCEDURES

1) Except as otherwise authorized in these policies, staff of ABACUS may view, use or disclose PHI only for purposes of client support.
2) Employees will not copy ePHI from client systems onto media or systems owned by ABACUS.
3) When permitted, for any use and disclosure of PHI, the minimum amount of information should be used or disclosed, as detailed in Policy 1020 Minimum Necessary Policy.
4) All employees are responsible for safeguarding clients' PHI and will comply with policies detailed in
   A) Policy 1030 Confidentiality Safeguards (Oral & Written)
   B) Policy 1050 Computer Usage
   C) Policy 1060 Portable Computing Devices and Home Computer Use
   D) The facility security plan for the employee's office location, as detailed in Policy 3015 Facility Security and Access Control
5) Confidentiality and Computer Security are everyone's responsibility – all staff are obligated to report potential incidents and violations as specified in Policy 1080 Duty to Report Violations and Security Incidents.
6) Customer Service and Technical Services staff are expected to follow procedures in the sections of this manual appropriate for their departments, including
   A) Policy 2000 Technical Support Procedures
   B) Policy 2005 Secure Network Configuration for Client Networks
   C) Policy 2010 Software Development Procedures
   D) Policy 2020 Source Code Management
   E) Policy 2030 Intellectual Property
   F) Policy 2040 Authentication, Passwords and Encryption Keys
7) Sales presentations and demonstrations must not use any client PHI.
8) All employees are expected to know and understand the policies and procedures contained in this HIPAA Policy manual.
9) Employees who do not follow policies and procedures in this HIPAA Policy manual are subject to sanctions as detailed in Policy 1900 Sanctions for Staff Violations of Privacy/Security Policies

MISCELLANEOUS PROVISIONS

1) ABACUS may use and disclose PHI as necessary
   A) For the proper management and administration of the business
   B) To comply with laws and regulations as detailed in 45 CFR 164.512(a)
   C) To a business associate that is a subcontractor
2) ABACUS does not sell or otherwise release any PHI of its customers including any derivative, de-identified information, to any 3rd party for any purposes.

1020 Minimum Necessary Policy

POLICY
The use and disclosure of PHI must be limited to the minimum necessary to perform the task or make the disclosure.

AUDIENCE
All Staff

REFERENCE
45 CFR 164.502(b)(1) Minimum Necessary Standard
EHNAC II. A.2, VI. B.5, VI. C.7, VI. C.11, VI. D.1, VI. D.5

PROCEDURES

1) Company restrictions on PHI
- A) ABACUS does not maintain any customer PHI on its networks
- B) ABACUS will not provide data conversion, application, hosting services to its customers
- C) ABACUS resells clearinghouse services to clients, but transmissions are direct between customers and the clearinghouse; ABACUS does not transmit or maintain any electronic claim PHI
- D) Customer Service / Technical Services staff may be exposed to PHI while providing customer support. This could occur while on site, over the phone, or via a remote access system. See Policy 2000 Technical Support Procedures which specifies procedures for destruction of any PHI received by ABACUS during customer support activities.

2) **Limiting Workforce Access to PHI**: Access to the PHI, and to any client systems that contain PHI, will be granted based on the individual's role and determined by the Security Officer of ABACUS. The Security Officer will identify:
- A) Those persons, who require access to PHI to carry out their duties, in the workforce, including subcontractors, interns and trainees, will be listed individually with the minimum necessary PHI required for successful job performance.
- B) The security officer will maintain and update this list as necessary to ensure that it is current at all times
- C) For each person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
- D) Safeguards will be developed and documented to restrict workforce access to the minimum necessary.
- E) The Security Officer will document the results of this analysis. See Appendix E Workforce Access to PHI and Safeguards for the results of the analysis.

3) Minimum Necessary does not apply:
- A) When responding to official requests from the Secretary of HHS
- B) When making disclosures required by law.

1030 Confidentiality Safeguards (Oral & Written)

POLICY
ABACUS shall maintain appropriate physical, technical, and administrative safeguards to safeguard Paper and Oral PHI.

AUDIENCE
All Staff

REFERENCES
45 CFR 164.530(c) – Administrative, Technical, and Physical Safeguards

PROCEDURES:

1) **General Procedures**
   A) For any office and other facilities utilized by ABACUS, including employee home offices, a physical security plan will be developed to protect confidentiality and security of client PHI. Employees must be familiar with the written facility security plan developed for their location. See Policy 3015 Facility Security and Access Control. Remote workers will have a customized security plan as prescribed in Policy 1060 Portable Computing Devices and Home Computer Use.
2) **No Disclosure of Client PHI**
   A) Any PHI seen or heard by an employee during performance of his/her job duties may not be disclosed in any manner - oral, written or electronic -- except as required for his/her job duties and permitted by these policies.
3) **Oral Privacy**
   A) Any permitted discussions involving PHI will done with discretion so as not to be overheard.
4) **Safeguards for Written PHI**.
   A) In the event that PHI from the system of one of ABACUS's clients is printed (for example, for support or troubleshooting purposes) these printed pages shall be safeguarded from disclosure except as permitted by these policies.
   B) When the use of the printed information is complete, any printed PHI must be shredded promptly.
5) **Contractor Safeguards**. Any subcontractors of ABACUS shall be placed under contract to adhere to appropriate safeguards for physical security as well as to safeguard oral and hardcopy PHI.
6) **Periodic Review**. These safeguards shall be reviewed and updated periodically.

1050 Computer Usage

POLICY
Each staff member is responsible for understanding and following the policies regarding use of company workstations and additional safeguards for workstations used to access servers hosting ABACUS's service.

AUDIENCE
All Staff

REFERENCE
45 CFR 164.310(b) Workstation Use and (c) Workstation Security
45 CFR 164.308(a)(5) Log in Monitoring
EHNAC II.A.5, III.C.1, VI. B.24, VI.C.6, VI.D.2, VI.D.4

PROCEDURES
GENERAL WORKSTATION USE

1) **System is for Job Duties**. Use of computer workstations provided by ABACUS, in general, must be limited to job-related duties.
2) **Limited Personal Use of Company Equipment Authorized**. Employees are expected to be productive and to perform their job duties during work hours. Limited use of computer workstations is allowed for personal use, such as for checking the weather or reviewing personal email. Limited use is defined as less than 15 minutes per day.
3) **Storage of Client PHI Restricted**. Personnel are prohibited from storing any client ePHI on any company-owned or personally-owned devices.
4) **E-Mail Use to transmit PHI**. Employees and contractors of ABACUS must not use standard email to send unencrypted PHI. If transmission of PHI is necessary, it must be encrypted prior to attachment when using standard email, or the use of secure, encrypted email may be used.
5) **Security Awareness**. All employees should understand how to avoid malicious software.
6) **All Information Subject to Monitoring**. Employee activity on company workstations and management platforms are subject to logging and monitoring.

WORKSTATION SECURITY

7) The Technical Services department is responsible for ensuring that company approved anti-virus software is operating on all company workstations at all times, that the anti-virus software is kept up-to-date and configured properly, and that all software patching is performed.

8) All employees must understand how to avoid malicious software, and must not change any settings on the anti-virus software.

9) Software installations and updates. Employees are prohibited from installing unlicensed and/or unauthorized software. Employees must obtain permission for Technical Services prior to installing any new software.

10) Workstations must not be setup in a public access area. Workstation monitors that are used to access PHI should not face in a direction that makes visual access available to unauthorized users.

11) All ABACUS servers must be secured with a strong password (see Policy 2040 Authentication, Passwords and Encryption Keys) and setup to automatically lock out user access after a maximum of three (3) minutes of inactivity.

USER IDs and PASSWORDS FOR COMPANY INTERNAL NETWORK AND MANAGEMENT PLATFORMS

A) All employees must adhere to the guidelines for user IDs and Passwords. Each employee is assigned a unique User ID and Password for their workstation, network account, and any management platforms (RMMs, etc.) Inappropriate use of systems attributable to an employee's User ID may result in employee

sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Employees must keep their passwords secure and confidential.

B) Passwords should be at least 8 characters long and include at least 1 number, upper case letter and lower-case letter. The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed. Pass phrases consisting of three or more words strung together are acceptable. For critical resources, including firewalls and servers, a stronger password may be required.
C) Passwords should be maintained only in a company-approved password vault or memorized. Written passwords must not be kept written in the vicinity of a workstation.
D) Users are required to change all passwords at least every 12 months.
E) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.
F) When changing passwords, previously used passwords should not be recycled.
G) Separate passwords should be used for each account.
H) Default passwords supplied by a vendor must always be changed.

1060 Portable Computing Devices and Home Computer Use

POLICY
Employees will follow appropriate security procedures when using mobile devices, when working at home with computing equipment, and when using personally-owned computing devices.

AUDIENCE
All Staff

REFERENCE
45 CFR 164.312(a)(2)(iv) Encryption and decryption
ISO 27002 11.7 Mobile computing and teleworking
EHNAC II.A.5

PROCEDURES
1) **Safeguards for laptops, tablets and other mobile devices**. Employees who use ABACUS provided laptop computers, tablets, smartphones, or other portable computing devices must follow appropriate security procedures:
   A) Full disk encryption must be employed on any devices which store PHI.
   B) Security updates for anti-virus, operating system, and application software must be promptly applied.
   C) When traveling via automobile, mobile computing devices may be left unattended only in a locked automobile trunk.
   D) When using public Wi-Fi networks to access company or client systems, including email, a VPN connection must be used. Employees shall use company equipment with public Wi-Fi networks only after receiving security training from the Security Officer and/or IT Staff.
2) **Lost devices**. Employees must immediately report the loss or theft of any company-owned devices to their supervisor and/or the Security Officer. Any supervisor receiving a report of a lost or stolen device shall immediately notify the Security Officer who shall treat this as a potential security incident and use the procedures in Policy 3090 Security Incident Response and Reporting.
3) **Teleworking.** The Security Officer shall review and approve teleworking arrangements by employees and independent contractors. The review shall evaluate:
   A) The existing physical security of the teleworking site
   B) The proposed physical teleworking environment, including the threat of access by family and visitors to the teleworking equipment
   C) The use of home networks and requirements or restrictions on the configuration of wireless network services
   D) Anti-virus protection, firewall requirements, and software patching procedures

   On a case-by-case basis, the Security Officer will issue guidelines for the teleworking arrangement to include:
   A) Classifications of information that the teleworker is authorized to store on his/her home system
   B) Physical security for the site
   C) Rules and guidance on family and visitor access to equipment and information
   D) The procedures for back-up and business continuity
   E) Procedures for appropriate security including anti-virus, firewall and software patching
4) **Employee-owned computing devices are prohibited**.

1080 Duty to Report Violations and Security Incidents

POLICY
Confidentiality of patient information, and the computer security required to protect PHI is taken very seriously at ABACUS. Employees are required to follow all rules in these policies. Any employee who becomes aware of a violation of these HIPAA policies, or becomes aware of a security incident, is obligated to immediately report this violation. Violations will be investigated and appropriate action will be taken.

AUDIENCE
All Staff

REFERENCES:
45 CFR 164.530(e)(1) –Sanctions

PROCEDURES:
1) Any employee observing a violation of any of the HIPAA Policies is to report the violation to the Security Officer and/or his/her supervisor. Failure to report a violation is in itself a disciplinable offense.
2) Any employee who becomes aware of a potential security incident shall immediately report the information to his/her supervisor and/or the Security Officer.
3) Supervisors receiving reports of potential violations and/or security incidents shall immediately report the matter to the Security Officer.
4) Upon learning of an incident, the Security Officer shall follow procedures in Policy 3090 Security Incident Response and Reporting.
5) For violations of these policies, the Security Officer will refer the incident to Executive Management who in turn will follow procedures in Policy 3080 Employee Sanctions.
6) A written incident report, including any disciplinary action taken, other corrective action, and recommended enhancements to procedures to prevent future similar incidents, will be written by the Security Officer. It will be filed in the HIPAA Compliance file.

POLICIES FOR ADMINISTRATIVE MANAGEMENT

1300 Application Certification and Notifications

POLICY
ABACUS application software will maintain compliance with all applicable CFR standards and requirements. ABACUS will maintain a current 3rd party certification that verifies this compliance and provide this certification to any customers, business associates, or authorized 3rd parties as requested. In the event that the application is found to be non-compliant with any standard, customers shall be immediately notified to cease using the application until an updated patch can be applied to remedy the compliance issue.

AUDIENCE
Management

REFERENCES:
EHNAC IX.A.4, IX.A.5, IX.A.8, IX.A.9, IX.A.10

PROCEDURES:

1) **Maintenance of certification.** ABACUS will obtain and maintain a compliance certification of its company policies and software applications by an accredited 3rd party.
   a. Records from this audit and certification shall be maintained for 2 years.
   b. This certification shall be made available to customers via the company website, and by request to business associates, representatives of the Department of Health and Human Services, and other 3rd parties authorized by the management.
2) **Notifications of not meeting requirements.**
   a. If ABACUS becomes aware that its software application does not meet one of the requirements of § 1311, except as provided in § 1311.300(h) and (i), it will immediately notify the Administration within one business day via email of the adverse report.
   b. ABACUS will also notify all of its customers using the application to immediately cease using the application…
      (a) to create, sign, transmit, or process electronic controlled substance or…
      (b) to cease using the application to process prescriptions that require additional information that is not properly imported, stored, and displayed in the application…
      until a patch fixing the issue can be applied to the software.
   c. This notification, as well as a copy of the adverse report, will be sent out within 5 business days via email to all customers who have provided an email contact and via 1st class mail to all other customers.
   d. The form letter text in Appendix F can be used to provide this notification by selecting the appropriate form that corresponds to the nature of the noncompliance. Form A is used for 2.b.a and Form B is used for 2.b.b.
3) **Delivering updates correcting noncompliance.**
   a. ABACUS will update its software applications to correct any non-compliance issues and push the patch update to its customers as soon as possible after learning that the software application does not meet any of the § 1311 requirements.
   b. ABACUS will send notification its customers with the update that installation of this update is necessary to bring the software application into compliance so that it can be used again. This notification will be sent via email to all customers who have provided an email contact and via 1st class mail to all other customers.
   c. The form letter text in Appendix F can be used to provide this notification.

1400 Marketing Standards

POLICY
ABACUS will market its products and services to the extent that the company can deliver on all advertised claims.

AUDIENCE
Management

REFERENCES:
EHNAC IV.A.1, IV.A.2

PROCEDURES:
1) Marketing will be created to highlight the strengths of products and services offered
   A) All advertising and marketing claims will be written in good faith to honestly portray the experience of the customer
   B) Any remarketing that is done will adhere to this same standard detailed in (A).

1500 Employee/Contractor Recruiting and Termination

POLICY
Employee backgrounds will be checked prior to hiring and individuals deemed to be high risk will not be hired. Upon termination of employment and/or an independent contractor arrangement, procedures will be followed to disable employee access to company and/or client information systems.

AUDIENCE
Management

REFERENCES:
45 CFR 164.308(a)(3)(ii)(B) –Workforce clearance procedure
45 CFR 164.308(a)(3)(ii)(C) – Termination procedures
EHNAC VI.B.7

PROCEDURES:
1) **Background Standards**. The human resource department will establish standards for acceptable background check results based on the sensitivity of the position. The following checks will be considered:
   A) Reference checks to verify prior employment
   B) Criminal background check – local
   C) Criminal background check – nationwide
   D) Credit reporting (to identify individuals with high debts who may be at risk of compromising company confidential information because of financial stress)
2) **Background checks**. Based on the standards selected, the human resource department will conduct the appropriate background check for hiring decisions. Background checks may also be employed as part of the clearance process for independent contractors. Decisions based on this information will be made on a case by case basis. Results of background checks will be maintained in the employee's personnel file.
3) **HIPAA Training**. Newly hired employees will be given HIPAA training appropriate to their roles and responsibilities in the company promptly after beginning employment. A record of the date of training will be maintained in the employee's personnel file. Training and recordkeeping will be done in coordination with the Security Officer.
4) **Access to Company Systems**. Access to company systems will be handled as detailed in Policy 3075 Employee System Access.
5) **Termination procedures**. Upon termination of an employee and/or independent contractor, the termination procedure will include the following steps, to be completed on the day of termination:
   A) Keys to company facilities will be returned
   B) Any company-owned computing equipment or other property will be returned
   C) Email accounts assigned to the individual will be re-directed to another employee and the password will be changed
   D) All computer accounts used by the individual will be disabled. (See Policy 2040 Passwords and Encryption Keys.)

   Records of these termination steps will be maintained in the employee's personnel file and/or independent contractor file.

1600 Disclosures Required by Law

POLICY
Rare circumstances, such as a court order, government audits or certain national security matters, may require the release of PHI, which will be done according to these procedures.

AUDIENCE
HIPAA Privacy Officer

AUTHORITY
45 CFR § 164.502(a)(3)
45 CFR 164.502(a)(4)

PROCEDURES
1) Requests for uncommon disclosures, such as court orders or government audits, shall be referred to the CEO for handling and management.
2) **Legal Review of Requests.** The company may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. For all requests, legal counsel will be consulted to provide guidance.
3) **Recordkeeping**. For all of the disclosures authorized below, the employee handling the disclosure will document the details of the disclosure on the Disclosure Log. Copies of all paperwork requesting the disclosure and copies of the records sent will be maintained if practical.

1800 Human Resource Management

POLICY
ABACUS will maintain a high level of performance from its staff and will engage in training, development, and evaluation of employees.

AUDIENCE
Management

REFERENCE
EHNAC V.B.1, V.B.2, V.B.3

PROCEDURES
1) Upon hiring, all new employees will be trained in the HIPAA guidelines and policies as detailed in Policy 1500 Employee/Contractor Recruiting and Termination.
2) Management will designate employees within each department who will train new members of the department in the skills and knowledge relevant their roles as they begin their employment.
3) Abacus is committed to the continuing education of staff. Employees are encouraged to identify and attend professional development and continuing education opportunities appropriate to their roles in the company. On an annual basis, as part of the performance planning process, a professional development/education plan will be prepared for each employee. This development plan will include Abacus in-service training and/or outside training. On a case-by-case basis, management will reimburse reasonable expenses incurred from these activities.
4) Management will develop criteria for evaluating all employees annually. Employees will receive a written report of their evaluation within one week of its completion and a copy of the evaluation will be stored in the HR records. These evaluations will include, but not be limited to, performance, professionalism, and dedication to continuing education.

1850 Mitigation

POLICY
ABACUS will mitigate, to the extent reasonable and practical, harm that is done to patients as a result of our violations of these HIPAA policies

AUDIENCE
HIPAA Privacy Officer

AUTHORITY
164.530(f) Mitigation
EHNAC VI.B.16

PROCEDURES
1) **Assessment.** The HIPAA Privacy Officer shall investigate and access the impact of any violations of these policies on ABACUS's clients and/or their customers. The assessment should evaluate any type of harm, including financial, reputation, inconvenience, embarrassment or any other type of harm.

2) **Mitigation.** The HIPAA Privacy Officer shall determine some action, within the power of the company, which can mitigate that harm. If it is within the scope of their authority, the HIPAA Privacy Officer shall take steps. If it is beyond the scope of the Privacy Officer's authority or budget, the Privacy Officer shall take the proposed action to the CEO who shall make the final decision about mitigation steps.

1900 Sanctions for Staff Violations of Privacy/Security Policies

POLICY
Confidentiality of PHI is taken very seriously at ABACUS. Employees are prohibited from improperly using or disclosing confidential patient information, intentionally or unintentionally. Employees are further expected to comply with all policies involving HIPAA mandated computer security. Employees who violate these policies will be subject to sanctions as detailed in this policy.

AUDIENCE
All Staff

AUTHORITY
45 CFR 164.530(e) Sanctions (Privacy rule)
45 CFR 164.308(a)(1)(ii)(C) Sanctions Policy (Security rule)
EHNAC VI.B.2

PROCEDURES
1) Any staff member observing a Privacy or Security Violation is to report the violation to his/her supervisor. Failure to report a Privacy Violation is in itself a disciplinable offense.
2) The supervisor should refer the incident to the Privacy Officer. The Privacy Officer shall, in conjunction with the HIPAA Security Officer and other management personnel as he/she deems appropriate, investigate the matter through discussing the matter with staff, patients, or others, and/or review of computer or paper audit trails.
3) The Privacy Officer or HIPAA Security Officer, in conjunction with the employee's supervisor, and the Office Manager will evaluate the severity of the violation, the degree of harm caused, the frequency of past violations, and the employee's overall record of performance with ABACUS. Based on this evaluation, one or more of the following sanctions will be applied:
   A) Coaching on allowed uses and disclosures
   B) Formal warning
   C) Formal reprimand
   D) Requirement to review policies and procedures
   E) Suspension from 1 to 30 days without pay
   F) Termination
4) For grievous violations, such as uses or disclosures of PHI for financial gain or made with malicious intent, immediate termination may be appropriate. For other violations, because of the wide variety of types of violation possible and circumstances involved, considerable flexibility in administering sanctions is given to management.
5) The Privacy Officer, in conjunction with other members of the management staff as he/she deems appropriate, shall take action to mitigate the harmful effects of the Privacy Violation, if this is reasonable and possible.
6) A written incident report will be written by the Supervisor/Privacy Officer and filed in the Privacy Officer's Privacy Violations file, in the employee's personnel file, and one will be given to the employee.

POLICIES FOR TECHNICAL STAFF

2000 Technical Support Procedures

POLICY

Employees will maintain confidentiality and use appropriate security procedures during technical support activities. The only access to PHI is for customer support as specified in 1020 Minimum Necessary Policy. The only access to customer systems permitted is with the supervision of that customer while providing support.

AUDIENCE

Technical Services / Customer Service Staff

REFERENCE

EHNAC II.A.5, III.B.1, III.B.2, III.B.3, III.B.4, VI.B.5, VI.B.8, VI.B.11, VI.B.18, VI.B.25, VI.C.10, VI.D.5

PROCEDURES

1) **Technical Support Infrastructure and Protocols**. ABACUS will utilize only support tools which allow secure methods for customer support. The Security Officer will review any support tools for compliance with HIPAA standards, develop customer support protocols for using those tools, and train customer service personnel on those protocols. The review of tools will include
   A) Remote Management & Monitoring Software
   B) Help Desk Software
   C) Remote Login Software/Services
2) **Client Verification**. For support inquiries, ABACUS will verify the identity of the caller for support calls. Voice recognition is an appropriate method of verification for individuals known to the ABACUS employee. Alternate methods are to request details from the caller regarding information that would be known only to an employee of the customer organization. Client verification is ESSENTIAL for any customer password reset requests. Before providing any password reset support, the employee will call the customer back using the number on record and speak only with a person on the authorized user list which is maintained for all customers.
3) **Customer Passwords.** The following procedures will be used for customer passwords:
   A) Staff must never know customer passwords and/or other logon information.
   B) Password resets. ABACUS software allows for support staff to remotely reset a customer password without the support staff knowing the password or being involved in the selection of a new password. This is only do be done in with proper client verification as detailed above.
   C) Any access to a customer system during a support session will be done with the supervision of the customer.
   D) It is possible that an employee incidentally learns a customer password during a support session. In this case, once support is complete, the customer shall be instructed to reset their password.
4) **Screensharing with Customers**. The HIPAA Security Officer must approve all screensharing technology to ensure that it maintains HIPAA standards of security for data in transit. Support personnel must utilize peer-to-peer connection with the customer.
5) **HIPAA Compliant Communications with Customers**.
   A) Customers will be instructed on HIPAA compliant methods of obtaining customer support, which is to redact PHI whenever possible. Customers will be instructed to never use email to send PHI, and not to enter or attach PHI to a support ticket.
   B) ePHI Received from Customers. In the event that a customer violates company support policies and sends PHI via email
      a) The customer should be immediately notified of the violation of support terms
      b) The ePHI should be destroyed using procedures using procedures below.
6) **Destruction of PHI received**. If hardcopy or ePHI is received by Abacus Technical Support, it must be immediately destroyed:
   A) Hardcopy. Screenshots, faxes and/other hardcopy with PHI shall be immediately redacted to remove PHI. When the need for the hardcopy is complete, the original must be destroyed by shredding.

B) Electronic. Any electronic PHI (e.g. a screenshot saved) must be immediately deleted. Computers in the customer service and tech support departments must be equipped with secure deletion software to wipe any deleted portions of the hard disk, per specifications in Policy 3060 Technical Safeguards.

7) **Transportation of Client Equipment/Media**. ABACUS staff will employ the following safeguards whenever moving client equipment and/or media containing ePHI:
   A) Servers and other equipment in production use, with ePHI or other client applications and data, will be backed up prior to any movement.
   B) Equipment with ePHI in internal storage and/or any media with client ePHI will be securely transported. If possible, stops will be avoided while transporting equipment and/or media. If stops cannot be avoided, the equipment and/or media will be kept in a locked trunk or other storage area, out of sight and all vehicle doors will be kept locked when not in the car.
8) **Customer Support Ticketing System.** ABACUS will utilize a ticketing system for providing customer support.
   A) When a customer calls for support and an employee answers the call, the ABACUS will record the customer's name, contact information, and description of the problem to create a support ticket in the system.
   B) Web access for customers to send a support request is available from the ABACUS web page. On the support ticket creation page, customers are instructed not to send ePHI in their descriptions of problems. They are unable to send attachments through this system.
   C) The customer service department will designate staff to listen to any voicemails that are left by customers requesting support. The request from the voicemail will be logged into the ticketing system and the time at which the call is placed will be logged.
   D) Customer Service and Technical Support staff will either take the call directly or call the customer back using the number from the support ticket. At this point, the employee is responsible to create a plan of action for the customer to service the request. Simple request may be resolved immediately with a single plan of action from a single employee. More complicated support requests may require multiple plans of action from multiple departments or levels within a single department.
   E) If a customer support request cannot be addressed solely by one of the departments or is determined to be highly complicated, that department is to involve management. The department and management will collaborate to devise a plan of action and will engage the customer in that plan of action as appropriate.
9) **Remote Customer Support.** When connected to a customers' computer, via ShowMyPC, and a screen shot is printed, needed to diagnose an issue or question but, containing PHI. All PHI not needed to solve the issue will be redacted. If an issue requires programming to resolve the issue, then the issue will be escalated in the following steps:
   A) STEP 1: The programmer will be called to view the issue while connected with the Customer (no PHI is to be collected, only viewed).
   B) STEP 2: If the only way to resolve the issue is to print out a screen shot, then non relevant PHI will be redacted. An example of non-relevant PHI would be, if an issue exist with the On-Hand quantity of a medication, but the print out contains patient information, to solve an On-Hand calculation issue the patient information is not required, so that information needs to be redacted as a company policy.
   C) STEP 3: In the extreme chance that the issue cannot be found by the above steps and the only way to reproduce or solve the issue is with the customers data and the database has been requested by the programmer. Special steps are to be taken to ensure that the customer understand what we are doing and that we get permission from the customer to get a copy of the data. Only the supervisor of Technical Support (TS), or appointee if he is absent, is authorized to download the customer database using the following procedure:
      a) While connected via ShowMyPC, the database will be downloaded to the designated USB using ShowMyPC File Transfer Service.
      b) Once downloaded, the USB will be taken to the programming department where the USB containing the database will be examine to resolve the issue.
      c) Once the issue has been resolved, all data from the USB and the entire USB will be wipe using Eraser and given back to the TS supervisor. The TS supervisor will verify that the USB has been wiped.

   A Ticket will be created detailing all the steps taken and conversations with the customer. Under no circumstance is PHI to be stored on any computer, on paper or any other media, moved, copied, manipulated or handled in an unsecured way or to any unsecured place that does not confirm to company policy. Under no circumstance is PHI to be stored on any computer or on paper or any other media after the issue has been resolved. Once the issue has been resolved, PHI data MUST be erased in a secure way or shredded.

2005 Secure Network Configuration for Client Networks

POLICY
Technical staff utilize appropriate secure network configuration principles when configuring and maintaining client networks.

AUDIENCE
Technical Staff

REFERENCES
Microsoft SCM Microsoft Security Compliance Manager
NIST National Vulnerability Database National Checklist Program Repository
CIS Secure Configuration Benchmarks Center for Internet Security Secure Configuration Benchmarks

PROCEDURES
1) **Applicability**. Services offered to clients will vary based on contract with client. This policy is applicable to clients who request secure network configuration, for example, for compliance with HIPAA Security standards.
2) **Scope for Policy**. ABACUS will employ the secure configuration for any of the following IT technology infrastructure managed for clients:
   A) Computer Servers
   B) Workstations
   C) Hypervisors
   D) Application Software, including browsers, Microsoft Office, etc.
   E) Routers and switches
   F) Databases
   G) Telephone Systems
   H) Peripherals
3) **Hardening Process**. All components will undergo the following hardening process:
   A) Install system
   B) Remove unnecessary software
   C) Disable or remove unnecessary usernames, especially any default administrator accounts
   D) Disable or remove unnecessary services. If system-specific, reputable configuration guides are available these should be used. For example:
      a) Microsoft's Security Baselines
      b) NIST Security Configuration Checklists
      c) Center for Internet Security's CIS Benchmarks
   E) Enable logging
   F) Patch system
   G) Install anti-virus and anti-malware
   H) Configure firewall. If the system can run its own firewall then suitable rules should be configured on the firewall to close all ports not required for production use
4) **Standard Images**. Standard images, created using the hardening principles above, may be used for workstation OS and other equipment.
5) **Passwords**. Systems will be staged without passwords. Passwords will be assigned by end-users.

2010 Software Development Procedures

POLICY
Technical staff will adhere to the company software development procedures during all phases of the software life cycle.

AUDIENCE
Technical Staff

REFERENCES
OWASP Top 10 Open Web Application Security Project Top 10 2013
CWE SANS Top 25 Most Dangerous Software Errors
PCI DSS 2.0 Payment Card Industry Data Security Standard Version 2.0
ISO 27001/27002 International Organization for Standardization - Information technology - Security techniques - Code of practice for information security management, Second edition 2013-10-01
EHNAC III.A.1

PROCEDURES
1) **Project Approval**. ABACUS will utilize a management process to review and approve all projects prior to initiation.
2) **Design Standards**. Security will be an integral part of software beginning with the initial system design. Applications will be designed so that the target customer is likely to find the application meeting or exceeding HIPAA compliance standards based on their environment. These standards should include at a minimum:
   A) Require a unique user ID for each user. This applies to administrative users as well as end users. Audit logging should be based on this unique user ID to allow tracing of activities to the responsible individuals.
   B) Secure authentication per ISO 27002 9.4.2. The system log-on procedure should:
      a) Not display system or application identifiers until the log-on process has been successfully completed;
      b) Validate log-on information only on completion of all input data, and if an error condition arises, not indicate which part of the data is correct or incorrect
      c) Limit the number of unsuccessful log-on attempts
   C) Secure communications. Use secure communications such as TLS.
   D) Password management per ISO 27002 9.4.3 standards
      a) Enforce the use of individual user IDs and passwords
      b) Allow users to select and change their own passwords and include a confirmation procedure to check for input errors
      c) Enforce appropriate password complexity based on standards set by the customer
      d) Enforce password changes on a frequency determined by the customer
      e) Maintain a record of previous user passwords and prevent re-use
      f) Not display passwords on the screen when being entered
      g) Store password files separately from application system data
      h) Store and transmit passwords in protected (e.g. encrypted or hashed) form.
   E) Session time-out. The time-out time window should be configurable by customer-administrator for all users of the customer.
   F) Audit logging of end-user actions, including records viewed, added/modified and deleted. In addition, flexible reporting/query of audit logs shall be provided.
   G) Granular access control capabilities, configurable by the customer-administrator, should be included.
   H) Proper use of cryptographic techniques, including password handling.
3) **Secure Programming Techniques**. The Security Officer, based on the technologies/platforms used by the company, will identify the secure programming techniques that will be used by company personnel. Industry frameworks/initiatives may be considered, such as SANS/CWE Top 25 Most Dangerous Software Errors, Microsoft Security Development Lifecycle, SAFECode and OWASP or others. The Security Officer will ensure that all programmers receive appropriate training and/or that the programmers demonstrate competency in these programming standards.

4) **Testing and Quality Assurance**. The quality assurance program will incorporate testing methodologies which include:
   A) To the extent possible, a second individual (not the author) reviews all code additions/changes made
   B) Functionality testing has been conducted to verify both accurate processing and that changes do not adversely affect the security of the system
   C) Production data are not used for testing or development
5) **Software Release Procedures**. The software release process shall ensure that:
   A) Separate development/test and production environments are used
   B) Separation of duties exists between development/test and production environments
   C) Test data and accounts, and debugging code, are removed prior to final release
   D) Documentation of changes is made, including an audit log of all updates to operational program libraries. Documentation shall include details of functional changes, to demonstrate compliance with applicable federal and state regulations
   E) Previous version(s) of application software is/are retained, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure for roll-back

2020 Source Code Management

POLICY
The Security Officer will implement procedures for the use of a source code management system. Technical staff will use source code control system for all source code development and maintenance work.

AUDIENCE
Technical Staff

REFERENCE
ISO 27002 12.4.3

PROCEDURES
Security Officer Responsibilities:
1) **Source Code Management system**. Select and implement a source code management approach appropriate to the needs of the organization.
2) **Access Control**. Limit access to source code based on a need to know.
3) **Source Code Backup**. Ensure that a secure backup is made of the source code.
4) **Assurances from 3rd Parties**. Ensure that satisfactory assurances of confidentiality and performance are obtained from any 3rd parties involved with hosting or maintaining a source code management system.

2030 Intellectual Property

POLICY
All source code is proprietary property of the company and must be protected. Employees and contractors will agree to cooperate with these policies as a condition of employment/engagement.

AUDIENCE
Technical Staff

PROCEDURES
1) **Intellectual Property**. All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected.
2) **Safeguards**. Safeguards employed to protect the company's intellectual property include:
   A) Non-Disclosure Agreements. All employees and independent contractors with access to company source code and documentation will be required to sign a non-disclosure agreement approved by the company CEO.
3) **Cooperation with Patent process**. Employees agree to participate with all actions requested by ABACUS to obtain patents, including executing any legal documents necessary. Employees further agree that all patents obtained will be owned exclusively by the company, and that employee's regular compensation package represents full and complete payment for services rendered.

2040 Authentication, Passwords and Encryption Keys

POLICY
The Security Officer will maintain control over the password and encryption key management process. Security procedures will be established for various types of passwords and encryption keys. The security of these credentials for both internal systems and customer systems will be carefully managed.

AUDIENCE
Technical Staff

REFERENCE
EHNAC VI.B.14, VI.D.2

PROCEDURES
2) The Security Officer will manage account assignment and password procedures for the various account types that utilize passwords. The Security Officer will develop procedures for management of all of these account types:

    A) Internal Accounts
        a) Employee Workstation/Network Domain accounts
        b) Employee Email accounts
        c) Company-owned Accounts
            (i) Domain Name Registrar account
            (ii) Hosting Company Control Panel account
            (iii) Cloud vendor accounts
            (iv) Other Service Providers
        d) Technical Resource Accounts
            (i) Hypervisers
            (ii) Servers
            (iii) DBMS
            (iv) Firewalls
            (v) Routers and Wireless Access Points
    B) Customer Systems
        a) Remote Access Tools
        b) Company subscriptions
        c) Personal accounts/subscriptions

3) **Multi-factor Authentication based on Risk Analysis**. When risk analysis identifies a resource as a high value target, multi-factor authentication will be utilized.
4) **One Account per Individual Rule**. As a general rule, every individual will have their own account and a confidential password. When this is possible, employees are prohibited from divulging their passwords.
5) **Exceptions where Shared Accounts are Allowed**. In some instances, technical resources (e.g. firewalls) and various vendors (e.g. a Domain Name Registrar) may offer only a single administrative account, in which case password sharing among staff members may be required. In such cases, passwords may be shared. The Security Officer will maintain a record of all such shared accounts and the employees who have access to the password.
6) **Password Security – General Rules**. Password security procedures will vary based on account type, however, as a general rule, the following security guidelines apply:
    A) Each employee is assigned a unique User ID and Password for their workstation, network account, and any management platforms (RMMs, etc.) Inappropriate use of systems attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution. Employees must keep their passwords secure and confidential.

B) Passwords should be at least 8 characters long and include at least 1 number, upper case letter and lower-case letter. The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in any way, as in a birth date, spouse, pet name, or anything which can be easily guessed. Pass phrases consisting of three or more words strung together are acceptable. For critical resources, including firewalls and servers, a stronger password may be required.
C) Passwords should be maintained only in a company-approved password vault or memorized. Written passwords must not be kept written in the vicinity of a workstation.
D) Users are required to change all passwords at least every 12 months.
E) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.
F) When changing passwords, previously used passwords should not be recycled.
G) Separate passwords should be used for each account.
H) Default passwords supplied by a vendor must always be changed.
I) When specifying answers to vendor security questions (for use with password reset requests) it is best to select questions whose answers cannot be easily discovered.

7) **Encryption Keys**. Various types of encryption keys exist. These include:
A) SSL certificate keys
B) Mobile device encryption keys
C) DBMS encryption keys
D) Backup media encryption keys

8) **Key Management**. The Security Officer shall manage key procurement/assignment, and changes in a manner appropriate to the number of keys and the security risks involved. For clients implementing encryption, technical support procedures will be developed for appropriate management of support requests.

9) **Password Vault**. The Security Officer may select, implement and maintain a utility for maintaining login credentials and passwords for important accounts and for encryption keys. Appropriate backup copies of the vault shall be made. Provisions for business continuity, in the event that the Security Officer is unavailable, shall provide dual-access of this password vault by the CEO or other individual specified by the CEO, per Policy 3010 Disaster Recovery Plan and Emergency Mode Operations.

10) **Access Control**. The Security Officer, shall provide employee and contractor access to passwords, encryption keys and systems in conformance with Policy 1020 Minimum Necessary and Policy 3075 Employee System Access. .

11) **Automatic Logoff.** Workstations connected to a domain will be configured for lockout after 5 incorrect login attempts.

2050 Operations Management

POLICY
The Security Officer will rigorously manage essential operational systems to protect the productivity and security of the staff and company.

AUDIENCE
HIPAA Security Officer

REFERENCE
EHNAC III.D.3, III.D.4, VI.B.3

PROCEDURES
1) **System Review.** The Security Officer will ensure that system logs are kept as detailed in 3025 Audit Control and Activity Review
2) **Bandwidth Monitoring**. The security officer will monitor the bandwidth capacity report on a daily basis and take corrective action if necessary.
3) **Audit Log Monitoring**. The firewall will be configured to notify the security officer if there is any intrusion attempt or other external attack on the network.
4) **Monthly Operations Review**. Security Officer will maintain all logs specified in this policy for a period of 3 years. The security officer will review all logs and activity, including bandwidth reports, firewall logs, and security incident reports, on a monthly basis to check for security concerns or unusual activity. Any findings of this nature will be documented. These logs will be reviewed again during the annual risk analysis.

2060 Change Management

POLICY
The Security Officer will orchestrate a rigorous change management process to protect the operations of the company, ensuring high productivity of staff at all times.

AUDIENCE
HIPAA Security Officer

REFERENCE
EHNAC III.E.1

PROCEDURES
1) **Scope of Change Management Process**. This process shall be used for all critical operational systems as identified in the security risk analysis.
2) **Change Management Process**. A formal change management process is used at ABACUS. The ticketing system is used for all infrastructure change requests. Infrastructure changes must be approved by either the President or Vice President. The President and/or Vice President will assess business risk prior to implementing any infrastructure changes.
3) **Fallback Procedures**. For any major change, fallback procedures are developed in advance, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events. The fallback procedures will include performing a backup of the system, prior to implementing the change, using the procedures detailed in Policy 3005 Data Backup.

POLICIES FOR EXECUTIVE MANAGEMENT & SECURITY OFFICER

2900 Security and Privacy Officer Appointment and HIPAA Documentation

POLICY
ABACUS shall appoint a single individual responsible to oversee computer security. This individual, the Security Officer, in addition to duties specified elsewhere, shall maintain the official compliance documentation for the HIPAA compliance. ABACUS shall appoint a single individual responsible to oversee privacy and breach notification, designated the Privacy Officer.

AUDIENCE
Management, HIPAA Privacy Officer, HIPAA Security Officer

REFERENCES
45 CFR 164.308(a)(2) Assigned security responsibility

REFERENCE
V.B.4, V.B.5, VI.B.4

PROCEDURES:
1) **Security Officer Appointment**. ABACUS shall designate an individual to be the Security Officer, who is responsible for overall compliance with HIPAA security regulations as well as terms of any HIPAA Business Associate agreements signed with clients. This appointment shall be documented in Appendix F.
2) **Privacy Officer Appointment.** ABACUS shall designate an individual to be the Privacy Officer, who is responsible for privacy and breach notification. This appointment is documented in Appendix F.
   A) In the event of a security incident and/or breach, the Privacy Officer will act according to the policies detailed in Policy 3090 Security Incident Response and Reporting and Policy 3035 Breach Reporting.
   B) The Privacy Officer will identify all legal or regulatory requirements relevant to the IT resources and operations of its organization and form policies to ensure compliance.
3) **HIPAA Mandated records**. The Security Officer shall maintain all HIPAA mandated records including the following:
   A) Written Risk Analysis Reports as detailed in Policy 3000 Security Management Process.
   B) Written Security Evaluations as detailed in Policy 3020 Periodic Security Evaluation
   C) Business Associate Contracts as detailed in Policy 3070 Business Associate Contracts
   D) Any sanctions that are applied as a result of non-compliance with HIPAA-mandated policies as detailed in Policy 3080 Sanction Policy.
   E) Incident Reports and other documentation specified by Policy 3090 Security Incident Response and Reporting and Policy 3035 Breach Reporting.
   F) Training records. Dates of HIPAA training shall be maintained in the personnel files of all staff and independent contractors. All members of staff who are responsible for HIPAA compliance, including protection of PHI, must have this designation documented in these records.
   G) Details for Addressable Implementation Specifications. For any of the HIPAA Implementation Specifications that are indicated "addressable", documentation will be maintained if this control is determined to be not applicable to ABACUS, why it is not applicable, and if it is handled in an alternate manner. This list is maintained in Appendix F.
   H) Policy and Procedures Audit Trail. A 6-year audit trail of HIPAA policies and procedures shall be maintained so that the policies can be identified at any point in time during the 6 year window.
   I) Compliance Notes. The Security Officer will maintain records of compliance activity including meeting notes, vendor contracts, internal audit activities.

3000 Security Management Process

POLICY
The Security Officer will orchestrate ABACUS's security management process.

AUDIENCE
Management, HIPAA Security Officer

REFERENCE
45 CFR 164.308(a)(1) Security management process
EHNAC III.C.1, VI.B.1, VI.F.4

PROCEDURES
1) The Security Officer will orchestrate the security management process. This will include:
   A) **Computer Security Risk Analysis**. A risk assessment will be conducted and updated as necessary. The Risk Assessment is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information kept on systems owned or managed by ABACUS. This Risk Analysis shall further identify risk related to employee access to PHI on client networks. The Computer Security Risk Analysis will be handled as follows:
      a) ABACUS will use the risk analysis methodology detailed in NIST SP 800-30 Revision 1 (September 2012)
      b) The risk assessment will guide the policy development and risk management process. Executive management will review the results of the risk analysis.
      c) The results of this assessment shall be documented and maintained for 6 years
      d) The Risk Assessment shall be updated on an annual basis, or more frequently if appropriate based on technical and environmental variables, product enhancements, infrastructure or other technological changes.
      e) The risk assessment shall be reviewed by the Security Officer, Privacy Officer, and company CEO; who will all give acknowledgement of this review.
   B) **Risk Management**. ABACUS shall manage the risks identified in the risk analysis:
      a) ABACUS shall articulate a risk threshold, that is, a dollar amount of risk that the company is willing to accept.
      b) Risks greater than this threshold should be either mitigated, that is the probability should be reduced, or transferred, either through contract or insurance
      c) The results of risk management decisions, and corrective action taken, including the timeframe for corrective action, shall be documented. Documentation shall be maintained for 6 years.
   C) **Manage IT Infrastructure, Create and Deploy Security Policies**. On an ongoing basis, implement and maintain the IT infrastructure, create Security Policies and Procedures, and deploy/update them. More specifically, he/she will
      a) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices
      b) Prepare recommendations for approval by ABACUS management including implementation of new and updated policies, acquisition of technical security measures, or physical security measures. ABACUS's executive officers shall have final authority on risk management decisions.
      c) Create policies and procedures necessary to mitigate security risks to the company and for compliance with regulatory requirements. Update these policies as often as necessary based on regulatory changes, infrastructure changes and/or environmental changes.
      d) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level so as to comply with HIPAA regulations.
      e) Train staff regarding compliance. Training shall be conducted that is appropriate to the staff person's job responsibilities and shall be conducted promptly after the individual's hiring.
      f) Monitor ABACUS's compliance with the information security policies, and take action as appropriate based on this monitoring

D) **Information System Inventory**. The Security Officer and/or Security Team shall maintain a correct and accurate inventory of the hardware, software and networking infrastructure.
   a) Content of Inventory:
      (i) Hardware inventory will document all servers, routers and other networking equipment, desktop computers, laptops, smartphones and other portable computing devices, external disk drives, and USB flash drives.
      (ii) Network infrastructure documentation will include network topology and all other information necessary to recreate the network in the event of a catastrophic event
      (iii) Software inventory will include all software installed on workstations, servers, and network gear.

3005 Data Backup

POLICY
The Security Officer will ensure that a robust data backup regimen is in place and operational at all times. The Security Officer shall personally ensure that the procedures below are consistently maintained.

AUDIENCE
HIPAA Security Officer

PROCEDURES
1) **Data Criticality Analysis**. A Data Criticality Analysis shall be performed and updated annually to support backup, data recovery and other contingency plan components. The backup regimen must be developed in a manner consistent with the data criticality.
2) **Multiple Backup Generations**. Backups should include as many generations as is practical to store. One backup per day is appropriate as well as any additional backups needed before changing/updating system software as detailed in Policy 2060 Change Management.
3) **Backup Software**. Appropriate backup software shall be maintained, with appropriate scripting. These scripts shall be reviewed and adjusted as appropriate whenever hardware or software upgrades are performed to ensure that appropriate data backup is maintained.
4) **Off-site storage**. Backup regimens for data determined by data criticality analysis to be "mission critical" or "important" should include an off-site backup, that is, in a separate facility from the one containing the physical hardware.
6) **Responsibility**. The Security Officer shall designate the employee with primary responsibility to personally handle the backup. In the event that he/she is absent from work, an alternate individual shall be responsible. All individuals responsible for this critical function should be trained and familiar with the backup design and the procedure for daily verification.
7) **Backup Media Security**. Backup media shall be maintained in a secure location, and the data must be encrypted.
8) **Testing and Plan Revision.** REVIEW AND UPDATE OF THE DATA BACKUP PLAN SHOULD BE CONDUCTED WITH ANY SIGNIFICANT UPDATE OF THE TECHNICAL ENVIRONMENT**.** On at least a quarterly basis, a trial restore shall be performed from the backup 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 shall be updated. The results of this process should be documented and maintained for 1 year.
9) **Data Recovery Plan.** The Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

3010 Disaster Recovery Plan and Emergency Mode Operation

POLICY
ABACUS personnel shall develop contingency plans to prepare for system failures, and for procedures for maintaining critical ABACUS operations in the event of system failure

AUDIENCE
HIPAA Security Officer

REFERENCE
NIST SP 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems
EHNAC VI.B.16, VI.C.2

PROCEDURES
1) **Preventative Measures**. The Security Officer shall, on an ongoing basis, evaluate the activities that are critical to ABACUS's operations and implement preventative measures to reduce the likelihood of system failure. These would include technical capabilities such as use of application servers distributed across multiple physical facilities, redundant internet connections, redundant storage technologies, backup power supplies, fire suppression systems, video monitoring and other physical security systems, database transaction logging and the like.
2) **Disaster Recovery Team**. If appropriate, the Security Officer shall establish a Disaster Recovery Team to assist in the preparation of contingency plans as well as to execute assigned tasks in the event of a disaster. The Security Officer shall direct this team and is responsible for all tasks identified in this policy.
3) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios should include, at a minimum, failure of one or more servers, data corruption of the database, catastrophic loss of the entire facility due to fire or other natural disaster, and the incapacitation/unavailability of the Security Officer. These scenarios shall be included in the written plan, and serve as the basis for the measures outlined below.
4) **System and Disaster Recovery Plan**. The Security Officer shall maintain a written system and disaster recovery plan, with detailed steps for each of the scenarios identified above.
5) **Plan Testing**. The Security Officer shall periodically test the disaster recovery plan above to verify the adequacy of the plan and security measures. The results of tests shall be documented.

3015 Facility Security and Access Control

POLICY
ABACUS shall ensure that all facilities housing computing equipment employ appropriate physical security and access control measures.

AUDIENCE
HIPAA Security Officer

REFERENCE
45 CFR 164.310(a)(1) Facility Access Controls
EHNAC VI.C.1, VI.C.3, VI.C.4

PROCEDURES
1) **Physical Security of Company Facilities**. Any company facilities, and facilities of subcontractors, shall maintain a written physical security plan designed to protect IT assets which are used to deliver client support services. These security plans are detailed in Appendix D – Facility Security Plans.

3020 Periodic Security Evaluation

POLICY
The Security Officer shall conduct periodic technical evaluations of ABACUS's physical, technical and administrative security measures. The frequency will be determined based on regulatory, environmental or operational changes affecting the security of electronic protected health information and/or compliance with regulatory standards.

AUDIENCE
HIPAA Security Officer

REFERENCE
45 CFR 164.308(a)(8) Evaluation
EHNAC VI.B.19

PROCEDURES
1) The Security Officer will evaluate the security measures employed by ABACUS. These evaluations will include:
   A) Quarterly external vulnerability scans for externally-facing IP addresses for company networks and hosted systems.
   B) Annual penetration testing for critical networks, performed by a qualified third party.
   C) Annual review and update of policies and procedures for ongoing regulatory compliance, contractual compliance and compliance with accreditation requirements.
   D) Other evaluations may be conducted on an as-needed basis at the discretion of the HIPAA Security Officer.
2) Continuous Improvement. The Security Officer shall use a continuous improvement process to improve security and compliance based on the results of these evaluations.
3) The results of the evaluations, and improvement activities, will be documented, and documentation shall be retained for 6 years.

3025 Audit Control and Activity Review

POLICY
System capabilities for maintaining audit trails of system use may, at the discretion of the Security Officer, be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews may be conducted to identify suspicious activity so that appropriate corrective action is possible.

AUDIENCE
HIPAA Security Officer

REFERENCE
EHNAC VI.D.5

PROCEDURES
1) **System Activity Logs**. Activity logs may be enabled at the following levels
   A) RMM. Remote Management and Monitoring Systems, shall be configured to enable audit logging.
   B) Operating Systems and Software. Audit policies should be set to log logon events, account management events, policy changes, and system events as appropriate based on best practices, consistent with OS and System Software configuration specifications detailed in Policy 3060 Technical Safeguards.
   C) Firewall Hardware and Software: Logs should be enabled to track inbound and outbound activity and configured based on best practices.
2) **Security on Logs**. Appropriate security features and passwords should be used at all levels above to permit log file access only by personnel authorized by the Security Officer.
3) **System Activity Review**. In a manner determined by the Security Officer, Management Platforms, Operating system, system software, and firewall logs should be regularly monitored to detect suspicious or unusual system activity, with corrective action taken as suspicious activity is identified. This responsibility may be delegated or contracted. The use of automated tools is preferred. Bandwidth logs and firewall logs will be monitored as detailed in Policy 2050 Operations Management
4) **Purge of Log files**. System log files which grow large may be purged under the direction of the Security Officer.

3030 Malicious Software Protection

POLICY
All company computer systems will be protected by virus and malicious software protection capabilities.

AUDIENCE
HIPAA Security Officer

REFERENCE
EHNAC VI.B.24

PROCEDURES
1) Servers used by Abacus are maintained with reputable and regularly updated anti-virus protection.
2) Computers used by employees and contractors for support and administrative purposes will be appropriately protected with anti-virus software which shall be regularly updated.
3) The Technical Services department is responsible for keeping anti-virus software up-to-date, as specified in Policy 1050 Computer Usage.
4) The HIPAA Security Officer shall conduct random audits to validate that anti-virus software is up-to-date.

3035 Breach Reporting

POLICY
ABACUS will investigate security incidents, determine if a security incident is a breach, and notify its clients regarding breaches of protected health information.

AUDIENCE
HIPAA Security Officer, HIPAA Privacy Officer

REFERENCE
45 CFR Part 164, Subpart D HIPAA Breach Notification Rule
EHNAC III.F.2, VI.B.21, VI.B.22,

PROCEDURES
1) Upon becoming aware of a privacy rule violation or security incident, the Security Officer and Privacy Officer shall take the following risk management steps:
   A) Establish a response team, including any contractor personnel and outside forensic consultants as appropriate.
   B) Take any steps necessary to preserve the data and evidence.
   C) Determine if the incident meets the definition of a breach. Follow this three-step procedure to determine if a breach occurred:
      i) Was there acquisition, access, use, or disclosure of PHI that violates the Privacy rule? If "no", there is no breach. Otherwise, proceed to the next step.
      ii) Does one of the statutory exceptions listed in the breach definition in Policy 1000 apply? If "yes", there is no breach. Otherwise, proceed to the next step.
      iii) Unless the incident is clearly a breach, the Team shall conduct a risk assessment. The risk assessment, per HIPAA regulations, shall consider at least the following factors:
         1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
         2. The unauthorized person who used the protected health information or to whom the disclosure was made;
         3. Whether the protected health information was actually acquired or viewed; and
         4. The extent to which the risk to the protected health information has been mitigated as detailed in 1850 Mitigation

   Legal counsel and other expert advice shall be obtained, if appropriate, for additional guidance. If the risk assessment demonstrates that there is a low probability that PHI has been compromised, then no breach has occurred and this process may stop. Otherwise, the Security Officer shall proceed with the steps that follow in the remainder of this policy. In either case, the results of this evaluation shall be documented and maintained for 6 years as detailed in Policy 2900 Security Officer Appointment and Duties.
2) **Breach Notification**. ABACUS's obligation is to notify customers of a breach; it is the customer's responsibility to notify the individual patients. Notification to customers must include information that the customer will need in order to make the prescribed notification to the patient.
   A) Timing of notification. The notification must be made within the time period prescribed in the Business Associate Agreements with customers.
   B) Content of Notification. For each client affected by the breach, the following information shall be provided:
      a) To the extent possible, the identification of each of the client's patients whose unsecured protected health information has been accessed, acquired, used or disclosed.
      b) A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known
      c) A description of the types of unsecured protected health information that were involved in the breach
      d) Any steps that individuals should take to protect themselves from potential harm resulting from the breach;

e) A brief description of what ABACUS is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches

Executive management approval must be obtained before sending the notification.

3) **Public Relations Strategy**. ABACUS shall develop and execute a public relations strategy to include a communications strategy with customers and the media. This step shall be executed concurrently with the step above.
4) **Law Enforcement Delay**. In the event a law enforcement official states to ABACUS that the notification to clients above would impede a criminal investigation or cause damage to national security, ABACUS shall
   A) If the statement is in writing and specifies the time for which a delay is required, delay notification to clients for the time period specified by the official, or
   B) If the statement was made orally, document the statement, including the identity of the official, and delay the notification, but no longer than 30 days from the date of the statement unless a written statement is submitted specifying further delay
5) **Documentation**. Documentation, including any notices provided, incident reports, meeting notes, especially those which document the date of the breach, shall be maintained for 6 years. For the legal purposes, including the timelines in policy, the date of breach discovery shall be the date that ABACUS should have become aware if it exercised reasonable diligence.

3040 Security Awareness Program

POLICY
ABACUS may conduct an ongoing security awareness program to train and refresh staff on ABACUS's security policies, to enhance their understanding of their role in providing security, and to alert them to new threats.

AUDIENCE
HIPAA Security Officer

REFERENCE
45 CFR 164.308(a)(5)(i) Security awareness and training
EHNAC VI.B.12, VI.B.13,

PROCEDURES
1) The Security officer will conduct initial security awareness training for all new employees, and to all employees and contractors upon implementation of these policies. Upon finishing the training, written record of the participation of each employee will be documented and maintained by the security officer and/or HR.
2) Quarterly security awareness reminders/updates will be provided to all employees via email and/or company server. The Security Officer shall develop a plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; evaluation and measurement techniques; and the frequency of training. Possible topics would include:
   A) Reinforcement of topics for the Security Training Program and Security Policies
   B) Information relating to current security exploits, vulnerabilities and threats
   C) Issues with new technologies and threats such as, ransomware, spear-phishing, and social engineering.
   D) Email and/or a Company Staff Meetings will be the primary delivery medium for this awareness program.

3050 Device and Media Disposal and Re-Use

POLICY
As detailed in 1020 Minimum Necessary Policy, ABACUS does not maintain any customer PHI. These procedures exist as best practice to safeguard confidential information. Electronic storage media and devices that contain client ePHI shall be cleaned of protected health information and other confidential information prior to disposal and/or re-use. The Security Officer shall determine any additional equipment owned by ABACUS which will be subject to the procedures below.

AUDIENCE
HIPAA Security Officer

REFERENCE
45 CFR 164.310(d) Device and Media Controls
EHNAC VI.C.8, VI.C.9

PROCEDURES
1) **Media Disposal Handled by Security Officer**. As specified in Policy 1050 Computer Usage, ABACUS employees are prohibited from storing Protected Health Information on removable media. In the event of a legitimate requirement to store data on a device such as a CD or USB drive, the employee must request permission and obtain special procedures from the Security Officer.
2) **Technical Guidance**. In accordance with instructions from the Secretary of HHS, technical guidance regarding media disposal should be obtained from NIST SP 800-88 *Guidelines for Media Sanitization*. ABACUS requires that at a minimum, data from electronic media should be "cleared", as defined in the referenced NIST documentation.
3) **Media Disposal and Re-use**. ABACUS preference for media disposal is to use a 3rd party contractor, and to obtain a Certificate of Destruction. Procedures vary based on type of storage media:
   A) **CDs, DVDs and Tapes**: CDs, DVDs and Tapes should be physically destroyed by a service who will issue a certificate of destruction.
   B) **Hard Drives and floppy disks**. Hard drives and floppy disks should be reformatted prior to disposal or re-use.
   C) **Other Media**. See NIST SP 800-88 for disposal/recycling methods for other media.
   D) **Notes**. Photocopiers, printers and other office equipment may include media subject to this provision!
4) **Records.** Records of Media disposal should be maintained for 6 years. The following records should be maintained:
   A) Item Description
   B) Make/Model
   C) Serial number(s) / Property Number(s)
   D) Backup Made of Information (Yes/No)
   E) If Yes, location of backup
   F) Item Disposition (Clear/Purge/Destroy)
      a) Date Conducted:
      b) Conducted by
      c) Phone #
      d) Validated By
      e) Phone #
   G) Sanitization Method used
   H) Final disposition of media (Disposed/Reused Internally/Reused Externally/Returned to Manufacturer /Other). Maintain Certificate of Destruction for 3rd party destruction.

3060 Technical Safeguards

POLICY
Technical Safeguards will be employed on systems used for Abacus operations, including those which host any RMS and from which employees will access client networks. These safeguards will be used to ensure that any systems that access client networks are free of malicious software so as not to compromise the security of client networks.

AUDIENCE
HIPAA Security Officer

REFERENCE
EHNAC II.A.5, II.A.6, III.C.1, III.D.7, III.D.9, VI.B.8, VI.B.23

PROCEDURES
1) The internal network environment for ABACUS's RMS shall be secured using the following controls:
   A) **Firewalls.** Hardware and/or software firewalls shall be employed to protect against network intrusions. These should be configured to prohibit all traffic, except for traffic explicitly identified as necessary for required functionality. The firewall should provide minimum information to unauthorized users. Other appropriate security features such as intrusion detection, reputation-based blacklisting, deep packet inspection, and other capabilities should be enabled if available.
   B) **Software Patching**. Operating system, network gear, and other system software (e.g. DBMS) shall be patched on a timely basis:
      a) Server operating systems, other server system software, and network gear shall be monitored no less frequently than weekly for vulnerabilities. Critical patches should be made as soon as possible, with routine patches applied monthly, or more frequently, based on the vendor's patch release cycle.
      b) Workstations shall be configured to automatically patch. At a minimum, the following software will be kept patched: all Microsoft software, all browsers, all Adobe products and Java. Third-party tools to monitor patch level may be utilized. Technical Services shall be responsible for keeping workstations patched.
   C) **Device and Software Hardening**. Network gear, servers, workstations and system software (such as DBMS and application software) shall be hardened using the following principles:
      a) Default administrator accounts must be deleted, and new ones added, using strong passwords with a minimum of 8 characters including at least one each of upper case letters, lower case letters, digits and special characters.
      b) The minimum feature set required for necessary functionality should be installed and/or enabled.
      c) Appropriate audit logging must be enabled.
      d) Baseline security configurations should be employed for devices and software, including but not limited to, operating systems, web servers, DBMS software, browsers, and desktop productivity suites. Configurations published by NIST, the Defense Information Systems Agency, Center for Internet Security, or other authority cited in the National Checklist Program (NCP) should be consulted.
   D) **Licensure Compliance**. All software is installed under the direction of the HIPAA Security Officer to ensure licensure and updates.
   E) **Virtualization Software and environment**. Virtualization-enabling software, aka "hypervisors", if used, shall be secured as follows:
      a) unneeded capabilities shall be disabled to reduce potential attack vectors
      b) A strong password (see Policy 2040 Passwords and Encryption Keys).
      c) Synchronize the virtualized infrastructure to a trusted authoritative time server, and synchronize the times of all guest OS's
      d) Harden the host OS of the hypervisor by removing unneeded applications, and setting OS configuration per the vendor's security recommendations
      e) Use separate logon credentials for each virtual server
   F) **Transmission Security**. For data in motion, ABACUS product and service offerings shall be consistent with the Secretary of HHS's guidance on securing PHI. Valid encryption processes for data in motion are

those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. These include, as appropriate, standards described
   a) NIST 800-77, *Guide to IPsec VPNs*,
   b) NIST 800-113, *Guide to SSL VPNs*
   c) Other FIPS 140-2 Security Requirements for Cryptographic Modules

G) **Wireless Networks**. Wireless networks, if employed, will be implemented with the following security options:
   a) The beacon shall be enabled
   b) The SSID should be changed from the default
   c) WPA2 should be enabled
   d) WPS should be disabled
   e) These security options should be reviewed annually and adjusted as appropriate as improved industry standards for wireless security are developed.
   f) A strong password (see Policy 2040 Passwords and Encryption Keys) shall be used.

H) **Encryption of desktop, mobile devices and portable media**. When encryption of end-user devices is determined appropriate based on risk analysis, ABACUS shall encrypt the device the framework detailed in NIST Special Publication 800-111, *Guide to Storage Encryption technologies for End User Devices*. Specifically, ABACUS
   a) should consider solutions that use existing system features (such as operating system features) and infrastructure
   b) should use centralized management for all deployments of storage encryption except for standalone deployments and very small-scale deployments

2) Third party hosting company security shall be monitored via periodic vulnerability evaluations. Corrective action shall be taken based on findings.

3070 Business Associate Contracts

POLICY
ABACUS will obtain satisfactory assurance that contractors with access to PHI will appropriately safeguard PHI by employing appropriate physical, technical and administrative procedures. Further, these contracts will pass along any additional obligations agreed in contracts with ABACUS's customers to the contractors.

AUDIENCE
HIPAA Security Officer, HIPAA Privacy Officer

REFERENCES:
45 CFR 160.103 Definitions (of Business Associate)
45 CFR § 164.502(e) Disclosures to Business Associates
45 CFR § 164.504(e) Business Associate Contracts
45 CFR 164.308(b) (1),(2),(3) Security Rule - Business Associate Contracts
EHNAC VI.B.2, VI.B.20, VI.E.1, VI.E.2, VI.E.3, VI.E.5

PROCEDURES

1) Contractors of ABACUS who have access to PHI will be described in these policies as "Business Associates", and the contract which extends ABACUS's HIPAA obligations to them will be referred to as a Business Associate Agreement.
2) ABACUS will have a written Business Associate Agreement with every Business Associate. See Appendix B - Sample HIPAA Business Associate Agreement.
3) Contracting Standards. ABACUS shall include in its contracts with contractors advance arrangements regarding responsibilities, decision making, and costs in the event of a breach caused by a contractor.
4) ABACUS will maintain a list of all Business Associates that have access to ePHI.
5) Due diligence will be exercised, as necessary in the Security Officer's judgment, to validate Business Associate compliance with the terms of the agreement.
6) In the event ABACUS learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, ABACUS will take steps to cure the breach or end the violation. If ABACUS is unable to cure the breach or end the violation, ABACUS will terminate the Business Associate Contract.

3075 Employee System Access

POLICY
System access will be granted to employees in a manner consistent with the HIPAA regulations, including specific policies for access control, granting access to new staff and staff with assignment changes, handling staff terminations, password selection, maintenance and use.

AUDIENCE
Executive Management, Supervisors, Security Officer

REFERENCE
EHNAC II.A.4, VI.B.5, VI.B.6, VI.B.11, VI.D.1, VI.D.2

PROCEDURES

AUTHORIZATION TO SYSTEMS AND ROLE-BASED ACCESS CONTROLS

Audience: Security Officer

1) The Security Officer shall maintain and document a current "minimum necessary" analysis, per Policy 1020 Minimum Necessary Policy which identifies the classes of persons (job descriptions) and the categories of Protected Health Information which they need access to.
2) ABACUS shall utilize the appropriate technical safeguards in the design of the service offering to limit access to PHI based on the Minimum Necessary Policy.
3) The authority to grant access to information systems rests with ABACUS executive management, is delegated to the Security Officer, and by the Security Officer to personnel responsible for system administration.
4) The Security Officer shall maintain an updated inventory of employees with access to PHI and the access rights which are granted.

SYSTEM AND FACILITY ACCESS FOR NEW HIRES

Audience: Supervisors, Contractors

1) The human resource department and/or HR Manager shall complete all hiring procedures as detailed in Policy 1500 Employee/Contractor Recruiting and Termination
2) Supervisors and Contractors shall direct requests for access to information systems to the Security Officer or his/her designee. The Security Officer will employ appropriate diligence in evaluating and granting requests.
3) The Security Officer shall authorize actions to provide system access.
4) Employees will receive Security Awareness Training, in the manner chosen by the Security Officer, in accordance with the Policy 3040 Security Awareness Program In addition, new employees will be given access to these policies and will sign written acknowledgement that they understand and will adhere to all policies. These acknowledgements will be maintained by the Security Officer in the compliance file.
5) User accounts and passwords should be assigned as detailed in Policy 2040 Passwords and Encryption Keys.

3090 Security Incident Response and Reporting

POLICY
ABACUS will monitor all electronic information systems for breaches of security, mitigate harmful effects of security incidents to the extent practicable, and document any such security incidents and their outcomes.

AUDIENCE
All Staff

REFERENCE
EHNAC III.D.5, VI.B.15, VI.B.24

PROCEDURES
Duties, Contingency Planning and Drills
1) The Security Officer is responsible for managing security incident response and reporting. This includes mitigation strategy, communications with law enforcement, clients and the media.
2) The Security Officer, with approval of ABACUS's executive management, may create a team of key individuals to assist in carrying out the incident response duties. The members of that team are documented in Appendix F
3) The Security Officer will develop contingency plans, such as identification of a computing forensics specialist, public relations firm, or legal counsel who can be contacted in the event of a serious incident. These 3rd parties are documented in Appendix F.
4) The Security Officer may conduct security incident drills to develop skills and improve performance in the event of a serious security incident, not limited to, but including a ransomware attack.

Security Incident Reporting and Response Procedure
1) Any employee who becomes aware of a potential security incident must immediately contact the Security Officer to report the incident.
2) The Security Officer will respond to all security incidents, within 2 hours of notification, with appropriate action based on the circumstances. This response will include:
   A) Notifying ABACUS's executive management of any serious incident
   B) Taking corrective action as appropriate to contain the incident
   C) Notifying customers, per any Business Associate Agreement executed under Policy 3070 Business Associate Contracts, within the timeframe agreed in the contract, and
   D) Following procedures specified in Policy 3035 Breach Reporting and Policy 1080 Duty to Report Violations and Security Incidents as appropriate.
   E) Mitigating effects of incident following the procedures specified in Policy 1850 Mitigation
   F) Notifying law enforcement as appropriate.
3) The Security Officer will file a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include
   A) Date and time of report
   B) Date and time of incident
   C) Description of circumstances
   D) Corrective action taken
   E) Mitigating action taken

   Documentation will be kept for 6 years.
4) The Security Officer and/or Incident Response Team will conduct a post-incident analysis to evaluate the ABACUS's safeguards and the effectiveness of response, and recommend to management any changes they believe appropriate.

Appendix A - Identifying Business Associates and Sample BAA

Identifying your Business Associates

Business Associates are obligated to identify subcontractors, who are also Business Associates, and place them "Business Associate" under a contract that meets the specifications of the HIPAA regulations. Further, these Business Associates, as of January 25, 2013, are directly regulated by the HIPAA regulations and for the first time are subject to the same civil and criminal penalties for any failures to comply with the portions of the HIPAA regulations that apply to them.

An abbreviated definition of "Business Associate" is a person or entity, other than a member of the workforce, that performs certain functions, activities or provides services that involve the use or disclosure of PHI on behalf of a covered entity or business associate.

More specifically, the functions and activities that create a Business Associate relationship are:

- claims processing or administration,
- data analysis, processing or administration,
- utilization review,
- quality assurance,
- patient safety activities listed at 42 CFR 3.20,
- billing,
- benefit management,
- practice management,
- repricing,
- legal,
- actuarial,
- accounting,
- consulting,
- data aggregation,
- management,
- administrative,
- accreditation or
- financial services.

Subcontractors of Business Associates are Business Associates. A significant change in the January 25, 2013 HIPAA Rule changes is that subcontractors of your business associates, who have access to PHI, are now Business Associates. For example, suppose you contract with a hosting provider. The hosting provider subcontracts with a computer forensics specialist for security incident response. The computer forensics specialist is a Business Associate. However, it is the hosting provider's responsibility, not yours, to place the computer forensics specialist under the Business Associate contract.

There may be entities who have access to PHI who do not meet the test of being a Business Associates. In such cases, it may be appropriate to include a confidentiality clause in any contract with that entity.

Full Definition of Business Associate from the HIPAA Rules (1/25/2013 Revision):

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management,

practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Sample HIPAA BAA for use with Subcontractors

Business Associates are obligated to place certain subcontractors (also "Business Associates") under a contract that meets detailed specifications that were updated on 1/25/2013. Below is a contract that meets these specifications. Note that it must be customized in Appendix A with a brief clause which defines the "allowed uses and disclosures". Several example clauses are included.

The Sample HIPAA BAA for use with Subcontractors is on the following page:

HIPAA BUSINESS ASSOCIATE AGREEMENT

This business associate agreement ("Agreement") is entered into by and between _____ ("BUSINESS ASSOCIATE") and _____., ("SUBCONTRACTOR").

RECITALS

1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 164. This agreement is written to comply with the revisions enacted in the HITECH statute in February 2009, the regulation changes published in August 2009 and further updates published January 25, 2013.

2) Terms used in this agreement, rendered in lower case, including but not limited to "covered entity", "business associate", "subcontractor", "protected health information ", "PHI", "unsecured protected health information", "electronic protected health information", "use", "disclose", "breach", and "security incident", shall have the same meaning as defined in most current versions of the above referenced regulations.

3) BUSINESS ASSOCIATE has entered into HIPAA business associate agreement with either a HIPAA covered entity, or with another HIPAA business associate.

4) Per the January 25, 2013 HIPAA Regulation changes, subcontractors of business associates are also business associates. This agreement is designed to satisfy a HIPAA business associate's obligation to place its subcontractor under a business associate agreement and to specify the details of that relationship.

NOW, THEREFORE, in consideration of the foregoing, the parties agree as follows:

1) **Allowed Uses and Disclosures of Protected Health Information**. The SUBCONTRACTOR provides services for the BUSINESS ASSOCIATE. The SUBCONTRACTOR may use and disclose protected health information only as follows:

   a) SUBCONTRACTOR may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, SUBCONTRACTOR may disclose protected health information to its employees, subcontractors and agents, in accordance with the provisions of this agreement.

   b) SUBCONTRACTOR may further use and disclose protected health information, if necessary
      i) for the proper management and administration of the SUBCONTRACTOR's business, and/or
      ii) to carry out the legal responsibilities of the SUBCONTRACTOR
      if the disclosure is either
      i) required by law, or
      ii) SUBCONTRACTOR obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the SUBCONTRACTOR of any instances of which it is aware in which the confidentiality of the information has been breached.

2) **Responsibilities of SUBCONTRACTOR**. With regard to its use and disclosure of protected health information, SUBCONTRACTOR agrees to do the following:
   a) Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.
   b) Use appropriate physical, technical and administrative safeguards to protect electronic protected health information, and comply with the requirements of the HIPAA Security Regulations (45 CFR Part 164 Subpart C) which are applicable to business associates.
   c) Report to the BUSINESS ASSOCIATE any security incident within 5 days of occurrence. If the security incident involves a known or potential disclosure of PHI in violation of the HIPAA Privacy rule, or if there is any other use or disclosure not provided by this contract, SUBCONTRACTOR shall conduct the risk assessment to prescribed by 45 CFR 164.402, to determine if a Breach occurred. The results of this risk assessment shall be provided to the BUSINESS ASSOCIATE contact person identified in the Notices section of this agreement, below, within 10 days. This notification may be done via phone and/or secure email to ensure timely response. In the event of a Breach, SUBCONTRACTOR shall provide to BUSINESS ASSOCIATE all information required by 42 CFR 164.410, within 20 days, in a manner mutually agreed by the two parties.
   d) Require that subcontractors who create, receive, maintain or transmit electronic protected health information on behalf of SUBCONTRACTOR comply with applicable HIPAA Security regulations by entering into a Business Associate contract with these subcontractors. The business associate contract shall meet the specifications of 45 CFR 164.314.
   e) Make available to the individual any requested protected health information, in accordance with procedures specified by BUSINESS ASSOCIATE and in compliance with 45 CFR 164.524, "Access of individuals to protected health information".
   f) Make available for amendment, and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR 164.526, "Amendment of protected health information".

g) Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528.

h) To the extent that SUBCONTRACTOR is to carry out BUSINESS ASSOCIATE's obligations under the HIPAA Privacy Regulations, 45 CFR 164 Part E, comply with the requirements of the Privacy Regulations in the performance of those obligations.

i) Business associates will comply with the minimum necessary standard in accordance with 45 CFR 164.504 "Uses and Disclosures: Organizational Requirements," including maintaining a current list of all individuals with access to PHI. This list shall be kept updated at all times.

j) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the BUSINESS ASSOCIATE's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

k) Return to the BUSINESS ASSOCIATE or destroy, as requested by the BUSINESS ASSOCIATE, within 30 days of the termination of this Agreement, the protected health information in SUBCONTRACTOR's possession and retain no copies or electronic back-up copies. If this is not feasible, SUBCONTRACTOR will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.

3) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

4) **Term and Termination**.

a) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

b) Termination. As provided for under 45 C.F.R. §164.504, the BUSINESS ASSOCIATE may immediately terminate this Agreement and any related agreement if it determines that the SUBCONTRACTOR has breached a material provision of this Agreement. Alternatively, the BUSINESS ASSOCIATE may choose to: (i) provide the SUBCONTRACTOR with 30 days written notice of the existence of an alleged material breach; and (ii) afford the SUBCONTRACTOR an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

5) **Survival**. The respective rights and obligations of SUBCONTRACTOR and BUSINESS ASSOCIATE under the provisions of Sections 2(j), detailing SUBCONTRACTOR's return and/or ongoing protections of protected health information, shall survive the termination of this Agreement.

6) **Indemnification**. SUBCONTRACTOR agrees to indemnify, and reimburse BUSINESS ASSOCIATE for all costs incurred by BUSINESS ASSOCIATE for SUBCONTRACTOR's violations of this agreement, including any breaches of unsecured PHI.

7) **Amendment**. This Agreement supersedes any previously negotiated HIPAA business associate agreements. Further, it may be modified or amended only in writing as agreed to by each party.

8) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to SUBCONTRACTOR _____
_____
_____
_____

If to BUSINESS ASSOCIATE: _____
_____
_____
_____

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of _____.

BUSINESS ASSOCIATE

By:_____
Name: _____

SUBCONTRACTOR

By:_____
Name:_____

Title: _____ Title:_____
Date:_____ Date:_____

Attachment A – Permitted Uses and Disclosures

SUBCONTRACTOR is authorized to use protected health information for the purposes of _____
_____
_____

[INSERT A CLAUSE THAT DESCRIBES SUBCONTRACTOR's ALLOWED USES AND DISCLOSURES. THIS WILL VARY DEPENDING ON THE NATURE OF THE RELATIONSHIP. THE FOLLOWING IS AN EXAMPLE OF A CLAUSE FOR A CONTRACT TRAINER.]

Example Clauses:
Trainer: Subcontractor is permitted to use and disclose ePHI only for the purposes of providing training services to Business Associate's customers. .

Appendix B - Sample HIPAA BAA - for use with Clients

HIPAA BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE Agreement ("Agreement") is entered into by and between _____ ("BUSINESS ASSOCIATE") and _____., (the "COVERED ENTITY").

RECITALS

1) The purpose of this Agreement is to comply with the HIPAA Privacy and Security regulations found at 45 C.F.R. Part 160 and Part 164. This agreement is written to comply with the revisions enacted in the HITECH statute in February 2009, the regulation changes published in August 2009 and further updates published January 25, 2013.

2) Terms used in this agreement, including but not limited to "covered entity", "business associate", "Protected Health Information (PHI)", "unsecured protected health information", "use", "disclose", "breach", and "security incident", shall have the same meaning as defined in most current versions of the above referenced regulations.

3) COVERED ENTITY is a covered entity and regulated by the HIPAA regulations.

4) Per the January 25, 2013 HIPAA Regulation changes, BUSINESS ASSOCIATE is also regulated by the HIPAA regulations, and further agrees to comply with the unique requirements of this agreement.

NOW, THEREFORE, in consideration of the foregoing, the parties agree as follows:

1) **Allowed Uses and Disclosures of Protected Health Information**. The BUSINESS ASSOCIATE provides services for the COVERED ENTITY. The BUSINESS ASSOCIATE may use and disclose protected health information only as follows:

   a. BUSINESS ASSOCIATE may use and disclose protected health information for the purposes specifically provided in Attachment A. In performance of the tasks specified in Attachment A, BUSINESS ASSOCIATE may disclose PHI to its employees, subcontractors and agents, in accordance with the provisions of this agreement.

   b. BUSINESS ASSOCIATE may further use and disclose PHI, if necessary

      i) for the proper management and administration of the BUSINESS ASSOCIATE's business, and/or

      ii) to carry out the legal responsibilities of the BUSINESS ASSOCIATE

      if the disclosure is either

      iii) required by law, or

      iv) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached.

2) **Responsibilities of BUSINESS ASSOCIATE**. With regard to its use and disclosure of protected health information, BUSINESS ASSOCIATE agrees to do the following:

   a. Use and/or disclose the protected health information only as permitted by this Agreement or as otherwise required by law; no further use or disclosure is permitted.
   b. Use appropriate physical, technical and administrative safeguards to protect electronic PHI, and comply with the requirements of the HIPAA Security Regulations (45 CFR Part 164 Subpart C) which are applicable to business associates.
   c. Report to the COVERED ENTITY any security incident, and any use or disclosure not provided by this contract, including breaches of unsecured protected health information as required by 45 CFR 164.410.
   d. Require that subcontractors who create, receive, maintain or transmit ePHI on behalf of Business Associate comply with applicable HIPAA Security regulations by entering into a Business Associate contract with these subcontractors. The Business Associate contract shall meet the specifications of 45 CFR 164.314.
   e. Make available to the individual any requested protected health information, in accordance with procedures specified by COVERED ENTITY and in compliance with 45 CFR 164.524, "Access of individuals to protected health information".
   f. Make available for amendment, and incorporate any amendments to protected health information in accordance with the requirements of 45 CFR 164.526, "Amendment of protected health information".
   g. Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528.
   h. To the extent that BUSINESS ASSOCIATE is to carry out COVERED ENTITY's obligations under the HIPAA Privacy Regulations, 45 CFR 164 Part E, comply with the requirements of the Privacy Regulations in the performance of those obligations.

i. Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the COVERED ENTITY's compliance with the HIPAA regulations, subject to attorney-client and other applicable legal privileges.

j. Return to the COVERED ENTITY or destroy, as requested by the COVERED ENTITY, within 30 days of the termination of this Agreement, the protected health information in BUSINESS ASSOCIATE's possession and retain no copies or electronic back-up copies. If this is not feasible, BUSINESS ASSOCIATE will limit further uses and disclosures to the reason that return/destruction is not feasible, and to extend the protections in this agreement for as long as the protected health information is in its possession.

3) **Electronic Transactions**. If Business Associate conducts any electronic transactions on behalf of Covered Entity that are subject to 45 CFR Parts 160 and 162 ("Electronic Transactions Rule") issued by HHS under the authority of HIPAA, Business Associate shall conduct all such transactions using the uniform formats and code sets, as required by the Electronic Transactions Rule.

4) **Mutual Representation and Warranty**. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

5) **Term and Termination**.

a. Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

b. Termination. As provided for under 45 C.F.R. §164.504, the COVERED ENTITY may immediately terminate this Agreement and any related agreement if it determines that the BUSINESS ASSOCIATE has breached a material provision of this Agreement. Alternatively, the COVERED ENTITY may choose to: (i) provide the BUSINESS ASSOCIATE with 30 days written notice of the existence of an alleged material breach; and (ii) afford the BUSINESS ASSOCIATE an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement.

6) **Survival**. The respective rights and obligations of BUSINESS ASSOCIATE and COVERED ENTITY under the provisions of Sections 2(j), detailing BUSINESS ASSOCIATE's return and/or ongoing protections of protected health information, shall survive the termination of this Agreement.

7) **Amendment**. This Agreement supersedes any previously negotiated HIPAA Business Associate agreements. Further, it may be modified or amended only in writing as agreed to by each party.

8) **Notices**. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to BUSINESS ASSOCIATE _____
_____
_____
_____

If to COVERED ENTITY: _____
_____
_____
_____

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of _____.

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:_____	By:_____
Name: _____	Name:_____
Title: _____	Title:_____
Date:_____	Date:_____

Attachment A – Permitted Uses and Disclosures

BUSINESS ASSOCIATE is authorized to use protected health information for the purposes of providing computer network support, network management, system backup, recovery testing, training and other computer related activities as agreed. {Customize as necessary!}

Appendix D -Facility Security and Access Plan

Physical Security: After business hours, the main door to the building is locked by the landlord's security guard. Only tenants have key fabs to the outside doors. The doors to the ABACUS's suite are kept locked except during normal business hours. An alarm system is used, with 3rd party monitoring, to detect intrusions.

Visitors. Only approved guests and visitors are allowed into the ABACUS suite. All visitors must sign-in and sign-out in visitor log, stating name, company, person visited, purpose of visit, time in and time out. A company employee must be with visitors at all times. Visit logs are kept for 1 year.

Opening Procedure: All employees are given office keys and the codes for the alarm system. The first person in disarms the alarm and unlocks the door for the day.

Closing Procedure: The office suite door is locked at 5PM when the office closes.

Security Cameras. Cameras are used to monitor ingress/egress from the building. The company suite has 32 security cameras recorded on two independent DVRs.

Server Room: Servers and equipment for the office are kept in the administrative section of the suite which is independently locked. Only the VP of Systems, and the programmer in charge of network administration have the keys.

No Hardcopy Passwords: No system passwords are to be handwritten on paper anywhere. Passwords are maintained in the password management system.

No ePHI: No ePHI is to be kept on servers of equipment in the company facility. ePHI must remain on the client-owned servers at client locations.

Appendix E - Workforce Access to PHI and Safeguards

Person, Classes of Persons, or Business Associates	***Categories of PHI Needed***	***Additional Safeguards(*)***
Company Owner	PHI on customer servers that is essential to a support issue that has escalated	Procedural controls detailed in 2000 Technical Support Procedures
Support Technicians	PHI contained on customer servers that is viewed during support.	Procedural controls detailed in 2000 Technical Support Procedures Workstations employ full disk encryption and run Eraser
Customer Service Supervisor	Switch portal access	Used for troubleshooting claim processing issues
Administrative Staff	None	

*Safeguards: All employees will receive training on ABACUS confidentiality policies and will be subject to sanctions for violations. The table above lists additional safeguards that will be employed

Employee Access To PHI
Employees in the customer and technical services department may encounter PHI during the course of supporting a customer. The HIPAA Security Officer and HIPAA Privacy Officer may also encounter PHI as they provide oversight to the customer and technical services staff. The following table lists all employees who may encounter PHI and their respective positions in the company.

Employee	**Title**
Orlando Alberro	President/HIPAA Security Officer
Roberto Alberro	Vice President/HIPAA Privacy Officer
Maria Zenteno	Director of Customer Support
Miguel Astorquiza	Director of Technical Support
Jennifer Santos	Sr. Customer Support Specialist
Yanet Figueredo	Sr. Customer Support Specialist
Madeline Quintana	Customer Support Specialist
F. Harvey Miranda	Technical Systems Specialist
Keneth Fiqueroa	Technical Systems Specialist

Appendix F – Miscellaneous

Policy 2900 Security and Privacy Officer Appointment and HIPAA Documentation

HIPAA Security Officer – Orlando Alberro
HIPAA Security Officer backup – Roberto Alberro

HIPAA Privacy Officer – Orlando Alberro
HIPAA Privacy Officer backup – Roberto Alberro

Addressable HIPAA Security Implementation Specifications Not Implemented

Reference	Implementation Specification	Comments
164.310(a)(1)	Maintenance Records	This is a small company, with one office. The owner is at the office daily and keeps all equipment in good repair. No formal policy is necessary.
164.310(d)(1)	Device and Media Controls -- Accountability	Abacus policy is to not maintain any ePHI on its servers. This control is not relevant.
164.308(a)(3)	Authorization and/or supervision	This is a small organization -- all employees know who their supervisor is – no policy is necessary to detail the procedures.
164.308(a)(5)	Log-in monitoring	There is no remote access to the system; based on the risk analysis this control is not high priority.
164.312(a)(2)(iii)	Automatic Logoff	Abacus maintains no systems that keep PHI. Further, this is a small office which rarely has visitors. This control is not necessary.

Policy 3090 Security Incident Response and Reporting

Incident Response Team
The following individuals serve on the Incident Response Team:

- Supervisor of Technical Services
- President

Legal Counsel to contact in event of Security Incident / Data Breach
If needed, legal counsel will be retained to for incident response. Forensic specialist will be retained by legal counsel to ensure that findings are protected under attorney-client privilege:
Amy S. Leopard, Partner
Bradley Arant Boult Cummings LLP
Roundabout Plaza, 1600 Division St. #700
Nashville, TN 37203
(615) 252-2309
aleopard@bradley.com

Computing Forensics Specialist
If needed, the following forensic specialist will be contacted to assist with incident response.
Interhack Inc.
Address: 5 E Long St, Columbus, OH 43215
Phone: (614) 545-4225
Web: http://web.interhack.com/

Policy 1300 Application Certification and Notifications

Text of the 2-form letter used to inform customers of adverse reports and the need to cease of the software applications is copied below.

Dear Customer:

FORM A.
It has come to our attention that our software, which you are utilizing, is noncompliant with requirement [INSERT APPLICABLE CFR CODE]. For this reason, to maintain your own compliance, you must immediately cease using the software to create, sign, transmit, or process electronic controlled substance

FORM B
It has come to our attention that our software, which you are utilizing, is noncompliant with requirement [INSERT APPLICABLE CFR CODE]. For this reason, to maintain your own compliance, you must immediately cease using the software to process prescriptions that require this additional information.

A copy of the adverse certification report detailing the requirements that have not been met is included.

We are working on an update that will fix this issue and we will have it available to use as soon as possible. You will be notified when that update is available.

Thank you,
Abacus

Text of the form letter used to inform customers that an update is required to bring the software application back into compliance so that it can be used again.

Dear Customer:
The latest software update corrects the previous non-compliance issue and brings the software into full compliance with requirement [INSERT APPLICABLE CFR CODE]. The software is now fully compliant and you may resume full functionality after you have installed the update

Thank you,
Abacus

ABACUS Disclosure Log

Date	Person or Entity receiving Records	Description of records disclosed	Customer(s) affected	Purpose of disclosure	Description of threat to health or safety (if reason is in response to health or safety threat or emergency)

ABACUS

COMPANY POLICIES AND PROCEDURES ACKNOWLEDGEMENT AND COMPLIANCE AGREEMENT

Name_____ Date_____

I have reviewed and understand the policies and procedures that are relevant to my job duties. These include:

Policy number	Description
1010	HIPAA – General Rules
1020	Minimum Necessary
1030	Confidentiality Safeguards (Oral & Written)
1050	Computer Usage
1060	Portable Computing Devices and Home Computer Use
1080	Duty to Report Violations and Security Incidents
1900	Sanctions for Staff Violations of Privacy/Security Policies
2000	Technical Support Procedures
2005	Secure Network Configuration for Client Networks
2010	Software Development Procedures
2020	Source Code Management
2030	Intellectual Property
2040	Authentication, Passwords and Encryption Keys
3015	Facility Security and Access Control

Further, I understand all other company policies that are relevant to my job duties and agree to comply with all policies.

I understand the requirement to maintain the strict confidentiality of any PHI in customer systems that I may encounter while providing customer support. I will not divulge any PHI to any individual except as expressly authorized in company policies. I understand that violation of this provision could result in termination and/or legal action.

Signature:_____ Date:_____