**1. Introduction**

Familyfirst Messenger, LLC ("Familyfirst") is committed to ensuring the confidentiality, privacy, integrity, and availability of all electronic protected health information (ePHI) it receives, maintains, processes and/or transmits on behalf of its Customers. As providers of compliant, hosted infrastructure used by health technology vendors, developers, designers, agencies, custom development shops, and enterprises, Familyfirst strives to maintain compliance, proactively address information security, mitigate risk for its Customers, and assure known breaches are completely and effectively communicated in a timely manner. The following documents address core policies used by Familyfirst to maintain compliance and assure the proper protections of infrastructure used to store, process, and transmit ePHI for Familyfirst Customers.

Familyfirst provides secure and compliant cloud-based software. This hosted software falls into two broad categories: 1) **Platform as a Service (PaaS)** and 2) **Platform Add-ons**. These Categories are cited throughout polices as Customers in each category inherit different policies, procedures, and obligations from Familyfirst.

**1.1 Compliance Inheritance**

Familyfirst provides compliant hosted software infrastructure for its Customers. Familyfirst has been through a HIPAA compliance audit by a national third-party compliance firm to validate and map organizational policies and technical controls to HIPAA rules. Familyfirst's company policies, procedures, and technologies are HITRUST Certified. Familyfirst's service offerings are available on AWS, Azure, Rackspace, and SoftLayer; current production systems on these platforms are included in Familyfirst's third-party audits and HITRUST certification.

Familyfirst signs business associate agreements (BAAs) with its Customers. These BAAs outline Familyfirst obligations and Customer obligations, as well as liability in the case of a breach. In providing infrastructure and managing security configurations that are a part of the technology requirements that exist in HIPAA and HITRUST, as well as future compliance frameworks, Familyfirst manages various aspects of compliance for Customers. The aspects of compliance that Familyfirst manages for Customers are inherited by Customers, and Familyfirst assumes the risk associated with those aspects of compliance. In doing so, Familyfirst helps Customers achieve and maintain compliance, as well as mitigates Customers risk.

Familyfirst does not act as a covered entity. When Familyfirst does operate as a business associate (not a subcontractor), Familyfirst does not interface with users to obtain or provide access to ePHI. Access to ePHI is through our customers' applications.

Certain aspects of compliance cannot be inherited. Because of this, Familyfirst Customers, in order to achieve full compliance or HITRUST Certification, must implement certain organizational policies. These policies and aspects of compliance fall outside of the services and obligations of Familyfirst.

Mappings of HIPAA Rules to Familyfirst controls and a mapping of what Rules are inherited by Customers, both Platform Customers and Add-on Customers, are covered in §2.

**1.2 Requesting Audit and Compliance Reports**

Familyfirst, at its sole discretion, shares audit reports, including its HITRUST reports and Corrective Action Plans (CAPs), with customers on a case by case basis. All audit reports are shared under explicit NDA in Familyfirst format between Familyfirst and party to receive materials. Audit reports can be requested by Familyfirst workforce members for Customers or directly by Familyfirst Customers.

The following process is used to request audit reports:

1 Email is sent to [contact@familyfirst.io](mailto:contact@familyfirst.io). In the email, please specify the type of report being requested and any required timelines for the report.

2 Familyfirst staff will log an Issue with the details of the request into the Familyfirst Compliance Review Activities Project on JIRA. JIRA is used to track requests status and outcomes.

3 Familyfirst will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, Familyfirst will send one for execution.

4 Once it has been confirmed that an NDA is executed, Familyfirst staff will move the JIRA Issue to "Under Review".

5 The Familyfirst Security Officer or Privacy Officer must Approve or Reject the Issue. If the Issue is rejected, Familyfirst will notify the requesting party that we cannot share the requested report.

6 If the Issue has been Approved, Familyfirst will send the customer the requested audit report and complete the JIRA Issue for the request.