**23. Familyfirst HIPAA Business Associate Agreement ("BAA")**

This HIPAA Business Associate Agreement (this "BAA") defines the rights and responsibilities of Provider and Customer with respect to Protected Health Information ("PHI") as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, including the HITECH Act and Omnibus Rule, as each may be amended from time to time (collectively, "HIPAA"). This BAA shall be applicable only in the event and to the extent Provider meets, with respect to Customer, the definition of a Business Associate set forth at 45 C.F.R. §160.103, or applicable successor provisions. This BAA shall only be applicable to Customer's Hosting Services or Services to the extent that Customer uses the Hosting Services for Customer's Applications and as specified in the Platform as a Service Agreement of which this Exhibit C is attached and fully referenced and incorporated herein (the "Agreement"). This BAA is intended to ensure that Business Associate and Customer will establish and implement appropriate safeguards where Business Associate may receive, create, maintain, use or disclose in connection with the functions, activities and services that Business Associate performs on behalf of Customer solely to perform its duties and responsibilities under the Agreement.

1 Applicability and Definitions. This BAA applies only where:

i Customer uses the Hosting Services to store or transmit any PHI as defined in 45 C.F.R. §160.103

ii Customer has applied the required security configurations, as specified in Section 5.2 of this BAA to Customer's Applications. Customer acknowledges that this BAA does not apply to any other accounts it may have now or in the future. Unless otherwise expressly defined in this BAA, all capitalized terms in this BAA will have the meanings in HIPAA.

2 Additional Meanings.

◦ "Business Associate" shall mean Provider, or Familyfirst Messenger, LLC.

◦ "HITECH ACT" shall mean the Health Information Technology for Economic and Clinical Health Act.

◦ "Individual" shall have the same meaning as the term "individual" in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

◦ "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

◦ "Protected Health Information" or "PHI" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information received by Business Associate from or on behalf of Customer.

◦ "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

◦ "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information, located at 45 CFR Part 160 and Subparts A and C of Part 164.

3 Permitted and Required Uses and Disclosures.

i Service Offerings. Business Associate may use or disclose PHI for or on behalf of Customer as defined in the Agreement.

ii Administration and Management of Services. Business Associate may Use and Disclose PHI as necessary for the sole purpose of the proper management and administration of Hosting Services. Any disclosures under this section will be made only if Business Associate obtains reasonable assurances from the recipient of the PHI that (i) the recipient will hold the PHI confidentially and will use or disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and (ii) the recipient will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4 Obligations of Business Associate.

i Limit on Uses and Disclosures. Business Associate will use or disclose PHI only as permitted by this BAA or as required by law, provided that any such use or disclosure would not violate HIPAA if done by a Covered Entity, unless permitted for a Business Associate under HIPAA.

ii Safeguards. Business Associate will use reasonable and appropriate safeguards to prevent Use or Disclosure of PHI other than as provided for by this BAA, consistent with the requirements of Subpart C of 45 C.F.R. Part 164 (with respect to Electronic PHI) as determined by Business Associate and as reflected in the Agreement, which includes Disk Encryption and Encryption In-Transit services.

iii Reporting. For all reporting obligations under this BAA, the parties acknowledge that, because Business Associate does not know the details of PHI contained in any of Customer Applications, there will be no obligation on the Business Associate to provide information about the identities of the Individuals who may have been affected, or a description of the type of information that may have been subject to a Security Incident, Impermissible Use or Disclosure, or Breach. Business Associate will ensure Customer access to Audit Logging to help Customer in addressing Customer's obligations for reporting under this BAA. Customer acknowledges Business Associate is under no obligation to provide additional support for Customer's BAA reporting obligations but may choose to provide such additional services at its sole discretion or at Customer expense.

iv Reporting of Impermissible Uses and Disclosures. Business Associate will report to Customer any Use or Disclosure of PHI not permitted or required by this BAA of which Business Associate becomes aware.

v Reporting of Security Incidents. Business Associate will report to Customer on no less than fourteen business (14) days from the date any Security Incidents involving PHI of which Business Associate becomes aware in which there is a successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System in a manner that risks the confidentiality, integrity, or availability of such information. Notice is hereby deemed provided, and no further notice will be provided, for unsuccessful attempts at such unauthorized access, use, disclosure, modification, or destruction, such as pings and other broadcast attacks on a firewall, denial of service attacks, port scans, unsuccessful login attempts, or interception of encrypted information where the key is not compromised, or any combination of the above.

vi Reporting of Breaches. Business Associate will report to Customer any Breach of Customer's Unsecured PHI that Business Associate may discover to the extent required by 45 C.F.R. § 164.410. Business Associate will make such report without unreasonable delay, and in no case later than four (4) hours after discovery of such Breach. Business Associate undertakes no obligation to report network security related incidents which occur on its managed network but does not directly involve Customer's use of Hosting Services.

vii Subcontractors. Business Associate will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to restrictions and conditions at least as stringent as those found in this BAA, and agree to implement reasonable and appropriate safeguards to protect PHI.

viii Access to PHI. Customer acknowledges that Business Associate is not required by this BAA to make disclosures of PHI to Individuals or any person other than Customer, and that Business Associate does not, therefore, expect to maintain documentation of such disclosure as described in 45 CFR § 164.528. In the event that Business Associate does make such disclosure, it shall document the disclosure as would be required for Customer to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.504(e)(2)(ii)(G) and §164.528, and shall provide such documentation to Customer promptly on Customer's request. In the event that a request for an accounting is made directly to Business Associate shall, within 5 Business Days, forward such request to Customer.

ix Accounting of Disclosures. Business Associate will make available to Customer the information required to provide an accounting of Disclosures in accordance with 45 C.F.R. § 164.528 of which Business Associate is aware, if requested by Customer. Because Business Associate cannot readily identify which Individuals are identified or what types of PHI are included in Customer Content, Customer will be solely responsible for identifying which Individuals, if any, may have been included in Customer Content that Provider has disclosed and for providing a brief description of the PHI disclosed.

x Internal Records. Provider will make its internal practices, books, and records relating to the Use and Disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services ("HHS") for purposes of determining Customer compliance with HIPAA. Nothing in this section will waive any applicable privilege or protection, including with respect to trade secrets and confidential commercial information.

5 Customer's Obligations:

i Appropriate Use of HIPAA Accounts. Customer is responsible for implementing appropriate privacy and security safeguards in order to protect PHI in compliance with HIPAA and this BAA. Without limitation, Customer shall: (i) not include protected health information (as defined in 45 CFR 160.103) in any Services that are not or cannot be HIPAA compliant, (ii) utilize the highest level of audit logging in connection with its use of all Customer Applications, and (iii) maintain the maximum retention of logs in connection with its use of all Services.

ii HIPAA Account Appropriate Configurations: Customer is solely responsible for configuring, and will configure, all Customer Applications as follows:

iii Encryption. Customer shall encrypt all PHI stored or transmitted outside the Services in accordance with the Secretary of HHS's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>, as it may be updated from time to time, and as may be made available on any successor or related site designated by HHS.

iv TLS Termination: All services must be served via TLS. Customer is responsible for providing, maintaining and updating a valid TLS certificate for use with the Service. TLS certificates must be a minimum of 4096 bit key size. Customer agrees to comply with Business Associate's requirements regarding TLS termination.

v Necessary Consents. Customer warrants that it has obtained any necessary authorizations, consents, and other permissions that may be required under applicable law prior to placing Customer Content, including without limitation PHI, on the Services.

vi Restrictions on Disclosures. Customer shall not agree to any restriction requests or place any restrictions in any notice of privacy practices that would cause Business Associate to violate this BAA or any applicable law.

vii Compliance with HIPAA. Customer shall not request or cause Business Associate to make a Use or Disclosure of PHI in a manner that does not comply with HIPAA or this BAA.

6 Term and Termination

i Term. The term of this BAA will commence on the Agreement Effective Date and will remain in effect until the earlier of the termination of the Agreement or notification by Customer that an account is no longer subject to this BAA.

ii Effect of Termination. At termination of this BAA, Business Associate, if feasible, will return or destroy all PHI that Business Associate still maintains, if any. If return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the PHI, limit further uses and disclosures to those purposes that make the return of the PHI infeasible, and make not further use or disclosure of PHI.

iii If Customer requests contemporaneously with any termination event or notice, Business Associate will allow Customer to have access to Customer's account for a reasonable period of time following termination as necessary for Customer to retrieve or delete any PHI at its then current monthly recurring rate; provided, however, that if the security of Customer's servers has been compromised, or the Agreement was terminated by Customer's failure to use reasonable security precautions, Business Associate may: (i) provide Customer with restricted access via a dedicated or private link or tunnel to Customer account or (ii) refuse to allow Customer to have access to Customer's account but will use reasonable efforts to copy Customer data on to media Customer provides to Business Associate, and will ship the media to Customer at Customer expense. Business Associate's efforts to copy Customer data onto Customer media shall be billable as an Additional Service at Business Associate's then current hourly rates.

7 No Agency Relationship. As set forth in the Agreement, nothing in this BAA is intended to make either party an agent of the other. Nothing in this BAA is intended to confer upon Customer the right or authority to control Business Associate's conduct in the course of Business Associate complying with the Agreement and BAA.

8 Nondisclosure. Customer agrees that the terms of this BAA are not publicly known and constitute Business Associate Confidential Information under the Agreement.

9 Entire Agreement; Conflict. Except as amended by this BAA, the Agreement will remain in full force and effect. This BAA, together with the Agreement as amended by this BAA: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement; and (b) supersedes all prior agreements and understandings (whether oral or written) between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement, this BAA or any other amendment or BAA to the Agreement or this BAA, the document later in time will prevail.

10 Miscellaneous.

i Amendment. Customer and Business Associate agrees to take such action as is reasonably necessary to amend this HIPAA BAA from time to time as is necessary for either party to comply with the requirements of the Privacy Rule and related laws and regulations.

ii Survival. Customer and Business Associate's respective rights and obligations under this HIPAA BAA shall survive the termination of the Agreement.

iii Interpretation. Any ambiguity in the Agreement shall be resolved to permit Customer to comply with HIPAA and the Privacy Rule.

SIGNATURE FOLLOWS