**21. 3rd Party Policy**

Familyfirst makes every effort to assure all 3rd party organizations are compliant and do not compromise the integrity, security, and privacy of Familyfirst or Familyfirst Customer data. 3rd Parties include Customers, Partners, Subcontractors, and Contracted Developers.

**21.1 Applicable Standards**

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

• 05.i - Identification of Risks Related to External Parties

• 05.k - Addressing Security in Third Party Agreements

• 09.e - Service Delivery

• 09.f - Monitoring and Review of Third Party Services

• 09.g - Managing Changes to Third Party Services

• 10.1 - Outsourced Software Development

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

• 164.314(a)(1)(i) - Business Associate Contracts or Other Arrangements

**21.2 Policies to Assure 3rd Parties Support Familyfirst Compliance**

1 Familyfirst does not allow 3rd party access to production systems containing ePHI.

2 All connections and data in transit between the Familyfirst Platform and 3rd parties are encrypted end to end.

3 A standard business associate agreement with Customers and Partners is defined and includes the required security controls in accordance with the organization's security policies. Additionally, responsibility is assigned in these agreements.

4 Familyfirst has Service Level Agreements (SLAs) with Subcontractors with an agreed service arrangement addressing liability, service definitions, security controls, and aspects of services management.

◦ Subcontractors must coordinate, manage, and communicate any changes to services provided to Familyfirst.

◦ Changes to 3rd party services are classified as configuration management changes and thus are subject to the policies and procedures described in §9; substantial changes to services provided by 3rd parties will invoke a Risk Assessment as described in §4.2.

◦ Familyfirst utilizes monitoring tools to regularly evaluate Subcontractors against relevant SLAs.

5 No Familyfirst Customers or Partners have access outside of their own environment, meaning they cannot access, modify, or delete anything related to other 3rd parties.

6 Familyfirst does not outsource software development.

7 Familyfirst maintains and annually reviews a list all current Partners and Subcontractors.

◦ The list of current Partners and Subcontractors is maintained by the Familyfirst Privacy Officer, includes details on all provided services (along with contact information), and is recorded in §1.4.

◦ The annual review of Partners and Subcontractors is conducted as a part of the security, compliance, and SLA review referenced below.

8 Familyfirst assesses security, compliance, and SLA requirements and considerations with all Partners and Subcontractors. This includes annual assessment of SOC2 Reports for all Familyfirst infrastructure partners.

◦ Familyfirst leverages recurring calendar invites to assure reviews of all 3rd party services are performed annually. These reviews are performed by the Familyfirst Security Officer and Privacy Officer. The process for reviewing 3rd party services is outlined below:

a The Security Officer initiates the SLA review by creating an Issue in the JIRA Compliance Review Activity (CRA) Project.

b The Security Officer, or Privacy Officer, is assigned to review the SLA and performance of 3rd parties. The list of current 3rd parties, including contact information, is also reviewed to assure it is up to date and complete.

c SLA, security, and compliance performance is documented in the Issue.

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

9 Regular review is conducted as required by SLAs to assure security and compliance. These reviews include reports, audit trails, security events, operational issues, failures and disruptions, and identified issues are investigated and resolved in a reasonable and timely manner.

10 Any changes to Partner and Subcontractor services and systems are reviewed before implementation.

11 For all partners, Familyfirst reviews activity annually to assure partners are in line with SLAs in contracts with Familyfirst.

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