F5 SECURITY ADDENDUM

This Security Addendum ("***Addendum"***) forms part of each Agreement between Customer and F5. Unless otherwise expressly defined in this Addendum, the capitalized terms used in this Addendum have the meanings assigned to them in the Agreement.

"**Agreement**" means the agreement pursuant to which F5 provides it's software as a service products ("**EUSA**") or the agreement pursuant to which F5 licenses its software products ("**EULA**").

"**Applicable Law**" means all laws, regulations and other legal requirements applicable to either (i) F5 in its role as provider of the Services or (ii) Customer. Each party is responsible only for the Applicable Law applicable to it.

"**Customer**" means the entity to which F5 provides its software as a service products or licenses its software products pursuant to an Agreement.

"**Customer Data**" means (1) for the EULA, data uploaded by Customer in iHealth, data provided by Customer in a support ticket in the Support Portal, data provided by Customer to F5 Personnel providing support by telephone, and data present on an F5 hardware product that you return to F5 through the RMA process, and (2) for the EUSA, software, data, text or image files, or information (including data that identifies a natural person) provided or uploaded or input by Customer, its Users, or its End Users into the software as a service products or otherwise made available by Customer, its Users, or its End Users to the applicable software as a service products.

"**Customer Policies**" means all of Customer's policies and standards applicable to F5 Personnel who come on-site at Customer's facilities in connection with F5's performance of the Services or its obligations under the Agreement, in each case, as such policies and standards are made available by Customer to F5 and as may be updated from time to time.

"**F5**" means the F5 entity with whom Customer has entered the applicable Agreement.

"**F5 Personnel**" means any F5 employees, contractors or other agents who assist in the performance of the Services, but excluding any employees, contractors or agents of F5's subcontractors and subprocessors engaged by F5 to provide the Services.

"**Process**" and its derivatives means to perform any operation or set of operations on, that is performed upon Customer Data, whether or not by automated means, including but not limited to, collection, procurement, obtainment, recording, organization, storage, adaptation or alteration, retrieval, access, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, destruction, or any other form of processing, including as "**process**" or "**processing**" may be defined under Applicable Law.

"**Safeguards**" means physical, technical, organizational, and administrative policies, procedures and practices.

"**Security Incident**" means the unauthorized access to, acquisition, disclosure, theft, or misuse of Customer Data stored on F5's equipment or in F5's facilities.

"**Services**" means any and all services, functions and responsibilities, as they may evolve, and to be performed by F5 under the Agreement.

"**Software**" means any and all software programs, programming and tools (and all documentation, improvements, upgrades, materials, and media related to any of the foregoing) used by F5 in the provision of the Services.

"**Support Portal**" means my.f5.com and any similar online property that F5 operates for the purpose of providing support information or receiving support inquiries for the Service.

"**Systems**" means any and all of the following required for the performance of the Services: (a) computer information systems, and other information technology, mechanical or electronic information systems, such as servers; (b) networks, routers, switches, firewall, managed network devices (e.g., VPN hosts, load balancers, controllers, accelerators) required for the performance or receipt of the Services; and (c) firmware and Software related to any of the foregoing.

1. F5 Personnel

1.1 **Background Checks**. F5 will ensure that all F5 Personnel are subject to reasonable background checks and will not permit F5 Personnel to assist in the performance of the Services if the applicable background check identifies any material issues, including without limitation any historical event that indicates such F5 Personnel presents an increased risk of violating F5's security protocols or procedures or Processing Customer Data without authorization.

1.2 **Training and Compliance**. F5 will provide appropriate training for F5 Personnel commensurate with their roles and responsibilities relating to the Services, including without limitation training with regard to email phishing and other social engineering techniques. F5 will be responsible for the acts and omissions of all F5 Personnel.

2. **Security.** F5 will implement and maintain Safeguards designed to (a) protect Customer Data in transit and at rest against accidental, unauthorized, or unlawful Processing and against all other unlawful activities; and (b) mitigate the risk of fraud or identify theft. Specifically:

2.1 **Customer Policies.** F5 will comply with Customer Policies in relation to security standards as they pertain to the Processing of Customer Data. Without limiting the foregoing, F5 will exercise reasonable due diligence to ensure that all F5 Personnel adhere to all Customer Policies.

2.2 **Cardholder Information**. If, in the provision of its software as a service products, F5 handles cardholder account and/or transaction information ("***Cardholder Data***"), operates within Customer's Cardholder Data environment, or could impact the security of Customer's Cardholder Data environment, then:

(a) F5 will comply with applicable rules, regulations, bylaws, standards, policies, and procedures of the card associations or debit card networks, including, to the extent applicable, the Payment Card Industry Data Security Standards ("***PCI-DSS***") currently in effect, and will implement and maintain appropriate measures and controls to comply with the PCI DSS requirements.

(b) F5 represents and warrants that F5: (i) is presently compliant with all applicable PCI-DSS requirements; (ii) to the extent required by the PCI-DSS requirements (i.e., after reaching appropriate transaction thresholds) F5 has undergone a PCI-DSS assessment performed by an independent Qualified Security Assessor within the last twelve (12) months; (iii) maintains a current, compliant Attestation of Compliance certificate (or has completed a Self Assessment Questionnaire), a report of validation, a report on compliance and any exceptions noted therein (collectively, the "***PCI Compliance Documentation***"), under PCI-DSS; and (iv) will make the PCI Compliance Documentation available for Customer's review upon request.

(c) F5 will maintain and implement an incident-response plan that meets minimum PCI-DSS requirements.

2.3 **Asset Management**. F5 will maintain an asset management system to ensure that F5's Systems are inventoried and network connections are subject to security controls; mechanisms exist to properly dispose of or reimage Systems; security risks associated with Systems are appropriately managed; and the use of removable media are subject to security controls, including encryption.

2.4 **Authorized and Unauthorized Software**. F5 will establish policies and practices to identify and manage the installation of authorized Software and detect and prevent installation or execution of unauthorized Software, on devices used by F5 to provide Services.

2.5 **Secure Configurations and Logs**. F5 will implement and maintain processes and controls to ensure multifactor authentication is used to access all Customer Data; to change all factory or provider default password settings for all Systems; and to ensure only ports, protocols, and services with validated business needs are running on each System. F5 will implement and maintain security log monitoring and maintenance of a secure record of access, attributable to named individuals, for at least 1 year.

2.6 **Vulnerability Assessment, Maintenance, and Patching**. F5 will maintain and comply with a

vulnerability identification, management and remediation policy that includes timelines for patching of identified vulnerabilities, requires performance of regular vulnerability scans using current scanning tools and upgrades to Software when earlier versions are no longer supported or patched.

2.7 **Security Protection and Monitoring**. F5 will employ industry-standard protection tools and techniques, including but not limited to firewalls, antivirus, network monitoring, and intrusion detection systems; deny-listing or allow-listing to prevent known malicious IP connections; and retention of audit records of logs for event analysis. F5 will use industry standard practices to monitor, detect, and assess unauthorized access, malicious code, suspicious exfiltration of data, copying or leakage of sensitive information, and other anomalous F5 Systems activity in a timely manner. F5's operations management and network security measures will include physical and/or logical separation of Customer Data from confidential or proprietary information of F5's other customers or clients, except to the extent otherwise necessary in connection with the Services:

2.8 **Business Continuity and Data Recovery**. F5 will implement and maintain a comprehensive business continuity program, including a recovery plan, designed to ensure F5 can continue to function in the event of any operational disruption and continue to provide services to Customer within a reasonable period after such disruption.

2.9 **Incident Response Plan**. F5 has, and will maintain, a written comprehensive incident response plan to detect, respond to, contain, investigate and remediate Security Incidents and incidents that compromise the confidentiality, integrity, and availability of F5 Systems, F5 networks, and Services. The plan identifies and assigns roles and responsibilities to key stakeholders and decision-makers across the organization. F5 will regularly test its incident response plan.

2.10 **Software Security**. For all Software developed in-house or procured from third-party developers ensure Software is developed and tested using secure Software development lifecycle practices pursuant to a documented development process that explicitly addresses security requirements, and identifies the standards and tools used in the development process.

2.11 **Penetration Testing/Vulnerability Scanning**. F5 will regularly conduct penetration tests and vulnerability scans, and promptly remediate any and all confirmed vulnerabilities determined critical by F5.

2.12 **Security Certification**

F5 will maintain at least one of the following annual security certifications or reports during the term of the Agreement (each, a "***Security Certification***"):

(i) an ISO/IEC ISO 27001 certification recognized by an accredited certification body which is a member of the International Accreditation Forum;

(ii) a Service Organization Control 2 Type II report prepared in accordance with the SSAE 18 reporting standard; or

(iii) another security certification or report from a nationally-recognized certification body or assessor.

The Security Certification will fully cover the security, availability, integrity, confidentiality, and privacy-related controls of the F5 Systems and F5 Personnel that Process Customer Data. F5 will promptly provide a copy of its most recent Security Certification, to Customer on an annual basis thereafter upon receipt of request from Customer. Such Security Certification is deemed F5's Confidential Information.

3. **Encryption.** F5 will hold all Customer Data stored (including temporarily) in digital form on an encrypted medium, and use industry standard encryption tools to encrypt (128 bit or higher) all records and files containing Customer Data.

4. **Security Incidents**

4.1 In the event of any Security Incident, F5 will inform Customer by telephone, in writing or by email of the Security Incident without undue delay after F5 becomes aware of a confirmed Security Incident. Such notice will contain a description of the Security Incident, the extent to which and what Customer Data was or is subject to the Security Incident and the identity of affected individuals, to the extent known.

4.2 F5 will provide Customer with the name and contact information for an employee or agent of F5 who will serve as Customer's primary contact and will be available to assist Customer in resolving obligations associated with the Security Incident.

4.3 F5 will investigate and remediate the Security Incident and provide Customer with details regarding measures taken or proposed to be taken by F5 to address the Security Incident and ensure that a similar Security Incident will not recur.

4.4 F5 will maintain and preserve all documents, records and other data related to any and all Security Incidents, in accordance with Applicable Laws.

5. **Modifications.** Customer acknowledges that from time to time F5 may modify its Systems or its security procedures. F5 will not make any mid-Service Term modifications to the extent that such modifications would, in the aggregate, materially and adversely reduce Vendor's levels of security.