**19. Employees Policy**

Familyfirst is committed to ensuring all workforce members actively address security and compliance in their roles at Familyfirst. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

**19.1 Applicable Standards**

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

• 02.e - Information Security Awareness, Education, and Training

• 06.e - Prevention of Misuse of Information Assets

• 07.c - Acceptable Use of Assets

• 09.j - Controls Against Malicious Code

• 01.y - Teleworking

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

• 164.308(a)(5)(i) - Security Awareness and Training

**19.2 Employment Policies**

1 All new workforce members, including contractors, are given training on security policies and procedures, including operations security, within 30 days of employment.

◦ Records of training are kept for all workforce members.

◦ Employees must complete this training before accessing production systems containing ePHI.

2 All workforce members are granted access to formal organizational policies, which include the sanction policy for security violations.

3 The Familyfirst Employee Handbook clearly states the responsibilities and acceptable behavior regarding information system usage, including rules for email, Internet, mobile devices, and social media usage.

◦ Workforce members are required to sign an agreement stating that they have read and will abide by all terms outlined in the Familyfirst Employee Handbook, along with all policies and processes described in this document.

◦ A Human Resources representative will provide the agreement to new employees during their onboarding process.

4 Familyfirst does not allow mobile devices to connect to any of its production networks.

5 All workforce members are educated about the approved set of tools to be installed on workstations.

6 All new workforce members are given HIPAA training within 30 days of beginning employment. Training includes HIPAA reporting requirements, including the ability to anonymously report security incidents, and the levels of compliance and obligations for Familyfirst and its Customers and Partners.

7 All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies. Additionally, remote security is maintained through the use of VPN tunnels for all access to production systems with access to ePHI data.

8 All Familyfirst-purchased and -owned computers are to display this message at login and when the computer is unlocked: *This computer is owned by Familyfirst Health, Inc. By logging in, unlocking, and/or using this computer you acknowledge you have seen, and follow, these policies and have completed this training. Please contact us if you have problems with this - contact@familyfirst.io.*

9 Employees may only use Familyfirst-purchased and -owned workstations for accessing production systems with access to ePHI data.

◦ Any workstations used to access production systems must be configured as prescribed in §7.8.

◦ Any workstations used to access production systems must have virus protection software installed, configured, and enabled.

◦ Familyfirst may monitor access and activities of all users on workstations and production systems in order to meet auditing policy requirements (§8).

10 Access to internal Familyfirst systems can be requested using the procedures outlined in §7.2. All requests for access must be granted by the Familyfirst Security Officer.

11 Request for modifications of access for any Familyfirst employee can be made using the procedures outlined in §7.2.

12 Familyfirst employees are strictly forbidden from downloading any ePHI to their workstations.

◦ Restricting transfers of ePHI is enforced through technical controls as described in §7.13.

◦ Employees found to be in violation of this policy will be subject to sanctions as described in §5.3.3.

13 Employees are required to cooperate with federal and state investigations.

◦ Employees must not interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.

◦ Employees found to be in violation of this policy will be subject to sanctions as described in §5.3.3.

**19.3 Issue Escalation**

Familyfirst workforce members are to escalate issues using the procedures outlined in the Employee Handbook. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer.

Security incidents, particularly those involving ePHI, are handled using the process described in §11.2. If the incident involves a breach of ePHI, the Security Officer will manage the incident using the process described in §12.2. Refer to §11.2 for a list of sample items that can trigger Familyfirst's incident response procedures; if you are unsure whether the issue is a security incident, contact the Security Officer immediately.

It is the duty of that owner to follow the process outlined below:

1 Create an Issue in the JIRA Compliance Review Activity (CRA) Project.

2 The Issue is investigated, documented, and, when a conclusion or remediation is reached, it is moved to Review.

3 The Issue is reviewed by another member of the Escalation Team. If the Issue is rejected, it goes back for further evaluation and review.

4 If the Issue is approved, it is marked as Done, adding any pertinent notes required.

5 The workforce member that initiated the process is notified of the outcome via email.