

APPENDIX E

BACKGROUND CHECK AND DATA PROCESSING REQUIREMENTS

BACKGROUND CHECK REQUIREMENTS

If the Candidate will have access to Authorized User data, data centers, or as otherwise determined by the Authorized User to be necessary, the Contractor and Candidate shall, prior to the commencement of any services pursuant to Request for Proposal (RFP) #23111, whether on or off-site, comply with all Authorized User onboarding and security clearance requirements, including training and signing certifications or agreements, required for access to Authorized User confidential information or data or required for access to Authorized User facilities or data centers, the preceding described, collectively, as "onboarding." This includes requirements related to the access to regulated data, including any requirements of New York State's public safety agencies, or those related to the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy (<https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>).

Contractor agrees that its Candidates performing services on-site at Authorized User facilities or data centers or those with logical access to Authorized User confidential information or data (i.e., log-in access) shall be required to undergo the same security clearances as those required of an Authorized User's employees. If not physically or virtually escorted, each Candidate designated to work under the Authorized User Agreement shall submit identifying information to the State and be fingerprinted. The Authorized User shall arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for a state criminal history record check and, at the Authorized User's discretion, to the Federal Bureau of Investigation for a national criminal history record check.

Contractor also agrees that its Candidates performing services on-site at Authorized User facilities or data centers may be required to comply with those health checks which the Authorized User requires of its own employees working on-site including for example providing proof of vaccination against, and/or testing for, infectious disease such as COVID-19.

Travel, lodging, and related expenses associated with the onboarding and security clearance process and fingerprinting of Candidates, are the responsibility of the Contractor and are not reimbursable.

The Authorized User shall make all suitability determinations on Candidates. For purposes of this Appendix, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Authorized User Agreement requirements without undue risk to the interests of the Authorized User or State. Failure of a security clearance or non-compliance with these requirements will disqualify any Candidate from performing any services on the Authorized User Agreement. If any Candidate is removed from providing services under the Authorized User Agreement, they may be subject to all onboarding and security clearance requirements if they are returned to performing services under the Authorized User Agreement.

All Candidates shall, at the termination of their providing services to the Authorized User under this RFP, comply with all Authorized User off-boarding and security procedures, including return to the Authorized User of any physical or logical access badges or other credentials that were issued by the Authorized User and required for their access to Authorized User confidential information or data or Authorized User facilities or data centers.

REGULATED DATA PROCESSING REQUIREMENTS

The Contractor agrees to comply with the following requirements for those data types indicated on Form 1: Task Order Request Form.. For the indicated data types, the following provisions shall be incorporated in and deemed a part of the task order, as applicable. OGS reserves the right to update Appendix E on a prospective basis on notice to Contractor in order to comply with the requirements of applicable laws, policies, rules or regulations.

1. CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

The Contractor agrees to comply with all requirements in the most recent approved version Criminal Justice Information Services (CJIS) Security Policy, available at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view> and the terms of this CJIS Security Addendum below.

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.1. Definitions

- a. “Contracting Government Agency (CGA)” - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.
- b. “Contractor” - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

1.2. Responsibilities of the Contracting Government Agency

The CGA will ensure that each Candidate receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

1.3. Responsibilities of the Contractor

The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

1.4. Security Violations

The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

- a. Security violations can justify termination of the appended agreement.
- b. Upon notification, the FBI reserves the right to:
 1. Investigate or decline to investigate any report of unauthorized use;
 2. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

1.5. Audit

The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum

1.6. Scope and Authority

This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

- a. The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
- b. The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
- c. This Security Addendum may only be modified by the FBI and may not be modified by the parties to the appended Agreement without the consent of the FBI.
- d. All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

2. SAFEGUARDING FEDERAL TAX INFORMATION (FTI)

2.1. Performance

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by Candidates with the following requirements:

- a. All work will be performed under the supervision of the Contractor.
- b. The Contractor and Candidate to be authorized access to Federal Tax Information (FTI) must meet the background check requirements defined in IRS Publication 1075. The Contractor will maintain a list of Candidates authorized access to FTI. Such list will be provided to the Authorized User and, upon request, to the IRS.

- c. FTI made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure of FTI to anyone other than the Contractor or Contractor Staff authorized is prohibited.
- d. All FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products will be given the same level of protection as required for the source material.
- e. The Contractor will certify that the FTI processed during the performance of this Contract will be completely purged from all physical and electronic data storage with no output to be retained by the Contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the Contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- f. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the Authorized User. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the Authorized User with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- g. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- h. No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.
- i. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- j. To the extent the terms, provisions, duties, requirements, and obligations of this Contract apply to performing services with FTI, the Contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the Authorized User under this Contract assumes toward the Contractor, and the subcontractor shall assume toward the Contractor all the same obligations, duties and responsibilities which the Contractor assumes toward the Authorized User under this Contract.
- k. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this Contract apply to the subcontractor, and the subcontractor is bound and obligated to the Contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the Authorized User under this Contract.
- l. For purposes of this contract, the term "Contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "Subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
- m. The Authorized User will have the right to void the Contract if the Contractor fails to meet the terms of FTI safeguards described herein.

2.2. Criminal/Civil Sanctions

- a. Each Candidate of a Contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such Candidate can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
- b. Each Candidate of a Contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such Candidate may be accessed only for a purpose and to

the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

- c. Each Candidate of a Contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the Candidate in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- d. Additionally, it is incumbent upon the Contractor to inform its Candidate of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of their employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- e. Granting a contractor access to FTI must be preceded by certifying that each Candidate understands The Authorized User's security policies and procedures for safeguarding FTI. The Contractor and Candidate must maintain their authorization to access FTI through annual recertification of their understanding of the Authorized User's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the Authorized User's files for review. As part of the certification and at least annually afterwards, the Contractor and each Candidate must be advised of the provisions of IRC sections 7213, 7213A, and 7431. The training on the Authorized User's security policies and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the Contractor and each Candidate must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

2.3. Inspection

The IRS and the Authorized User, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit FTI. Based on the inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with FTI safeguard requirements.

3. COMPLIANCE WITH HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), HI-TECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT OF 2009), AND OTHER HEALTH INFORMATION PRIVACY AND SECURITY LAWS

3.1. Definitions

The following terms used in this Section shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

- a. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in this Section may refer to Contractor or its Subcontractor(s), to the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of the Authorized User.
- b. "Covered Entity". By entering into the Contract, the Authorized User does not affirm that it necessarily meets the definition of a "Covered Entity" or a "Business Associate" under the HIPAA statute and rather affirms that the Authorized User may in a given instance be acting as a "conduit" or in another capacity providing services to other entities, some of which themselves may be covered entities. But to the extent the Authorized User is deemed to be covered by HIPAA or HI-TECH, the Parties agree the term "Covered Entity" in this Section shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.
- c. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- d. "Medicaid Confidential Data" (MCD) includes all information about a Medicaid recipient or applicant, including enrollment information, eligibility data and protected health information. The NYS Department of Health (DOH) is the Single State Agency responsible for the administration of the New York State Medicaid program in New York State, including ensuring the security and confidentiality of MCD data.

3.2. HIPAA Protected Health Information Obligations and Activities of Contractor

To the extent Contractor or its Subcontractor(s) create, receive, maintain, or transmit protected health information on behalf of the Authorized User pursuant to their responsibilities under the Contract, Contractor agrees that it is subject to, will abide by, and will require in writing its Subcontractors to similarly abide by, the following requirements applicable to Business Associates under HIPAA, agreeing to:

- a. Not use or disclose protected health information other than as permitted or required by the Contract or as required by law;
- b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Contract;
- c. Report to the Authorized User within ten (10) business days or fewer any use or disclosure of protected health information not provided for by the Contract of which it becomes aware. In no event shall Contractor exceed the timeframe for reporting to the Authorized User breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Contractor shall provide the Authorized User all information reasonably requested by the Authorized User concerning any breach. Contractor shall also provide the following information to the Authorized User upon first instance of the notification of breach: the identification of each individual whose unsecured protected health information has been, or is reasonably believed by Contractor, to have been, accessed, acquired, used, or disclosed during the breach.
- d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of Contractor agree in writing to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information;
- e. Make available protected health information in a designated record set to the Authorized User, in a manner to be prescribed by the Authorized User within a reasonable timeframe

not to exceed fifteen (15) days, absent extenuating circumstances, as necessary to satisfy obligations which the Authorized User or the entities it provides services to reasonably believe applicable to them under 45 CFR 164.524. In the event Contractor or its Subcontractor(s) receive any request for such protected health information directly from an individual, Contractor shall refer such request to the Authorized User within a reasonable timeframe not to exceed ten (10) business days.

- f. Make any amendment(s) to protected health information in a designated record set as directed by the Authorized User pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy obligations that the Authorized User reasonably believes it has under 45 CFR 164.526, in the manner as prescribed by the Authorized User and within twenty (20) business days of such request. In the event Contractor or its Subcontractor(s) receive any request to amend a data set directly from an individual, Contractor shall refer such request to the Authorized User within a reasonable timeframe not to exceed ten (10) business days;
- g. Maintain and make available the information required to provide an accounting of disclosures to the Authorized User as necessary to satisfy obligations that the Authorized User reasonably believes it has under 45 CFR 164.528, in the manner as prescribed by the Authorized User and within ten (10) business days of such request. In the event Contractor or its Subcontractor(s) receive any request for an accounting of disclosures directly from an individual, Contractor shall refer such request to the Authorized User within a reasonable timeframe not to exceed ten (10) business days;
- h. To the extent Contractor or its Subcontractor(s) are to carry out one or more of obligation(s) the Authorized User may have under Subpart E of 45 CFR Part 164, in performing such obligations, comply with the requirements of Subpart E that apply to the Authorized User; and
- i. Make either Contractor's or its Subcontractor(s)', or Both's internal practices, books, and records available to the Secretary of the Department of Health and Human Services and to the Authorized User, for purposes of determining compliance with the HIPAA and HI-TECH Rules.

3.3. Permitted Uses and Disclosures of Protected Health Information by Contractor and its Subcontractor(s)

- a. Contractor and its Subcontractor(s) may only use or disclose protected health information as necessary to perform the services set forth in the Contract, provided however, that if de-identified information can be used in lieu of individually identifiable health information with the same effect, Contractor and its Subcontractor(s) shall use de-identified information in their performance of the Contract in accordance with 45 CFR 164.514(a)-(c).
- b. Contractor and its Subcontractor(s) may use or disclose protected health information as required by law.
- c. Contractor and its Subcontractor(s) agrees to make only those uses, disclosures and requests for protected health information that are consistent with the minimum necessary policies and procedures of the Authorized User or the entit(ies) for whom the Authorized User provides services which entail the creation, reception, maintenance, or transmittal of protected health information.
- d. Contractor and its Subcontractor(s) may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 except as may be provided for in the Contract or for the proper management and administration of Contractor or its Subcontractor(s), including the carrying out of the Contractor's or its Subcontractor(s)' legal responsibilities.

3.4. Other Health Information Obligations and Activities of Contractor

Contractor or its Subcontractor(s) may not disclose other types of health information protected by federal, State or local law including but not limited to personally identifiable mental health information protected under NYS Mental Hygiene Law §33.16, other personally identifiable health information or HIV information protected under NYS Health Law sections §18 or Article 27-F, or substance abuse information protected under federal regulations 42 CFR Part 2.

Contractor or its Subcontractor(s) may not disclose Medicaid Confidential Data without the prior written approval of the New York State Department of Health (DOH), either directly or as provided to Contractor or its Subcontractor(s) through the Authorized User. If contacted by DOH, while also informing the Authorized User, Contractor or its Subcontractor(s) shall reasonably work with DOH to identify any individuals who may have inappropriately or unlawfully accessed Medicaid Confidential Data. Contractor agrees to ensure that Contractor and any agent, including a Subcontractor, to whom Contractor provides Medicaid Confidential Data, agrees to the same restrictions and conditions that apply throughout the Contract. Further, Contractor agrees to state in any such agreement, contract or document that the party to whom Contractor is providing the Medicaid Confidential Data may not further disclose it without the prior written approval of the New York State Department of Health. Contractor agrees to include the notices preceding, as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Contractor enters into that involves Medicaid Confidential Data.

The federal Center for Medicare and Medicaid Services (CMS) requires that all contracts and/or agreements executed between the Department of Health and any second party that will receive Medicaid Confidential Data must include contract language that will bind such Parties to ensure that contractor(s) abide by the regulations and laws that govern the protection of individual, Medicaid confidential level data.

Medicaid Confidential Data includes all information about a recipient or applicant, including enrollment information, eligibility data and protected health information.

Contractor must comply with the following State and federal laws and regulations:

- Section 367b(4) of the NY Social Services Law
- New York State Social Services Law Section 369 (4)
- NYS Mental Hygiene Law §33.16,
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1
- Social Security Act, 42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Please note that Medicaid Confidential Data released to Contractor may contain AIDS/HIV related NYS Confidential Information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Contractor:

“This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure.”

3.5. Alcohol and Substance Abuse Related Confidentiality Restrictions

Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

3.6. Term and Termination

- a. Termination for cause under HIPAA or HI-TECH. The Term of this Section shall be as described elsewhere in the "Term" section of the Contract. Among the other reasons for which ITS may terminate the Contract prior to the end of its Term date for cause, the Authorized User may terminate the Contract if the Authorized User determines the Contractor or its Subcontractor(s) have violated a material term of this HIPAA and HI-TECH Compliance Section of the Contract, and Contractor or its Subcontractor(s) have not cured the breach or ended the violation within any time that has been specified by the Authorized User.
- b. Contractor's and its Subcontractor(s)' Obligations Upon Termination. Upon termination of the Contract for any reason, Contractor and its Subcontractor(s) shall return to the Authorized User, transfer to another of the Authorized User's contractors as directed by the Authorized User, or, if agreed to by the Authorized User on an individual case-by-case basis, destroy all protected health information received from the Authorized User, or created, maintained, or received by the Contractor and its Subcontractor(s) on behalf of the Authorized User, that the Contractor and its Subcontractor(s) still maintain in any form. Contractor and its Subcontractor(s) shall retain no copies of the protected health information. Contractor understands and agrees and will require of its Subcontractor(s) in writing that Contractor and its Subcontractor(s) are required to receive written approval from the Authorized User prior to the return, transfer or destruction of any protected health information.
- c. Survival. Contractor's and its Subcontractor(s)' obligations under this HIPAA and HI-TECH Compliance section of the Contract shall survive the termination of the Contract.

3.7. Miscellaneous

- a. Regulatory References. A reference in the Contract to a section in the HIPAA or HI-TECH Rules means the section as in effect or as amended.
- b. Amendment. The Parties agree to take such action as is necessary to amend the Contract from time to time as is necessary for compliance with the requirements of the HIPAA or HI-TECH Rules and any other applicable law.
- c. Interpretation. Any ambiguity in the Contract shall be interpreted to permit compliance with the HIPAA or HI-TECH Rules.
- d. Sub-contractors. Contractor shall require any Subcontractors that it uses that create, receive, maintain, or transmit protected health information on behalf of the Authorized User under the Contract to conform to these HIPAA and HI-TECH Compliance requirements in addition to any other security, privacy or applicable terms of the Contract.