Foundation Medicine, Inc.
Subcontract Addendum A: FAR and Special Requirements
For Commercial Item Subcontracts

This Addendum supplements the terms and conditions of the agreement between Foundation Medicine, Inc. (FMI) and Subcontractor in support of U.S. Government Contract No. 36C10G19D0032 between FMI and the U.S. Department of Veterans Affairs (Government Contract).

A. General Provisions

Subcontract Reporting. Upon request by FMI, Subcontractor shall furnish to FMI all information that may be required for FMI to comply with the reporting requirements specified at FAR 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (OCT 2018).

Exclusions. If the agreement is valued in excess of $35,000, Subcontractor represents that, as of the effective date of this agreement, neither the Subcontractor nor its subcontractor(s), nor any of the Subcontractor's or its subcontractor(s)' respective principals, are debarred, suspended, or proposed for debarment by the U.S. Government. The Subcontractor must confirm this representation on the effective date of this agreement if the effective date occurs after the date on which the Subcontractor executes the agreement.

Small Business Status. Unless Subcontractor informs FMI otherwise in writing, Subcontractor represents that it does not qualify as a small business for U.S. Government procurement purposes.

U.S. Government Reporting. No confidentiality provision included in this agreement may be construed to prohibit or otherwise restrict the Subcontractor, as a subcontractor of FMI under a U.S. Government contract, from lawfully reporting waste, fraud, or abuse to a designated investigative or law enforcement representative of the federal department or agency authorized to receive such information under the procurement.

B. FAR and VAAR Clauses

Except as otherwise provided in this Addendum, or where a substitution of parties would not be reasonable in a specific clause due to the mutual expectation of the parties to this agreement, the following terms used in the FAR clauses incorporated by referenced in this Addendum shall have the following meanings:

1. "Contracting Officer" or "Government" shall mean FMI;
2. "Contractor" or "Offeror" shall mean the Subcontractor that is a party to this agreement;
3. "Contract" shall mean this agreement between FMI and Subcontractor;
4. "Subcontract" shall mean any lower-tier subcontract entered into by Subcontractor in furtherance of its contract with FMI; and
5. "Subcontractor" shall mean such lower-tier subcontractor engaged by Subcontractor to furnish supplies or services to the Subcontractor that is a party to this agreement.

1. Clauses Incorporated by Reference

The clauses referenced below are hereby incorporated by reference, with the same force and effect as if they were set out in full text, subject to the notes following each clause citation. Flowdown to lower-tier subcontractors is required as indicated in the instructions for "subcontracts" in each clause. The full text of each clause may be accessed electronically at http://www.acquisition.gov.

FAR Clause	Title of Clause	Date
52.203-11	Limitation on Payments to Influence Certain Federal Transactions (*applies if this Subcontract exceeds $150,000*)	Sep 2007
52.203-13	Contractor Code of Business Ethics and Conduct	Oct 2015

	(*applies if this Subcontract exceeds $5,500,000 and has a performance period of more than 120 days; the meaning of the terms "Government" and "Contracting Officer" are not changed*)	
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (*the meaning of the term "Government" is not changed)*	Jan 2017
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (*the meaning of the terms "Government" and "Contracting Officer" are not changed*)	Jul 2018
52.209-6	Protecting the Government's Interest when Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (*applies if this Subcontract exceeds $35,000 and is not for commercially available off-the-shelf items*)	Oct 2015
52.219-8	Utilization of Small Business Concerns (*must be included in in all lower-tier subcontracts that offer further subcontracting opportunities*)	Nov 2016
52.222–21	Prohibition of Segregated Facilities (*applies to the same extent as FAR 52.222-26*)	Apr 2015
52.222-26	Equal Opportunity (*applies unless exempted by the rules, regulations, or orders of the Secretary of Labor; an exemption applies if this Subcontract is (i) valued at $10,000 or less, unless the Subcontractor receives or can be expected to receive in a twelve-month period agreements covered by the clause valued at more than $10,000 in the aggregate or (ii) for work performed outside the United States with employees recruited outside the United States*) **FMI AND SUBCONTRACTOR SHALL, IF APPLICABLE, ABIDE BY THE REQUIREMENTS OF 41 CFR 60-1.4(a), 60-1.7, 60-1.35(c), 60-300.5(a), 60-741.5(a), AND 29 CFR PART 471, APPENDIX A, AS UPDATED FROM TIME TO TIME. AMONG OTHER REQUIREMENTS, THESE REGULATIONS PROHIBIT DISCRIMINATION AGAINST QUALIFIED PROTECTED VETERANS, QUALIFIED INDIVIDUALS ON THE BASIS OF DISABILITY, AND INDIVIDUALS ON THE BASIS OF RACE, COLOR, RELIGION, SEX, SEXUAL ORIENTATION, GENDER IDENTITY OR NATIONAL ORIGIN. THESE REGULATIONS REQUIRE THAT COVERED PRIME CONTRACTORS AND SUBCONTRACTORS TAKE AFFIRMATIVE ACTION TO EMPLOY AND ADVANCE IN EMPLOYMENT QUALIFIED PROTECTED VETERANS, QUALIFIED INDIVIDUALS WITH DISABILITIES, AND INDIVIDUALS WITHOUT REGARD TO THEIR RACE, COLOR, RELIGION, SEX, SEXUAL ORIENTATION, GENDER IDENTITY, OR NATIONAL ORIGIN.**	Sept 2016
52.222-35	Equal Opportunity for Veterans (*applies if this Subcontract is $150,000 or more, unless exempted by the rules, regulations, or orders of the Secretary of Labor; an exemption applies if this Subcontract is for work performed entirely outside the United States with employees recruited or transferred outside the United States*)	Oct 2015
52.222-36	Equal Opportunity for Workers with Disabilities (*applies if this Subcontract exceeds $15,000, unless exempted by the rules, regulations, or orders of the Secretary of Labor; an exemption applies if this Subcontract is for work performed entirely outside the United States with employees recruited or transferred outside the United States*)	July 2014
52.222–37	Employment Reports on Veterans (*applies if this Subcontract is $150,000 or more, unless exempted by the rules, regulations, or orders of the Secretary of Labor; an exemption applies if this*	Feb 2016

	Subcontract is for work performed entirely outside the United States with employees recruited or transferred outside the United States)	
52.222-40	Notification of Employee Rights Under the National Labor Relations Act (*applies if this Subcontract exceeds $10,000 and will be performed wholly or partially in the United States*)	Dec 2010
52.222-41	Service Contract Labor Standards (*applies if this Subcontract exceeds $2,500 and has a principal purpose of furnishing services at least in part in the United States through the use of service employees*; *the meaning of the terms "Government" and "Contracting Officer" are not changed*)	Aug 2018
52.222-50	Combating Trafficking in Persons (*FMI may take appropriate action against the Subcontractor, including termination of this Subcontract, for violation of paragraph (b); if a certification is required under paragraph (h)(5), the Subcontractor will submit the certification at FAR 52.222-56 before award and during performance of the Subcontract*)	Mar 2015
52.222-54	Employment Eligibility Verification (*applies if this Subcontract exceeds $3,500 and will be performed at least in part in the United States, unless this Subcontract is only for supplies or is for commercial services that are part of the purchase of a commercially available off-the-shelf ("COTS") item, or an item that would be a COTS item but for minor modifications, and the services are normally provided for that item*)	Oct 2015
52.222–55	Minimum Wages Under Executive Order 13658 (*applies to the same extent as FAR 52.222-41*)	Dec 2015
52.222–62	Paid Sick Leave Under Executive Order 13706 (*applies to the same extent as FAR 52.222-41*)	Jan 2017
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (*applies if Subcontractor is a small business concern*).	Dec 2013
VAAR Clause	**Title of Clause**	**Date**
852.237-7	Indemnification and Medical Liability Insurance *(applies if healthcare providers will be providing services under this Subcontract)*	Jan 2008

2. Special Requirements

The interpretive guidance provided above does not apply to the following provisions. Further, the following provisions are applicable to the extent Subcontractor is subject to HIPAA or has access to U.S. Government Department of Veteran Affairs information (including personally identifiable information).

B.6 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE

(a) As a covered entity, the VA is required to by law to obtain satisfactory assurance of a Business Associate that the Business Associate appropriately safeguards protected health information it receives or creates on behalf of the covered entity. Contractors and any Subcontractors must adhere to the provisions of Public Law 104-191, HIPAA to include the Administrative Simplification Provisions of the law and associated rules and regulations published by the Department of Health and Human Services (HHS). The Contractor shall comply with all HIPAA-related rules and regulations to include Electronic Transactions, the Standards for Privacy of Individually Identifiable Health Information, and the Security Standards. This includes both the Privacy and Security Rules published by HHS. As required by HIPAA, HHS has promulgated rules governing the use and disclosure of protected health information by covered entities. The covered entity component of the VA is the Veterans Health Administration (VHA). Business associates must follow VHA privacy policies and practices. All Contractors and business associates must receive privacy training annually. For Contractors and business associates who do not have access to VHA computer systems, this requirement is met by completing VHA National Privacy Policy training, other VHA approved privacy training or Contractor furnished training that meets the requirements of HHS Standards for Privacy of Individually Identifiable Health information as determined by VHA. For Contractors and business associates who are granted access to VHA computer systems, this requirement is met by completing VHA National Privacy Policy training or other VHA approved privacy training. Proof of training is required.

(b) Any violation of HIPAA will be reported to FMI in writing within one (1) business day of the Contractor's discovery of an occurrence. Included in the report will be a description of the occurrence, patient names (if known), location, date and time. A copy of any filed police report will be provided by the Contractor to FMI within one (1) business day of completion.

(c) Security must be designed into the system to protect patient information as required by HIPAA. All external network connects to the remote server shall be via encrypted SSL connects, VPN software and hardware. The process and method in which the transmission or routing of VA image data shall be reviewed and approved in accordance with form VA 6500.6. All patient information remains the sole property of the Government and shall not be used for any purpose other than those stipulated in this contract. The VAMCs shall act as primary custodian of the patient information (including both the image data and the report) for all purposes related to Government records retention requirements. Patient information, including images shall be retained by the Contractor only for the minimum period of time required to comply with any applicable laws, regulations, and the retention policies stated herein. Upon request, the Contractor shall provide the Government and FMI with access to information pertaining to the way the Contractor maintains NPOP/VAMC patient data and the steps taken on an ongoing basis to assure the privacy and security thereof. This includes information regarding computer network architecture, configuration of firewall(s), routers, and other pieces of networking equipment, information about installed security software, and audits of patches of known security vulnerabilities. All relevant security-related patches and anti-virus updates shall be installed with seven (7) days of initial release. Patient lists, no matter how developed, shall be treated as privileged information. Lists and names of patients shall not be disclosed or revealed in any way for any use outside this contract. Contractor must meet all VA required security restrictions and Contractor representatives shall undergo all HIPAA/confidentiality related training to comply with V15 requirements.

(d) Contractors are not to retain any copies of the sequencing and corresponding clinical data, even unidentified data (i.e., data that has had patient information redacted).

B.8 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

(a) A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or Task Order.

(b) All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

(c) Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

(d) Custom software development and outsourced operations must be located within the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

(e) The contractor or subcontractor must notify FMI immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor’s employ. FMI must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

B.9 VA INFORMATION CUSTODIAL LANGUAGE

(a) Information made available to the Contractor or Subcontractor by VA or FMI for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

(b) Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA or FMI, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA and FMI. Any data destruction done on behalf of VA or FMI by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification

by the Contractor that the data destruction requirements above have been met must be sent to FMI within 15 days of termination of the contract.

(c) The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

(d) The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(e) If VA or FMI determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for FMI to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause.

(f) If the contract is terminated for cause, any associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

(g) The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

(h) The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

(i) Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's or FMI's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to FMI for response.

(j) The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to FMI for response

(k) Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above-mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to FMI for response.

(l) For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to FMI and the assigned COR for each applicable facility.

B.10 SECURITY INCIDENT INVESTIGATION

(a) The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify FMI and the assigned COR for the applicable facility and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

(b) To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to FMI and VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

(c) With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

(d) In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, Contractor personnel, and its Subcontractors and their personnel shall cooperate with FMI and VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with FMI and VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B.11 LIQUIDATED DAMAGES FOR DATA BREACH

(a) Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to FMI for liquidated damages incurred by FMI in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

(b) The contractor/subcontractor shall provide notice to FMI and VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

(c) Each risk analysis shall address all relevant information concerning the data breach, including the following:

(1) Nature of the event (loss, theft, unauthorized access);

(2) Description of the event, including:

(a) Date of occurrence;

(b) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Names of individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(6) Amount of time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

(8) Known misuses of data containing sensitive personal information, if any;

(9) Assessment of the potential harm to the affected individuals;

(10) Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate; and

(11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(d) Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to FMI liquidated damages incurred by FMI in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

(1) Notification;

(2) One year of credit monitoring services consisting of automatic daily monitoring of at least three relevant credit bureau reports;

(3) Data breach analysis;

(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.