**3. Policy Management Policy**

Familyfirst implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all Familyfirst workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained to assure ease of finding policies at specific historic dates in time.

**3.1 Applicable Standards**

**3.1.1 Applicable Standards from the HITRUST Common Security Framework**

• 12.c - Developing and Implementing Continuity Plans Including Information Security

**3.1.2 Applicable Standards from the HIPAA Security Rule**

• 164.316(a) - Policies and Procedures

• 164.316(b)(1)(i) - Documentation

**3.2 Maintenance of Policies**

1 All policies are stored and up to date to maintain Familyfirst compliance with HIPAA, HITRUST, NIST, and other relevant standards. Updates and version control are done similar to source code control.

2 Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by both the Security and Privacy Officer to assure they are accurate and up-to-date.

3 Familyfirst employees may request changes to policies using the following process:

4 The Familyfirst employee initiates a policy change request by creating an Issue in the JIRA Compliance Review Activity (CRA) project. The change request may optionally include a GitHub pull request from a separate branch or repository containing the desired changes.

5 The Security Officer or the Privacy Officer is assigned to review the policy change request.

6 Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

7 If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

8 If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using Familyfirst's change management process (§9.4).

9 All policies are made accessible to all Familyfirst workforce members. The current master policies are published at [https://policy.datica.com](https://policy.datica.com/).

◦ Changes are automatically communicated to all Familyfirst team members through integrations between GitHub and Slack that log all GitHub policy channels to a dedicated Familyfirst Slack Channel.

◦ The Security Officer also communicates policy changes to all employees via email. These emails include a high-level description of the policy change using terminology appropriate for the target audience.

10 All policies, and associated documentation, are retained for 6 years from the date of its creation or the date when it last was in effect, whichever is later

i Version history of all Familyfirst policies is done via GitHub.

ii Backup storage of all policies is done with Box.

11 The policies and information security policies are reviewed and audited annually, or after significant changes occur to Familyfirst's organizational environment. Issues that come up as part of this process are reviewed by Familyfirst management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing polices is outlined below:

12 The Security Officer initiates the policy review by creating an Issue in the JIRA Compliance Review Activity (CRA) project.

13 The Security Officer or the Privacy Officer is assigned to review the current Familyfirst policies.

14 If changes are made, the above process is used. All changes are documented in the Issue.

15 Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

16 If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

17 Policy review is monitored on a quarterly basis using JIRA reporting to assess compliance with above policy.

18 Familyfirst utilizes the HITRUST MyCSF framework to track compliance with the HITRUST CSF on an annual basis. Familyfirst also tracks compliance with HIPAA. In order to track and measure adherence on an annual basis, Familyfirst uses the following process to track HITRUST audits, both full and interim:

19 The Security Officer initiates the HITRUST audit activity by creating an Issue in the JIRA Compliance Review Activity (CRA) project.

20 The Security Officer or the Privacy Officer is assigned to own and manage the HITRUST activity.

21 Once the HITRUST activity is completed, the Security Officer approves or rejects the Issue.

22 If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

23 Compliance with annual compliance assessments, utilizing the HITRUST CSF as a framework, is monitored on a quarterly basis using JIRA reporting to assess compliance with above policy.

Additional documentation related to maintenance of policies is outlined in §5.3.1.