

## FINELINE HIPAA COMPLIANCE POLICY

Fineline may use or disclose Protected Health Information received from or created or received on behalf of client ("PHI") and nonpublic personal information received from or created or received on behalf of client ("Personal Information") to perform functions, activities, or services for, or on behalf of client as specified per written agreement, provided that such usage or disclosure would not violate the HIPAA privacy and security regulations, GLB or other federal or state privacy and security laws that are applicable.

1. With regard to its use and/or disclosure of PHI or Personal Information, Fineline hereby agrees and represents and warrants to client that Fineline shall:

- a. not use or further disclose any PHI or Personal Information other than as permitted by an agreement or required by law;
- b. at all times maintain and use appropriate safeguards to prevent uses or disclosures of any PHI or Personal Information other than as permitted by an agreement or required by law, and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information ("E PHI") (as defined in 45 CFR Section 160.103) that Fineline creates, receives, maintains, or transmits on behalf of client, including, at a minimum, the safeguards, policies and procedures with respect to E PHI set forth in Fineline's HIPAA Policies and Procedures.
- c. ensure that any and all subcontractors or agents to whom Fineline provides any PHI or Personal Information agrees in writing to the same conditions and restrictions that apply to Fineline with regard to the PHI or Personal Information; and
- d. ensure that any and all subcontractors or agents to whom Fineline provides E PHI agree in writing to implement reasonable and appropriate safeguards to protect E PHI.

2. With regard to its use and/or disclosure of PHI, Fineline agrees, represents and warrants to client that Fineline shall:

- a. report promptly to client any: (i) use or disclosure of any PHI of which it becomes aware that is not permitted by the Agreement and (ii) any Security Incident (defined in 45 CFR Section 164.304) of which it becomes aware;
- b. mitigate, to the extent practicable, any harmful effect that is known to Fineline of a use or disclosure of PHI by Fineline in violation of the requirements of this Agreement;
- c. in the time and manner designated by client, make available PHI in a Designated Record Set, to client, or as directed by client, to an individual, in order for client to respond to individuals' requests for access to information about them in accordance with the HIPAA privacy regulation;
- d. in the time and manner designated by client, make any amendments or corrections to the PHI in a Designated Record Set that client directs in accordance with the HIPAA privacy regulation;
- e. in the time and manner designated by client, document such disclosures of PHI and information related to such disclosures as would be required for client to respond to a request by an individual for an accounting of disclosures of PHI in accordance with the HIPAA privacy regulations;
- f. in the time and manner designated by client, make available to client, or as directed by client, to an individual, the information documented in accordance with subsection (e) above, to permit client to respond to a request by an individual for an accounting of disclosures, in accordance with the HIPAA privacy regulations; and
- g. in the time and manner designated by client or the Secretary of HHS, make its internal practices, books and records relating to the use and disclosure of PHI available to client, or the Secretary of HHS for purposes of determining clients' compliance with the HIPAA privacy regulations.

4. Each term and condition required by HIPAA and/or GLB shall be effective on the compliance date applicable to client or the effective date of the Agreement, under the HIPAA privacy and security regulation and/or GLB, respectively.

5. Upon the termination or expiration of the Agreement for any reason, Fineline shall return to client or destroy all PHI and/or Personal Information, and retain no copies in any form whatsoever. This provision shall apply to PHI and/or Personal Information that is in the possession of subcontractors, vendors or agents of Fineline.

6. Fineline agrees that this agreement or an order may be terminated by client upon written notice to Fineline in the event that client determines that Vendor has violated any material term of this policy. Alternatively, client may

choose to provide Fineline with written notice of the existence of an alleged material breach of this policy and afford Fineline an opportunity to cure said breach upon mutually agreeable terms. Failure to cure, or a determination by client that cure is not practicable or possible, shall be grounds for the immediate termination of agreement. Fineline agrees to defend, indemnify and hold harmless client against any and all claims, liabilities, judgments or damages asserted against, imposed upon or incurred by client that arise out of any violation of this policy.

7. The Parties agree to take such action as is necessary to amend this agreement from time to time as is necessary for client to comply with the requirements of HIPAA, the HIPAA privacy and security regulations, GLB and other federal and state privacy, security and consumer rights laws and regulations applicable to client. Fineline agrees to cooperate with and assist client in order for client to meet its obligations under applicable privacy and security laws and regulations.

10. The terms and conditions required by HIPAA shall be construed in light of any applicable interpretation of and/or guidance on the HIPAA privacy and security regulations issued by HHS from time to time. Any ambiguity in the agreement shall be resolved in favor of a meaning that permits client to comply with applicable laws and regulations.

## FINELINE PRINTING HIPAA POLICIES AND PROCEDURES

A Risk Analysis was performed and the following was developed:

### **I. Administrative Safeguards**

- A. Security Management Process.
  - (1) Log file audits are performed randomly to prevent, detect, contain and correct security violations.
  - (2) Written reports of Log file audits are available to analyze physical and logical security, network configuration, change/problem, vulnerability management and recovery services.
- B. Assigned Security Responsibility. The Director of IT is Fineline's security official - Workforce Security. Security (firewall with intrusion detection) is in place that prevents those workforce members without authorized access from obtaining any electronic records.
- C. Information Access Management. In place is an access authorization to ensure access to EPHI is appropriate.
- D. Security Awareness and Training. Implement security awareness, training and updates are performed regularly to and (i) guard against, detect and report viruses and other malicious software, as appropriate, and to (ii) create, change, and safeguard passwords (password retention policy).
- E. Security Incident Procedures.
  - (1) address security incidents – notify all parties immediately and report the loss.
  - (2) Identify and respond to security incidents, mitigate their harmful effects to the extent possible, and document the incidents and the outcome.
- F. Contingency Plan. Employ Data backup systems covers occurrences that could damage systems that contain EPHI.
- G. Evaluation. Director of IT periodically evaluate policies and procedures in light of the requirements contained in this Policy A, and make changes to such policies and procedures as appropriate.

### **II. Physical Safeguards**

- A. Facility Access Controls. Server room is physically locked and restricted entry is limited to Director of IT and VP of Operations. hardware is password protected. limit physical access to electronic information systems and the facilities in which they are housed only to those workforce members whose access is authorized by Business Associate and is appropriate.
- B. Workstation Use. Password protections for workstations that access EPHI, to minimize risks of disclosure of EPHI.
- C. Workstation Security. Implement physical safeguards to reduce the risk that unauthorized users will access workstations that access EPHI. Screensavers and system lock out occurs in an appropriate amount of inactivity. No EPHI is stored locally on workstations.
- D. Device and Media Controls. Implement policies and procedures regarding the physical movement of physical movement of hardware and media is not used if data is on physical media it is immediately destroyed or returned that contains EPHI.

### **III. Technical Safeguards**

- A. Access Control. Internal access of EPHI is governed by Microsoft Active Directory. External transfer is encryption using 1024 bit IPsec technology Implement technical policies and procedures to: (i) allow access to EPHI only to those persons or software programs that have been granted appropriate access rights, and (ii) use encryption technology with respect to EPHI transmissions over public networks.
- B. Audit Controls. Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.
- C. Integrity. Access control lists are utilized to ensure EPHI from improper alteration or destruction.
- D. Person or Entity Authentication. Implement procedures to verify the person or entity accessing EPHI is the one claimed – username and password protected. Password retention policy ensures user is authorized/
- E. Transmission Security. Implement technical measures to protect the EPHI against unauthorized access when being transmitted.

## SECURITY POLICY

This policy applies (i) when Vendor requires electronic access to Provider and/or Provider's Information Systems; (ii) in addition to any of Vendor's obligations under the Agreement, any Business Associate Agreement or other agreement, or any requirements imposed upon Vendor by applicable laws or regulations; and (iii) in addition to any Provider due diligence that may be performed regarding Vendor's systems and security practices. In the event of a conflict between this policy and any other term between the parties, the terms most protective of Provider, in Providers' determination, shall apply.

**1. Definitions.** The following terms shall have the meanings as set forth below:

1.1 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Provider Information or interference with the operations of any of the Vendor Processing Resources. Security Incidents are classified as follows:

(a) "High Severity" or severity 1 (severe impact) means external loss or exposure of Provider's Information, causing significant impact to mission critical information technology systems including large-scale outages. Incidents or exposures classified at this level affect critical Provider's Information Systems and will affect Providers' customers.

(b) "Medium Severity" or severity 2 (major impact) means internal loss or exposure of Provider's Information, causing significant business interruption. Incidents or exposures classified at this level affect non-critical Provider's Information Systems and may affect Providers' customers.

(c) "Low Severity" or severity 3 (moderate impact) means loss or exposure of Provider's public information, causing a limited or confined business interruption. Incidents or exposures classified at this level affect Provider's Information Systems or assets, but do not affect Providers' customers.

1.2 "Providers Information" includes Private and Confidential Information of Provider as such is defined in the Agreement, Personal Non-Public Information, as defined under the Gramm-Leach-Bliley Act and implementing regulations ("GLB"), as well as Protected Health Information and Electronic Protected Health Information, as such terms are defined in 45 C.F.R. Parts 160 and 164 (or successor regulations).

1.3 "Provider's Information Systems" means information systems resources supplied or operated by Provider or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity which are owned, controlled or administered by or on behalf of Provider.

1.4 "Vendor Processing" means any information collection, storage or processing performed by Vendor or its contractors (i) which directly or indirectly supports the services or functions now or hereafter furnished to Provider under the Agreement, (ii) using any Provider Information, or (iii) in respect of any other information if performed on behalf of Provider or in support of Providers' business, operations or services.

1.5 "Vendor Processing Resources" means information processing resources supplied or operated by Vendor, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Vendor Processing.

## 2. Security Management

2.1 Vendor Security Contact. Vendor shall provide a security representative as the single point of contact for Provider on all security issues, who shall be responsible for overseeing compliance with this Policy.

2.2 Policies and Procedures. Vendor shall maintain written security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, availability, or security of Vendor Processing Resources and/or Provider Information. Such policies and procedures shall (i) assign specific data security responsibilities and accountabilities to specific individual(s); (ii) include a formal risk

management program which includes periodic risk assessments; and (iii) provide an adequate framework of controls that safeguard Provider Information Systems and Provider Information.

2.3 Infrastructure Protection. Vendor shall maintain industry standard procedures to protect Vendor Processing Resources, including, at a minimum:

- (a) Formal security programs (policies, standards, processes, etc.);
- (b) Processes for becoming aware of, and maintaining, security patches and fixes;
- (c) Router filters, firewalls, and other mechanisms to restrict access to the Vendor Processing Resources, including without limitation, all local site networks which may be accessed via the Internet (whether or not such sites transmit information);
- (d) Resources used for mobile access to Provider Information Systems shall be protected against attack and penetration through the use of firewalls; and
- (e) Processes to prevent, detect, and eradicate malicious code (e.g., viruses, etc.) and to notify Provider of instances of malicious code detected on Vendor Processing Resources or affecting Provider Information.

### 3. Risk Management

3.1 General Requirements. Vendor shall maintain appropriate safeguards and controls and exercise due diligence to protect Provider Information and Vendor Processing Resources against unauthorized access, use, and/or disclosure, considering all of the below factors. In the event of any conflict or inconsistency, Vendor shall protect the Provider Information and Vendor Processing Resources in accordance with the highest applicable requirement:

- (a) Federal, state, legal and regulatory requirements;
- (b) Information technology and healthcare industry best practices;
- (c) Sensitivity of the data;
- (d) Relative level and severity of risk of harm should the integrity, confidentiality, availability or security of the data be compromised, as determined by Vendor as part of an overall risk management program;
- (e) Providers' data security requirements, as set forth in this Policy, the due diligence process and/or in the Agreement; and
- (f) Any further information security requirements which are included in a statement of work or equivalent document which is attached to or relates to the Agreement.

3.2 Security Evaluations. Vendor shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Provider Information and Vendor Processing Resources. Vendor shall document the results of these evaluations and any remediation activities taken in response to such evaluations, and provide to Provider a copy.

3.3 Internal Records. Vendor shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. In response to such events, Vendor shall take appropriate action to address and remediate identified vulnerabilities to Provider Information and Vendor Processing Resources.

3.4 Client Audits. Finline agrees to permit client, its auditors, its customers, or any governmental authority, upon reasonable advance notice, to inspect and examine Finline Processing Resources, the facilities used to perform Finline Processing, as well as policies, procedures, plans, and other records and documentation as reasonably necessary for client to verify Finline's compliance with this Policy. Provider reserves the right to require Vendor to install appropriate systems management and security software to ensure appropriate protection is in place. Provider shall not disclose any information learned by Provider in the course of performing any such inspection or examination except as may be reasonably necessary for Provider to comply with obligations relating to the protection of Provider Information or as may otherwise be required by law.

3.5 Remediation. Finline will remedy any High Severity security exposure or finding discovered by client within twenty-four (24) hours from the time the finding is identified and notice is provided to Finline. Finline will remedy any Medium to Low Severity security exposure or finding discovered by Provider within two (2) to five (5) business days, from the time the finding is identified and notice is provided to Finline. If Finline does not address the exposure or finding within the applicable time obligation, client shall have the right to immediately terminate access to client Information Systems and client information without penalty to the services related to the access.

3.6 Audit Practices. Finline will provide to client, at least annually, information on its audit processes, procedures and controls, including a report on any findings and remediation efforts. Finline will also provide to client an independent attestation of Finline's security practices and process controls that provide sufficient evidence of such practices and controls (e.g., Statements on Auditing Standards 70 Type II equivalent, etc.).

3.7 Vendor Locations. Unless previously authorized by client in writing, all work performed by Finline related to any agreement shall be performed from the location(s) designated in the agreement and/or relevant Statement of Work(s). For any location(s) outside of the 50 United States where Finline performs work related to the agreement for client, Finline also agrees to maintain the following security controls:

- (a) Finline will conduct either a SAS70 Type II Audit, a BS-7799 certification, or an ISO27001 certification at all Offshore Locations from which work is performed by Finline related to the agreement and will provide the resulting audit reports to client. The audits or certifications will be conducted once annually, and each report will cover a twelve month term. The audit report will be issued to client no later than 30 days after the audit is completed.
- (b) Finline will conduct assessments of general control objectives, as defined by client. These objectives may be periodically updated by client, effective upon delivery to Finline to address additional Services that Finline will provide to client.
- (c) Finline will comply with all future BS-7799 regulations, ISO27001 standards, or that of its successor(s), as issued by the SEC and the Public Company Accounting Oversight Board, British Standards Institute (BSI), or International Standards Organization (ISO).
- (d) In the event that Finline's audit report does not meet client requirements, client may exercise its rights under Section 3.4 of this policy. All costs associated with such audit(s) shall be paid by Finline.
- (e) At clients' request, Finline will provide a quarterly management representation letter reflecting any material changes in the environment utilized for the provided Services.

#### **4. Personnel Security**

4.1 Access to client information. Finline will require its employees, contractors and agents who have, or may be expected to have, access to client information or client Information Systems to comply with the provisions of any agreement, including any confidentiality agreement(s) or Business Associate Agreement(s) binding upon Finline. Finline will remain responsible for any breach of these agreements by its employees, contractors, and agents.

4.2 Security Awareness. Finline will ensure that its employees and contractors remain aware of industry standard security practices, and their responsibilities for protecting the client information. This shall include, but not be limited to:

- (a) Protection against malicious software (such as viruses);
- (b) Appropriate password protection and password management practices; and
- (c) Appropriate use of workstations and computer system accounts.

4.3 Sanction Policy. Finline will maintain a sanction policy to address violations of Finline's internal security requirements or security requirements which are imposed on Finline by law, regulation, or contract.

4.4 Supervision of Workforce. Finline will maintain processes for authorizing and supervising its employees, temporary employees, and independent contractors and for monitoring access to client information, client Information Systems and/or Finline Processing Resources.

4.5 Background Checks. Finline will maintain processes to determine whether a prospective member of Finline's workforce is sufficiently trustworthy to work in an environment which contains Finline Processing Resources and client information. At a minimum, such processes shall meet the requirements set forth in the Background Investigations outlined in any agreement.

**5. Physical Security.** Finline will maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Finline Processing Resources and areas in which client information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). Finline will adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be

maintained. Fineline will maintain appropriate records of maintenance performed on Fineline Processing Resources and on the physical control mechanisms used to secure Fineline Processing Resources. Fineline will obtain clients' prior written approval prior to moving storage or processing of client information, or personnel which have access to client information or client Information Systems, to a location outside the U.S.

## **6. Software**

6.1 Software Licensing. Any access provided to Fineline is limited to client information and client Information Systems and client is not granting Fineline a license to use the software programs contained within clients' Information Systems. Any license to the software programs contained within the clients Information Systems shall be pursuant to a separate agreement between the parties.

6.2 Software Usage. Fineline will not attempt to reverse engineer or otherwise obtain copies of the software programs contained in clients' Information Systems. Any agreements do not transfer Fineline title of any ownership rights or rights in patents, copyrights, trademarks and trade secrets included in clients Information Systems.

## **7. Security Monitoring and Response**

7.1 Incident Response. Fineline will maintain formal processes to detect, identify, report, respond to, and resolve Security Incidents in a timely manner.

7.2 Incident Notification. Fineline will notify client in writing and provide a resolution plan within two (2) hours of any Security Incident(s) which result in, or which Fineline reasonably believes may result in, unauthorized access to, modification of, or disclosure of client information, client Information Systems or other client applications.

7.3 Incident Resolution. After obtaining a written notification and resolution plan, client will determine the severity of the Security Incident and advise Fineline of such severity. If client considers the risk to be a High Severity exposure, Fineline will resolve or mitigate the High Severity within twenty-four (24) hours of providing such notice. If client considers the exposure a Medium or Low Severity exposure, then Fineline will resolve or mitigate the risk within two (2) to five (5) business days of providing such notice. If Fineline does not resolve the Security Incident within the applicable time obligation, client shall have the right to immediately terminate access to client information and client Information Systems without penalty.

7.4 Site Outage. Fineline will promptly report to client any Fineline site outages where such outage may impact client or Fineline's ability to fulfill its obligations to client.

## **8. Communication Security**

8.1 Exchange of Confidential Information. The parties agree to utilize a secure method of transmission when exchanging Confidential Information electronically.

8.2 Encryption. Fineline will maintain encryption, in accordance with standards mutually agreed upon between the parties, for all transmission of client information via public networks (e.g., the Internet). Such transmissions include, but are not limited to:

- (a) Sessions between web browsers and web servers;
- (b) Email containing client information (including passwords); and
- (c) Transfer of files via the Internet (e.g., FTP).

8.3 Protection of Storage Media. Fineline will ensure that storage media containing client information is properly sanitized of all client information or is destroyed prior to disposal or re-use for non- Fineline Processing. All media on which client information is stored shall be protected against unauthorized access or modification. Fineline will maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Fineline Processing or on which client information has been stored.

8.4 Data Integrity. Fineline will maintain processes to prevent unauthorized or inappropriate modification of client information, for both data in transit and data at rest.

## 9. Access Control

9.1 Identification and Authentication. All access to any client information or any Finline Processing Resources shall be Identified and Authenticated as defined in this Section. "Identification" refers to processes which establish the identity of the person or entity requesting access to client information and/or Finline Processing Resources. "Authentication" refers to processes which validate the purported identity of the requestor. For access to client information or Finline Processing Resources, Finline will require Authentication by the use of an individual, unique user ID and an individual password or other appropriate Authentication technique approved by client in writing. Finline will obtain written approval from client prior to using digital certificates as part of Finline's Identification or Authorization processes. Finline will maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Finline and/or used by Finline in connection with any agreements.

9.2 Account Administration. Vendor shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Vendor Processing Resources and Provider Information. These processes shall be required for both Provider-related accounts and Vendor's internal accounts for Vendor Processing Resources, and shall include procedures for granting and revoking emergency access to Vendor Processing Resources and Provider Information. All access by Vendor's employees or contractors to Provider's Information Systems shall be subject to advance approval by Provider and shall follow Provider standard policies and procedures.

9.3 Access Control. Vendor shall maintain appropriate access control mechanisms to prevent all access to Provider Information and/or Vendor Processing Resources, except by (i) specified users expressly authorized by Provider and (ii) Vendor personnel who have a "need to access" to perform a particular function in support of Vendor Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Vendor shall maintain processes to ensure that employee or contractor access to Electronic Protected Health Information is revoked no later than 2 business days upon termination. Vendor shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access Provider Information or Vendor Processing Resources.

## 10. Network Security

10.1 Authorized Access. Finline will only have access to client Information Systems authorized by client and will use such access solely for providing services to client. Finline will not attempt to access any applications, systems or data which client has not authorized Finline to access or which Finline does not need to access in order to perform services for client. Finline further agrees to access such applications, data and systems solely to the extent minimally necessary to provide services to client. Finline's attempt to access any applications, data or systems in violation of the terms in this Section 10.1 shall be a material breach of any agreement.

10.2 Remote Access Requirements. In the event client authorizes Finline to remotely access clients' Information Systems, Finline will only do so only from locations approved by client in writing. These locations may include, but are not limited to, Finline primary locations, co-locations, employee home offices, and required business travel destinations. Finline remote access is subject to clients' security and audit controls as referenced below in sections 10.3 and 10.4.

10.3 Remote Access Security Controls. In the event the client authorizes Finline to remotely access clients Information Systems, unless authorized by client in writing, only client-owned and maintained mobile/PC devices (i.e., laptops, electronic notebooks, desktop PCs, etc) may be used for remote access into clients' Information Systems. In the event that client approves Finline-owned mobile/PC devices for remote access connections, Finline agrees to the following security controls:

- (a) Finline will procure mobile/PC devices and related operational hardware, manage the facilities used for remote or at home use, and provision access to Provider systems.
- (b) Finline will establish mutually agreed upon policies, procedures and protocols that are to address the facilities requirements for remote or at home access.
- (c) Mobile/PC devices shall be registered with the clients' security guard or the clients' manager, as required.

- (d) Finline will restrict administrative rights to mobile/PC device and will provide client field support the rights necessary to verify configuration on periodic basis.
- (e) Finline will configure the mobile/PC device according to clients' connectivity requirements, including approved VPN software.
- (f) Finline will maintain mobile/PC device password and screen saver safeguards.
- (g) Finline will disable all wireless capability from the mobile/PC device when not in use.
- (h) Finline will only use current, commercially supported operating systems on the mobile/PC device.
- (i) Finline will only use current and up to date patches, hot fixes, and service. client reserves the right to require installation of appropriate systems management and security software to ensure adequate protection.
- (j) Finline will not simultaneously connect to the client's network and a non-secure network (third party network or other non-standard connections).
- (k) Finline may only connect to client through a client approved network.
- (l) Finline remote access users shall adhere to client's standard authentication protocols including, but not limited to, network and application login accounts, and/or two factor authentication tokens.
- (m) Finline will remotely connect to client's systems using only the following client-provided solutions:
  - (i) External Corporate Connection through a dedicated private network connection and/or via Virtual Private Network Business To Business Internet Connection ("VPN B2B"), with appropriate firewall rules to restrict connectivity to only required resources, or
  - (ii) External Corporate Connection Virtual Private Network Client solution to a specified user group to restrict connectivity to only required resources, or
  - (iii) External Corporate Connection with a CITRIX presentation model, restricting connectivity and access to only required resources.

10.4 Remote Access Audit Controls. Unless authorized by client in writing, all contracted work by Finline shall be conducted from the designated Finline location. If client authorizes Finline personnel to provide services to client remotely, the following audit controls shall apply:

- (a) Finline will monitor remote or at home users on a periodic basis, which shall include both quarterly onsite audits and a summary report on findings and remediation efforts. Finline will provide such reports to client.
- (b) Finline will follow the additional confidentiality obligations:
  - (i) Finline will not remove any client information from Finline location(s), and will not print or download any including information resulting from connectivity or access to the client system(s), without prior approval of client.
  - (ii) Finline will inventory any client information obtained by Finline and shall return or destroy client information as required by client. If requested by client, Finline will provide a certificate of secure destruction.
  - (iii) Finline will comply with all client policies and procedures regarding the safekeeping of client information. Policies and procedures do include limitations regarding the storage of information on mobile/PC devices.
  - (iv) Finline will keep any client information, in a secure file cabinet, when such information is not in use.
  - (v) Finline will maintain written security management policies and procedures regarding secure possession of client information when traveling and utilizing client information in public environments.

**11. Software Development.** If the Agreement involves the development of software product(s) for client, such software shall be developed and maintained in accordance with the development methodology specified by client. Such software shall satisfy the appropriate client information security policies and guidelines that are furnished by client to Finline (which will be incorporated herein by reference). Finline shall comply with any instructions, guidelines or minimum compliance controls that are furnished by client to Finline (which will be incorporated herein by reference) to enable client to comply with the Sarbanes Oxley Act and/or other applicable laws and regulations.

**12. Business Continuity Management.** Finline will, at its sole expense, establish and maintain (i) written business continuity plans for the Services and supporting facilities and (ii) written disaster recovery plans for critical technology and systems infrastructure and (iii) proper risk controls to enable continued performance under any

agreement in the event of a disaster or other unexpected break in services. Fineline will update and test the operability of any applicable Contingency Plan at least annually, and will maintain each such plan upon the occurrence of a disaster event. A disaster is defined as an unanticipated incident or event, including, without limitation, force majeure events, technological accidents, or human-caused events, that may cause a material service or critical application to be unavailable without any reasonable prediction for resumption, or that causes data loss, property damage or other business interruption without any reasonable prediction for recovery, within a commercially reasonable time period.

**13. Compliance with Laws.** Fineline complies with all federal, state and local laws, regulations, ordinances and requirements relating to the confidentiality, integrity, availability, or security of clients information applicable to Fineline's obligations under agreement. In relation to and in conjunction with Fineline's obligations under any Business Associate Agreement, Fineline will maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of client as required by 45 CFR, Part 164, Subpart C.

**14. Third Parties.** Fineline will ensure that any agent, including a subcontractor, to whom Fineline provides Electronic Protected Health Information agrees to maintain reasonable and appropriate safeguards to protect such Electronic Protected Health Information; provided, however, that Fineline shall not assign, delegate, or subcontract any obligation of Fineline owed to client in violation of any agreements.

**15. Amendments.** Agreements may be modified by a written agreement executed by Fineline and client. Notwithstanding the foregoing or anything else, client may amend this agreement by providing thirty (30) days advance written notice of such amendment if client reasonably determines that such amendment is necessary for client to comply with the Standards for Privacy of Individually Identifiable Health Information or the Security Standards for the Protection of Electronic Protected Health Information (both of which are set forth at 45 CFR Parts 160 and 164) or any other federal, state or local law, regulation, ordinance, or requirement relating to the confidentiality, integrity, availability, or security of individually identifiable medical or personal information.