

H-1 SPECIFICATIONS

Privacy and Data Security

(Revised October 2016)

1. Contract Documents

These H-1 Specifications, together with all other specifications referenced in the contract, constitute an integral part of the agreement between LSC Communications LLC or one of its subsidiaries (hereinafter referred to as "LSC") and the Supplier ("Agreement"). The Supplier must notify the appropriate LSC Purchasing or Global Strategic Sourcing representative in writing immediately if it cannot meet all requirements of these Specifications.

2. Definitions

1. "Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information as described in 45 C.F.R. § 164.402, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. It also includes, except as provided elsewhere in this paragraph 1.a., the unintentional loss or inadvertent disclosure of Personal Information, or the attempted or successful unauthorized access, use, disclosure, modification, destruction or transfer of Personal Information, or any other type of information security breach, loss, corruption or interference with system operations involving Personal Information. Breach does not include: (i) any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of Supplier if such acquisition, access or use was made in good faith and within the course and scope of such employee's or individual's authority and does not result in further use or disclosure by any person in a manner not permitted by 45 C.F.R. § 164 Subpart E; or (ii) any inadvertent disclosure by an individual who is authorized to access PHI at a facility operated by Supplier to another individual authorized to access PHI at the same facility and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by 45 C.F.R. § 164 Subpart E.
2. "Breach Notification Rule" means the final regulatory provisions set forth at 45 C.F.R., Parts 160 and 164, Subparts A and D.
3. "CMS" means the Center for Medicare and Medicaid Services.
4. "Covered Entity Client" shall mean each of LSC's clients that qualifies as a "Covered Entity" under 45 C.F.R. § 160.103.
5. "Designated Record Set" shall have the meaning as the term is defined in 45 C.F.R. § 164.501.
6. "Downstream Entity" means any party that enters into an agreement with a Delegated Entity or with another Downstream Entity for purposes of providing administrative or health care services related to the agreement between the Delegated Entity and the QHP Issuer. The term Downstream Entity is intended to reach the entity that directly provides administrative services or health care services to qualified individuals, qualified employers, or qualified employees and their dependents.
7. "Electronic PHI" means information that comes within paragraphs 1(i) or 1(ii) of the definition of PHI as defined in 45 C.F.R. § 160.103, limited to the information created or received by Supplier from or on behalf of LSC.

8. "Exchange" means a governmental agency or non-profit entity that meets the applicable standards of 45 C.F.R. §155, subpart D and makes QHPs (as defined below) available to individuals and employers. This term includes both state and Federally-facilitated Exchanges
9. "GLBA" means the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) and the regulations promulgated from time to time thereunder.
10. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the final regulations promulgated by the U.S. Department of Health and Human Services from time to time thereunder.
11. "HITECH" means the Health Information Technology for Economic and Clinical Health Act as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 and the final regulations promulgated by the U.S. Department of Health and Human Services from time to time thereunder.
12. "Individual" has the same meaning as the term "individual" in 45 CFR § 160.103 and shall include persons who qualify as a personal representative in accordance with 45 C.F.R. § 164.502(g).
13. "Massachusetts Data Security Law" means Massachusetts General Law Chapter 93H and the regulations promulgated from time to time thereunder.
14. "Personal Information" means any non-public information - whether in paper or electronic form supplied by LSC that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, address, social security number, driver's license or state identification card number, insurance policy number, financial or credit or account numbers (with or without any required security code, access code, personal identification number or password) or any other non public personally identifiable information as defined by any Privacy Law .
15. "Privacy Laws" means HIPAA, HITECH, GLBA, the Massachusetts Data Security Law, the Privacy Principles and any other applicable privacy or data security laws, rules or regulations.
16. "Privacy Rule" means the final federal privacy regulations issued pursuant to HIPAA, as amended from time to time, codified at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
17. "Privacy Principles" means the EU-U.S. Privacy Shield Framework Principles issued by the U.S. Department of Commerce, the text of which may be available at ec.europa.eu/justice/data-protection/files/privacy.
18. "Protected Health Information" or "PHI" shall have the same meaning as the term "PHI" in 45 C.F.R. § 164.103, limited to the information created or received by Supplier from or on behalf of LSC.
19. "Qualified Health Plan" or QHP means a health plan that has been certified that it meets the standards described in 45 C.F.R. § 156, subpart C, or that has been approved by the state Exchange through which such plan is offered.
20. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
21. "Security Rule" means the final federal security regulations issued pursuant to HIPAA as amended from time to time, codified at 45 C.F.R. Part 160 and Part 164, Subparts A and C.

22. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by guidance issued by the Secretary of the Department of Health and Human Services (the "Secretary").

All terms used in these Specifications that are not otherwise defined herein have the same meaning as those terms under the Privacy Laws. A reference in these Specifications to a section in a Privacy Law means the section as in effect or as amended from time to time.

3. Purpose

LSC has certain obligations under Privacy Laws with regard to Personal Information and PHI that LSC receives from its clients or owns or licenses, and has agreed with its clients or is otherwise required under Privacy Laws to maintain an agreement with each agent or subcontractor that has or will have access to the Personal Information or PHI. These Specifications set forth the parties' agreement with respect to applicable provisions of (i) the privacy and security requirements of the Privacy Laws, and (ii) with respect to the applicable Medicare Advantage and Medicare Part D regulatory requirements described in Section 7 below.

4. Minimum Necessary

Supplier agrees to limit, to the extent practicable and except as permitted by 45 C.F.R. § 164.502(b)(2), its uses and disclosures of, and its requests for, PHI and other Personal Information under these Specifications to de-identified PHI (as defined in 45 C.F.R. § 164.514(b)) or, if de-identified PHI is not sufficient for Supplier's purpose, to the minimum necessary PHI or other Personal Information to accomplish the intended purpose of such use, disclosure or request.

5. Obligations of Supplier

1. *Permitted Uses and Disclosures.*

i. *Use and Disclosure.* Supplier may use or disclose PHI or other Personal Information only to provide services to LSC under the Agreement. Supplier is not authorized to use or further disclose PHI in a manner that would violate the Privacy Rule if done by a Covered Entity Client or by LSC on behalf of a Covered Entity Client. Notwithstanding any other provision of these Specifications, Supplier may use and disclose PHI or other Personal Information for the proper management and administration of the Supplier or to carry out the legal responsibilities of the Supplier, provided that any such disclosures are either Required By Law or Supplier obtains reasonable assurances from the recipient of such information that the information 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 recipient and the recipient will notify Supplier of any instances of which the recipient is aware in which the confidentiality of the information has been breached. Supplier may not use or disclose PHI or other Personal Information other than as permitted or required by these Specifications or as Required by Law.

ii. *Safeguards.* At any and all times during which Supplier is processing PHI or other Personal Information, or otherwise having access to such PHI or other Personal Information, it will develop, implement and maintain safeguards, documented in writing, to prevent the use or disclosure of PHI or other Personal Information other than as provided by the Privacy Rule and these Specifications, and will comply, where applicable, with the Security Rule with regard to Electronic PHI. Such safeguards shall include, but not be limited to, provisions to: (i) ensure the

security and confidentiality of PHI and other Personal Information; (ii) protect against the use or disclosure of PHI or other Personal Information other than as provided for in these Specifications, (iii) protect against any anticipated threats or hazards to the security or integrity of PHI or other Personal Information; (iv) protect the confidentiality, integrity, and availability of Electronic PHI or other electronic Personal Information that it receives, maintains or transmits on behalf of LSC, and (v) protect against unauthorized access to or use of PHI or other Personal Information. Supplier shall comply with Mass. 201 CMR 17.03 and 17.04, as such regulations are amended from time to time.

iii.*Privacy Principles.* In connection with Supplier's processing of Personal Information that is subject to the Privacy Principles:

1. Supplier will (i) provide at least the same level of privacy and data security protection as is required under the Privacy Principles and (ii) process such Personal Information only to perform the Services under Supplier's contract with LSC or as otherwise instructed by LSC;
2. If Supplier determines that it is unable to protect such Personal Information in accordance with the Privacy Principles, it will (i) immediately notify LSC; (ii) immediately cease processing such Personal Information, (iii) take reasonable and appropriate steps to remediate such inability, and (iv) immediately notify LSC upon such remediation; and
3. Without the prior consent of LSC, Supplier will not disclose or otherwise transfer any Personal Information that is subject to the Privacy Principles (i) outside of the United States, or (ii) to any third party, except as required by applicable law or court order.

iv.*Suppliers and Agents.* Supplier shall (1) ensure that any third party, including an agent or subcontractor, to whom it provides PHI or other Personal Information received from, or created or received by Supplier on behalf of, LSC agrees, in writing, to at least same restrictions and conditions that apply through these Specifications to Supplier with respect to such information and (2) be liable for the acts or omissions of any such party.

v.*Internal Practices.* Supplier agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI and Personal Information received from, or created or received by Supplier on behalf of, LSC available to LSC, its client(s) and government agencies for purposes of determining compliance with a Privacy Law.

vi.*Accounting for Disclosures.* Supplier agrees to document any disclosures of PHI or Personal Information by Supplier, including documentation required by 45 C.F.R. § 164.528. Within three (3) business days of notice by a client, LSC or a government agency, Supplier shall make available to LSC or, at LSC's request, the client or government agency such information as is in Supplier's possession.

vii.*Access to PHI and Personal Information.* Within three (3) business days of a request by LSC, a client or government agency for access to PHI or Personal Information about an individual contained in a Designated Record Set, Supplier shall make available to LSC or, at LSC's request, the client or government agency, such PHI or Personal Information. Supplier will: (1) immediately notify LSC of any request by a data subject to exercise any right with respect to Personal Information, including the right to access, correct, amend or delete such Personal Information; (2) at the direction of LSC, cooperate and assist LSC in responding to any such data subject request; and (3) upon LSC's request, correct, amend, delete or take any other action with respect to Personal Information. As between LSC and Supplier, LSC shall be responsible for determining whether to deny access to the PHI or Personal Information and Supplier shall comply with such determinations. If Supplier maintains any PHI in a Designated Record Set electronically, and LSC requests an electronic copy of such PHI, Supplier will provide an

electronic copy in the form and format requested by LSC, if feasible. If it is infeasible for Supplier to provide an electronic copy in the form and format requested by LSC, Supplier will provide a readable electronic copy of such PHI in a form and format as agreed by Supplier and LSC.

viii. *Amendments.* Supplier agrees to make any amendment to PHI or Personal Information in a Designated Record Set, as requested by the client or LSC.

ix. *Carrying Out Covered Entity Client Obligations.* To the extent Supplier is to carry out a Covered Entity Client's obligations under the Privacy Rule; or (b) LSC's obligations on behalf of a Covered Entity Client under the Privacy Rule, Supplier will comply with the requirements of the Privacy Rule that apply to the Covered Entity Client in the performance of such obligations.

2. *Notification of Breach.* With the exception of law enforcement delays that satisfy the requirements under 45 C.F.R. § 164.412 or as otherwise required by applicable Privacy Laws, Supplier agrees to promptly report to LSC any Breach of Personal Information or Unsecured PHI and in no case later than five (5) calendar days after discovery of a Breach in accordance with the applicable Privacy Laws. Supplier's notification of a Breach under this section shall include, to the extent known:

.the identification of each Individual whose PHI or other Personal Information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach;

i. a brief description of what happened, including the dates of the Breach and discovery of the Breach, if known;

ii. the scope of the Breach, including a description of the types of PHI or Personal Information involved; and

iii. a description of Supplier's response to the Breach.

Supplier shall provide any additional information concerning the Breach as reasonably requested by LSC. Supplier will also assist and cooperate with LSC with any necessary or appropriate disclosures and other investigative, remedial and monitoring measures as a result of the Breach, including but not limited to notification to affected individuals or regulating authorities as may be required by law. At the direction of LSC, Supplier shall provide such notifications in accordance with the Breach Notification Rule and applicable state law and/or pay for the reasonable and actual costs associated with LSC's provision of those notifications, any remediation, and LSC's legal fees. Supplier further agrees to immediately report to LSC any Security Incident of which it becomes aware.

3. *Mitigation.* Supplier shall mitigate, to the greatest extent reasonably possible, any deleterious effects from any Breach of Personal Information or Unsecured PHI, any Security Incident or any other improper use or disclosure of PHI or Personal Information.

4. *Training.* Supplier represents that all employees, agents, representatives, and work force members whose services are used to fulfill obligations under these Specifications or the underlying agreement are appropriately trained in order to satisfy the terms of these Specifications.

5. *Business Associate Agreements.* Notwithstanding the previous provisions, Supplier also shall be bound by the restrictions, terms, and conditions of the business associate agreements that LSC has entered into with Covered Entity Clients and that are provided to Supplier under these Specifications. Upon request (and approval by applicable Covered Entity Clients), LSC shall provide copies of the applicable business associate agreements(s) into which LSC has entered, that apply to Supplier's work under these Specifications, including any new business associate agreements LSC may enter following the execution and delivery of these Specifications, and all the provisions of all such agreements shall be automatically incorporated into these Specifications.

Where any business associate agreement requires LSC to take action within a certain time frame and such action would require Supplier to notify or respond to LSC in order for LSC to fulfill its obligations to any Covered Entity Client, Supplier shall promptly notify or respond to LSC to enable LSC to meet its obligations.

6. *Disclosure for Remuneration.* Supplier shall not directly or indirectly receive remuneration in exchange for disclosing PHI received from LSC, or created or received by Supplier on behalf of LSC. Supplier shall not disclose PHI received from LSC, or created or received by Supplier on behalf of LSC, for marketing purposes.

6. Information Security Requirements.

1. *Duty to Protect and Standards for Protecting PHI and Personal Information.* Supplier shall comply with all Privacy Laws that govern the privacy or security of Personal Information, including but not limited to, the Security Rule, the Privacy Principles and the requirements set forth in the Massachusetts 201 CMR 17.03 and 17.04. Supplier shall implement a written comprehensive information security program which shall include but is not limited to the following:

- .Designating one employee as the Security Official, to develop and maintain the comprehensive information security program;
- i. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing Personal Information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks.
- ii. Developing security policies for employees relating to the storage, access and transportation of records containing PHI or Personal Information inside and outside of business premises.
- iii. Imposing disciplinary measures for violations of the comprehensive information security program rules.
- iv. Preventing terminated employees from accessing records containing Personal Information.
- v. Reasonable restrictions upon physical access to records containing Personal Information and storage of such records and data in locked facilities, storage areas or containers.
- vi. Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Personal Information; and upgrading information safeguards as necessary to limit risks.
- vii. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices or environment that may reasonably implicate the security or integrity of records containing Personal Information.
- viii. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Personal Information.

2. *Computer System Security Requirements.* Supplier shall include in its information security program a computer security system that complies with the Security Rule, including but not limited to the following elements:

.Secure user authentication protocols including:

1. control of user IDs and other identifiers;
2. a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
3. control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

4. restricting access to active users and active user accounts only; and
5. blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
 - i. Secure access control measures that:
 1. restrict access to records and files containing Personal Information or PHI to those who need such information to perform their job duties; and
 2. assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
 - ii. Encryption of all PHI and Personal Information at rest and during transmission, using an encryption methodology or technology approved by the Secretary.
 - iii. Reasonable monitoring of systems, for unauthorized use of or access to Personal Information;
 - iv. For files containing Personal Information or PHI on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Personal Information.
 - v. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
 - vi. Education and training of employees on the proper use of the computer security system and the importance of Personal Information and PHI security.

7. Medicare Advantage, Medicare Part D and Qualified Health Plan Regulatory Compliance.

Certain services provided by Supplier may be subject to regulatory requirements applicable to Medicare Advantage plans, Medicare Part D plans, and Qualified Health Plan ("QHP") issuers and their delegated and downstream entities pursuant to Title XVIII of the Social Security Act and any subsequent amendments or relevant regulations promulgated thereto ("Medicare Regulations"), and/or the Patient Protection and Affordable Care Act ("ACA") and any subsequent amendments or relevant regulations promulgated thereto ("ACA Regulations"). To the extent that Supplier provides Services that are subject to Medicare or ACA Regulations, the following shall apply:

1. *Fraud, Waste and Abuse Training.* In accordance with, but not limited to 42 C.F.R. § 423.504(b)(4)(vi)(C)&(D) and 42 C.F.R. § 422.503(b)(4)(vi)(C)&(D) (and corresponding subregulatory guidance), Supplier agrees and certifies that it, as well as its agents and subcontractors that provide services under the underlying agreement ("Supplier Personnel") shall participate in annual fraud, waste and abuse compliance training and implement effective lines of communicating compliance issues as requested by LSC or its customers, or as otherwise required by applicable law. Such training shall be required for any new Supplier Personnel that are involved in the performance of any services under the underlying agreement within 90 days of initial hire or contracting and annually thereafter.

Training options. Suppliers may satisfy the training requirement in one of two ways: (1) Completion of the general compliance and/or FWA training modules located on the CMS Medicare Learning Network (MLN). Once the individual completes the training module, the system will generate a certificate of completion. Or, (2) Incorporation of the CMS standardized training modules into the organization's existing compliance training materials/systems. If

Supplier chooses option 2, CMS training content must not be modified. However, Supplier can add to the CMS training to cover topics specific to their organization

i. *Training documentation.* Supplier must maintain certificates or documentation of training completion and will furnish a certificate of training such as certificates of completion, training logs, system generated reports, spreadsheets, etc. upon request by LSC, its customers or the Department of Health and Human Services ("HHS"). Documentation of training completion such as training logs, reports, etc. must include at minimum employee names, dates of employment, dates of completion, and passing scores (if captured) to clearly document training completion.

2. *Background Checks.* Supplier certifies that neither it nor any of its Supplier Personnel that perform services under the underlying agreement are listed on either the Office of Inspector General, HHS or the General Services Administration exclusion list. Supplier shall immediately notify LSC if any Supplier Personnel are excluded by a state or federal health care program. At least monthly (or as otherwise required by LSC, its customers or HHS), Supplier shall, upon request, perform and document (or shall allow LSC to perform and document) appropriate background checks of applicable Supplier Personnel to ensure compliance with this requirement.

3. *Inspection of Books and Records; Record Retention.* In accordance with, but not limited to, 42 C.F.R. § 422.504(i) and/or 42 C.F.R. § 423.505(i) and/or 45 C.F.R. § 156.340, Supplier acknowledges that LSC, LSC's customers, HHS, the Comptroller General or their designees have the right to timely inspect, evaluate and audit Supplier and/or certain Supplier books, records, computers and other electronic systems related to the underlying agreement or services provided under the underlying agreement. Such audit rights shall continue for a period of ten (10) years from termination of the underlying agreement or the date of the completion of any audit, whichever is later or for such longer period to the extent required by 42 C.F.R. § 422.504(e)(4) and/or C.F.R. § 422.505(e)(4) and/or 45 C.F.R. § 156.340(b)(4) or other applicable law, and Supplier shall maintain all applicable books and records in accordance thereto. Supplier shall produce upon request by HHS, or its designees, any books, contracts, or records relating to the Part D program, to either the Part D sponsor to provide to CMS, or directly to CMS or its designees.

4. *Compliance with Medicare Law.* Supplier shall comply with all applicable federal laws, regulations, and CMS instructions as well as all applicable state and federal laws and regulations including, but not limited to the provisions of 45 C.F.R. Parts 155 and 156, to the extent relevant in performing its duties and obligations on behalf of LSC or its customers.

5. *Automatic Amendment.* Supplier agrees to include in these Specifications such other terms and conditions as CMS may find necessary and appropriate in order to implement Medicare Regulations.

6. *Consistency with CMS Contracts.* The parties agree that the services performed by Supplier are consistent with and comply with the contractual obligations of Medicare Advantage plans, Part D plan sponsors and QHP issuers under their contracts with CMS.

7. *Freedom from Conflict of Interests.* As required by LSC's customers, Supplier shall require their managers, officers and directors responsible for the administration of Part D benefits to sign a conflict of interest statement, attestation or certification at the time of hire and annually thereafter certifying that the individual is free from any conflict of interest in administering or delivering Part D benefits.

8. *Qualified Health Plan Regulatory Compliance.* Vendor shall include in its contract with any Downstream Entities, and require such Downstream Entities to include in their contracts with other Downstream Entities, language that is the same or substantially similar to that contained in these Specifications, and which expressly requires each Downstream Entity to:

- .Comply with all applicable state and federal laws and regulations, including but not limited to the provisions of 45 C.F.R. Parts 155 and 156, to the extent relevant, in performing or assisting in the performance of the duties and obligations set forth in these Specifications; and
- i.Grant access to its books, contracts, computers, or other electronic systems (including medical records and documentation), relating to such downstream entity's compliance with applicable provisions under 45 C.F.R. Parts 155 and 156 in connection with the duties and obligations set forth in these Specifications, to HHS and its Office of Inspector General (or their designees), for the duration of the period in which these Specifications is effective, and for a minimum of ten (10) years from the date these Specifications terminate.

8. **Term and Termination**

1. *Term.* The Term of these Specifications shall be effective as of the Agreement's Effective Date and shall terminate when all of the PHI and Personal Information provided by LSC to Supplier or created or received by Supplier on behalf of LSC is destroyed or returned to LSC.
 2. *Termination for Cause.* Without limiting the termination rights of the parties pursuant to the Agreement, upon either party's knowledge of a violation of a material term of these Specifications by the other party, the non-breaching party may either: (a) provide an opportunity for the breaching party to cure the breach or end the violation, or terminate the underlying agreement, if the breaching party does not cure the breach or end the violation within five (5) business days of notice of breach by the non-breaching party; or (b) immediately terminate these Specifications (and Agreement), if cure is not reasonably possible.
 3. *Effect of Termination.*
 - .Except as permitted by subsection (ii) below, upon termination of the Agreement for any reason, Supplier shall return or destroy all PHI or other Personal Information received from LSC, or created or received by Supplier on behalf of LSC which Supplier still maintains in any form. This provision shall apply to PHI or other Personal Information that is in the possession of subcontractors or agents of Supplier. Supplier shall retain no copies of the PHI or Personal Information.
 - i.In the event that returning or destroying the PHI or other Personal Information is infeasible, Supplier shall notify LSC in writing and may retain the PHI subject to this Subsection 8.c.2. and LSC's approval. Supplier shall extend the protections of these Specifications to such PHI or other Personal Information and limit further uses and disclosures of such PHI or other Personal Information to those purposes that make the return or destruction infeasible, for so long as Supplier maintains such PHI or other Personal Information.
 4. *Compliance with these Specifications.* Compliance with the terms of these Specifications is a material term of the underlying agreement and any and all agreements pursuant to which LSC is making available PHI and other Personal Information to Supplier. Breach of these Specifications shall constitute a default by Supplier under the underlying agreement and any and all other agreements between the parties and shall give rise to LSC's immediate right to terminate the Agreement and such other agreements.
9. **Indemnification.** Supplier shall indemnify, defend and hold LSC harmless against any and all claims, liabilities, losses, damages, costs or expenses, including reasonable attorneys' fees and legal expenses incurred by LSC as a result of Supplier's violation of these Specifications or any Privacy Laws or Breach of Unsecured PHI.

10. **Miscellaneous**

1. *Amendment.* LSC may amend these Specifications at any time to comply with the requirements of Privacy Laws, as they may be amended from time to time, and any implementing

regulations thereto that may be promulgated or revised from time to time. The governing version of these Specifications shall be the version in effect at the time services are provided by Supplier. LSC shall retain copies of all versions of these Specifications during the term of the Agreement and records showing the effective dates of each version.

2. *Survival.* The obligations of Supplier under these Specifications shall survive the termination of these Specifications.

3. *Entire Agreement.* These Specifications and the Agreement embody and constitute the entire agreement and understanding between the parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitments, and understandings pertaining to the subject matter hereof.

4. *Conflict.* In the event of any conflict between these Specifications and the Agreement as to the subject matter referenced herein, these Specifications shall control.

5. *No Assignment.* Supplier may not assign its rights and obligations under these Specifications without the prior written consent of LSC.