NFP® | Health

NFP HEALTH SERVICES ADMINSTRATORS

Financial Management Services

System and Organization Controls (SOC) for Service Organizations Report for the period of July 1, 2019 to June 30, 2020

Grant Thornton

Contents

I. **Report of Independent Service Auditors**

Board of Directors and Management
NFP Health Services Administrators

Scope

We have examined NFP Health Services Administrators' (the "Company") description of its financial management services provided to HealthSource RI ("HealthSource RI" or "user entity") under the subcontract with Deloitte Consulting, LLP (the "System") titled "NFP Health Services Administrators' Description of its System and Controls" for processing the user entity's transactions ("description") throughout the period July 1, 2019 to June 30, 2020 (the "specified period") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "NFP Health Services Administrators' Assertion." The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to HealthSource RI's internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to HealthSource RI's internal control over financial reporting.

The Company uses subservice organizations listed in Table 1 in Section III of this report. The description in Section III of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the specified period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and

- evaluating the overall presentation of the description, the suitability of the control objectives stated in the description, and the suitability of the criteria specified by the service organization in its assertion.

Inherent limitations
Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in NFP Health Services Administrators' assertion:

a.   The description fairly presents the financial management services that was designed and implemented throughout the period July 1, 2019 to June 30, 2020.

b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2019 to June 30, 2020 and subservice organizations and the user entity applied the complementary controls assumed in the design of NFP Health Services Administrators' controls throughout the period July 1, 2019 to June 30, 2020.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2019 to June 30, 2020 if complementary subservice organization and user entity controls assumed in the design of NFP Health Services Administrators' controls operated effectively throughout the period July 1, 2019 to June 30, 2020.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of the Company, HealthSource RI, and their auditors who audit and report on such user entity financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the user entity themselves, when assessing the risks of material misstatement of the user entity's financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Grant Thornton LLP

Philadelphia, Pennsylvania
August 17, 2020

II.NFP Health Services Administrators' Assertion

We have prepared the accompanying description of NFP Health Services Administrators' (the "Company") financial management services provided to HealthSource RI ("HealthSource RI" or "user entity") under the subcontract with Deloitte Consulting, LLP (the "System") for processing the user entity transactions throughout the period July 1, 2019 to June 30, 2020 (the "specified period"), for HealthSource RI and their auditors who audit and report on such user entity financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and HealthSource RI themselves, when assessing the risks of material misstatements of HealthSource RI's financial statements.

The Company uses subservice organizations listed in Table 1 in Section III of this report to provide various services. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if the complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the user entity.

We confirm, to the best of our knowledge and belief, that:

A. The description fairly presents the System made available to HealthSource RI for processing their transactions as it relates to controls that are likely to be relevant to HealthSource RI's internal control over financial reporting. The criteria we used in making this assertion were that the description:

1. Presents how the system made available to HealthSource RI was designed and implemented to process relevant user entity transactions, including, if applicable:

   a. The type of services provided, including, as appropriate, the classes of transactions processed;

   b. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for HealthSource RI;

   c. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for HealthSource RI;

> d. How the system captures and addresses significant events and conditions other than transactions;
>
> e. The process used to prepare reports or other information for the user entity;
>
> f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;
>
> g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and
>
> h. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

2. Includes relevant details of changes to the service organization's system during the specified period.

3. Does not omit or distort information relevant to the service organization's system.

B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the specified period to achieve those control objectives if the subservice organizations and the user entity applied the complementary controls assumed in the design of the Company's controls throughout the specified period. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Company;

2. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

III. NFP Health Services Administrators' Description of System and Controls

A. Scope and Purpose of the Report

This report describes the control structure of NFP Health Service Administrators' ("NFP Health") as it relates to its financial management services for the period of July 1, 2019 to June 30, 2020 (the "specified period"). This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of NFP Health, HealthSource RI ("HealthSource RI" or the "user entity"), and their auditors who audit and report on such user entity financial statements or internal control over financial reporting ("ICFR") and have a sufficient understanding to consider it, along with other information, including information about the controls implemented by the user entity themselves, when assessing the risks of a material misstatement to the user entity's financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

The scope of this report is limited to financial management services. HealthSource RI and their auditors are responsible for determining if the services provided to them by NFP Health are in the scope of this report.

B. Overview of Services Provided

NFP Health provides financial management services to the State of Rhode Island under a subcontract with Deloitte Consulting, LLP ("Deloitte"). Since January 2013, Deloitte has been engaged in delivering the Unified Health Infrastructure Project ("UHIP") on behalf of the State of Rhode Island. In delivering this project, Deloitte is designing, developing, implementing and operating a technology platform and system to support a statewide Health Insurance Exchange, under the Patient Protection and Affordable Care Act.

Under UHIP, Deloitte is responsible for development of the system technology, hosting services, ongoing maintenance, fulfilling requested enhancements, as well as payment processing through an integrated financial management system. NFP Health's subcontract with Deloitte addresses the financial management component of services provided.

HealthSource RI ("HSRI"), contracted with NFP Health to build a small-group only ("SHOP") enrollment portal to replace the SHOP enrollment portion of the Deloitte UHIP system. As part of this effort, NFP Health split the financial management system into two separate databases and user interfaces. The code system and controls are exactly the same across both systems except where explicitly called out in this document and in the controls spreadsheet document. The two systems together represent the financial management system for HSRI.

As part of this subcontract, NFP Health provides Core Premium Billing Services ("CPBS") and staff to support financial management services. These services include:

- Processing system with batch and real time integration with Rhode Island State Health Insurance Exchange ("HIX"). HIX is a service available in every state that helps individuals, families, and small businesses shop and enrol in medical insurance.

- Technical maintenance support for the system, and a technical support Call Center to support technical issues.

- Ongoing reporting on customer support interactions through pre-defined reports.

- Proactive review and follow up on issues with payment.

- Generate, print, and mail premium and user fee invoices to relevant parties.

- Automated payment collection processes and interfaces.

- Execution of online payments for employers/individuals, and bank payments. NFP Health is limited to providing a National Automated Clearing House Association ("NACHA")-compliant file of requested payments to the bank, it is the bank that processes these payments – NFP Health records them in the billing system.

- Backups, security, and disaster recovery.

- Approval and quality-controlled process for processing payments to Issuers as well as for refunds to customers.

C. Relevant Aspects of the Overall Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning controls and the emphasis given to controls, as expressed by NFP Health's policies, procedures, methods, and organizational structure. The following is a description of the components of internal control pertaining to NFP Health's systems.

1. Control Environment and Control Activities

a. Management's Philosophy and Operating Style

Management of NFP Health is responsible for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values held by NFP Health. Organizational values and behavioral standards are communicated to personnel through policy statements and formal codes of conduct as detailed in the Employee Handbook, and mandated regular training relating to personal information, privacy, and the handling of sensitive data.

b. Organizational Structure

The NFP Health organizational structure provides a framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Cross training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

The Executive Management Team consists of the Chief Executive Officer ("CEO"), Chief Operating Officer ("COO"), Vice President of Exchange Services for NFP Health, with oversight by the COO of HSA Insurance, the parent company of the NFP Health business unit. The COO manages the operations team, handles escalations and is the binding approver for client-requested changes to the system. Responsibilities also include, but are not limited to, the following:

- Ensuring the development and implementation of a strategic plan.

- Setting standards and expectations for leadership and other key positions.

- Monitoring the quality of the organization's services/delivery and ensuring maximum client satisfaction.

- Securing and protecting the organization's assets

The Implementation Team is managed by the Implementation Lead. The Implementation and Technology Lead is in constant contact with the client; determining requirements, reporting progress and procuring feedback.

The Release Management Team is responsible for organizing bi-weekly development meetings, led by the Release Management Lead. These bi-weekly meetings are held for the purpose of communicating requirements, change requests and report progress. Developers, testers, business specialists, infrastructure and operations, attend these mandatory meetings. Each member has the opportunity to communicate status and report any issues encountered.

The Technical Operations Team, consisting of the Client Engagement Lead, Delivery Lead, Project Management Office ("PMO"), Technology Operations Manager, Testing and Quality Assurance ("QA") Lead and Release Management Lead, is led by the Technology Operations Manager. This team is responsible for monitoring and maintaining the organization's infrastructure and systems, the security of its networks, and the consistency and integrity of organization's data. The team leverages JIRA/Azure DevOps software for project management and issue tracking and discusses these items during regular meetings.

The PMO, consisting of personnel from the Technical and Operations Team, is responsible for recording minutes of each meeting, including the bi-weekly development meetings, and tracks the status using the Microsoft Project Plan. Risks and issues are immediately identified and addressed. Additionally, JIRA/Azure DevOps is used to capture bugs found by testers and tracks status through resolution.

The Financial Operations Team, consisting of Finance and Billing Specialists, Call Center Team, Project Specialist and Operations Support, is managed by the Premium Billing & Operations Lead. This team helps ensure that client specific procedures and protocols are followed. Job sharing is utilized for succession planning and operational redundancy.

The Call Center Team is governed by standard operating procedures established by the client, coupled with NFP Health best practices. Call recording is utilized for quality assurance.

c.   Commitment to Competence

The Executive Management Team is responsible for determining the competency levels required at each position; they do so by considering NFP Health's objectives and strategies and the plans to achieve them. The Executive Management Team has defined and analyzed the tasks necessary to fulfil particular roles including such factors as the extent to which individuals must exercise judgment and the extent of related supervision. In addition, management determines the knowledge and skills required to perform certain job functions such that each position at NFP Health has a pre-defined set of technical knowledge and personal skills required for each level of employment. These competency requirements, which are communicated to personnel and candidate employees during the hiring process, help to ensure that current and new employees are qualified for their position.

d.   Human Resource Policies and Practices

NFP Health has formal personnel policies and procedures that include hiring practices, training, performance reviews, and a code of conduct. These policies and procedures are reviewed and updated on an annual basis. Confidentiality of customer information is stressed during the hiring and training process. Employees and departments within NFP Health have specific goals and objectives by which they are measured. The organizational structure of NFP Health is communicated to employees at the time of hire and lines of responsibility are clearly defined. Job descriptions are clearly communicated and described to the employees and the procedures to be followed are clearly defined and available to the employees. When a new employee joins NFP Health, they participate in a series of training sessions to enable new employees to familiarize themselves with NFP Health's procedures.

NFP Health is committed to the hiring, retention and continued training of skilled staff. New employees are not hired without dual level interviews by internal Human Resources ("HR") staff and an appropriately skilled and qualified current employee. Additionally, the receipt of appropriate references is required. The appropriate Executive Management Team member authorizes new hire and internal promotions.

Staff are professionally qualified and engage in training to receive and maintain qualifications. Personnel are encouraged to maintain and increase their skills and knowledge.

As part of the process of employee development, each employee undergoes an annual Performance Development Review ("PDR") to help ensure employees are aware of what is expected of them and to provide feedback on individual performance. The first phase of the PDR focuses on goal setting and planning between the supervisor/manager and the employee, while the second phase covers the annual performance reviews and merit increases. In the evaluation, employees are required to perform a self-assessment and then supervisors/managers are required to evaluate and document the performance of employees. The annual performance review meeting provides an opportunity for the supervisor/manager and employee to discuss accomplishments and on-going professional development opportunities. Both are encouraged to engage in on-going performance feedback discussions and evaluations throughout the year.

2. **Risk Assessment**

Risk assessment and monitoring are built into the contract of services and are performed by both Technical Operations and Financial Operations personnel, with oversight by the Executive Team. The focus of risk assessment processes is on both the ongoing operations and maintenance of the current system, as well as evaluating new enhancements, fixes or other changes to the system, to prevent changes in functionality from placing core functionality and customer-facing capabilities at risk.

For Technical Operations, risk assessment is handled by proactive research into known vulnerabilities in any aspect of the infrastructure that may require patching, updates, rule changes, or similar enhancements and modifications. From a development standpoint, risks relating to performance are addressed by stress-testing and use case testing in lower environments prior to the promotion of code into production, to confirm that performance/response issues are not anticipated, and that the functionality provided, produces the results expected by the client.

For Financial Operations, risk assessment is handled based on the leading practices established within the operations of the parent company of NFP Health, HSA Insurance, which includes periodic audits involving personnel or auditors on behalf of every major health insurance carrier in New England.

3. **Monitoring, Information and Communication**

Technology monitoring includes 24/7 monitoring of uptime and downtime of the systems, the performance/speed of the system, and various other aspects of performance, and leverages pre-defined escalation policies and personnel coordinated through an escalation system. The monitoring systems for performance are handled through third-party distributed remote agents that provide real-time alerts of any issues detected from outside of the data center, as well as a second layer that monitors internally to the data center network, and at the application and database level via an independent third-party solution.

System performance is tracked and reported to the client on a monthly basis, which includes the following measures:

a. Real-Time Transaction Performance

- Transactions that require interface with a third-party application or Commercial Off-the-Shelf ("COTS") application.

- Transactions that require integration across multiple enterprise databases and/or middleware interaction.

- Image Retrieval: the time it takes to get a viewable image to the application service. This service level agreement ("SLA") applies to images generated from systems under NFP Health's control.

b. Member Statement SLAs

- Monthly Account Statements are mailed no later than the Account Statement mailing date agreed to in the Billing Cycle.

- Notifications to the Exchange within 24 hours if any Account Statements were not included in the monthly Account Statement run.

- Member Account Statements that accurately reflect account balance and payment due are produced and mailed.

- Refund amounts are determined accurately.

- Members entitled to a refund are identified to HIX.

4. **Information Systems Overview**

NFP Health's Technology Operations Department is responsible for the integrity of infrastructure and systems that support the CPBS system. Technology Operations builds, deploys, maintains and monitors all hardware, networks, operating systems, databases and applications associated with CPBS. Operations Department members are responsible for granting and revoking access to CPBS system; securing customer, client and company data; and overseeing the change management and release management processes. Refer to the paragraphs below for the additional information.

a. Application Overview

CPBS system is an application consisting of a database and core software modules that allow loading of enrollment data, creation of bills, and processing of payments.

Specifically, the application includes modules for loading enrollments, running monthly billing, processing Automated Clearing House ("ACH") and lockbox payments, and aggregating premium for payment to the appropriate carriers to which premium is due. It also includes a web-based user interface for use by Call Center and financial staff to research enrollment and billing transactions, and process reversal of payments, reallocation of payments, and the setup of refunds.

The application is housed at third-party colocation data center facilities and is managed and monitored by the Development and Technology Operations team.

b. Location

NFP Health's infrastructure is located in data centers managed by two subservice organizations, TierPoint LLC, and CenturyLink. The primary data center is located in Marlborough, MA, while the secondary data center is located in Highlands Ranch, CO.

c. Core Infrastructure

NFP Health's core infrastructure consists of the following items:

- Cisco Nexus switches for core switching and routing.

- Cisco Adaptive Security Appliance ("ASA") firewalls to provide perimeter security.

- F5's Big-IP Load Balancers used to load balance incoming network traffic.

- Cisco's Unified Computing System ("UCS") platform to provide memory and compute via null storage blade servers.

- NetApp Storage Area Networks ("SAN") to provide network storage.

- VMware is used to provide a virtual server environment.

d. Operating Systems, Virtualization and Network Domain

NFP Health uses VMware ESXi with the majority of its server infrastructure running Windows Server. Within the operating system, NFP Health leverages Internet Information Services ("IIS") and .NET for its applications. Network is managed through Active Directory.

e. Databases

NFP Health's applications leverage Microsoft ("MS") SQL Server 2012 Enterprise. To provide management and monitoring of its MS SQL instances, NFP Health leverages the services of Rackspace Technology Inc. (f/k/a TriCore Solutions) (Norwell, MA). Rackspace Technology provides 24/7/365 monitoring and management for its databases.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

10

D. Control Objectives and Description of Controls

1. New Customer Setup and Modifications

NFP Health receives batches of new and existing customer activity from the Rhode Island UHIP. Customer enrollment information, such as name, Social Security Number ("SSN"), address, health insurance plan, as well as the premium line amounts and any federal, state or other subsidies, are transferred to the Financial Management System from UHIP, using Electronic Data Interchange ("EDI") files.

These files are reviewed daily via a combination of quality control queries, and through Operations personnel, who look for known issues that are fixed upon receipt. This helps ensure that customer data comes across completely and accurately, for further payment and billing processing. In the event that an error is noted, the event is tracked through resolution within 24 hours, by sending a "999" response file to UHIP. The "999" response file is used to confirm receipt of the file and communicate errors with the data. UHIP personnel are responsible for resolving the error through the UHIP system, which is the source of truth for enrollment data.

For new customers, a unique customer ID is created by UHIP application, and is used as the common reference between UHIP and CPBS. The unique customer ID is transferred to CPBS using the above-mentioned EDI files.

Individual enrollments and SHOP enrollments split into separate systems and separate databases, where SHOP enrollments originate in the NFP Health SHOP enrollment portal. As with UHIP application, unique customer and member IDs are created in the portal and used as the common reference between the portal and CPBS.

As enrollments are created and updated in the portal, the transactions are queued up for a nightly process that uses the same CPBS web services employed in bringing in individual enrollment adds and changes. This batch process is logged and monitored, with notifications upon error going to the IT team.

For SHOP enrollments only, on a daily basis, excluding weekends and holidays, the carriers are notified via an "834" file of new SHOP enrollment and changes to activate or amend policy. This process includes identifying add/changes/terminations in the SHOP CPBS system, extracting them, and formatting them as "834" EDI. These EDI files are then delivered to the carriers, with full logging and error notification. File failures are researched and resolved by the IT team. Individual enrollments are sent to carrier directly by UHIP.

Daily emails indicating that 834s have been posted are delivered to the technical operations team. Any errors or failures are noted in these emails. Additionally, EDI 999 responses to the daily 834s to carriers are analyzed each business day. Finally, SLA reporting is done monthly to the client to indicate 834s were sent on a daily basis, excluding weekends and holidays. This report also includes information indicating when an 834 was not sent to a carrier because no enrollment data needs sending on that business day.

2. Billings

Billing statements are generated for customers in two different scenarios:

Daily – For initial enrollments, a billing statement is generated, which the customer can reference to make payment for the first month of coverage. If one-time ACH payments have been made and matched to an initial enrollment, this initial statement shows the payment and current amount due. The billing statement further reflects the payment status, as well as totals for the first month's premium lines. These are produced on a daily basis, for the relevant customers, only after the enrollment information is processed through the normal daily enrollment batches, and the current day's ACH payments and any previous day's lockbox/scanned payments are applied.

Monthly – Regular billing, for new or existing customers, is typically run on the 25th of the month, but can be moved based upon State of Rhode Island directive or to match business days vs. calendar days, meaning if the 25th falls on a Saturday or Sunday, the State of Rhode Island can decide to bill on the Friday before or on the Monday after. Monthly statements include transactions that have happened since the previous month, such as a payment received, payment rejected, plan changes, addition or termination of people from the plan, subsidies added or removed, as well as regular, ongoing monthly premium lines.

The statement generation process creates a pre-defined XML file. The resulting XML file is transmitted to the mail house vendor used by NFP Health to print and mail the statements, via a Secure File Transfer Protocol ("SFTP") location shared by the mail house and NFP Health. The mail house is notified of the transmission of the XML file, and a request to transform the statements into electronic portable document format ("PDF"), and then hard copy, is generated. As part of the transformation, the mail house creates a scanline that is unique to each customer and statement. The scanline is used when the payment coupon (the top third of the statement) is sent in with a check or money order, to be scanned at the lockbox or via a remote scanner at a carrier.

Once the PDFs are created, they are uploaded by the mail house back to the SFTP site and NFP Health operations personnel are notified. The SFTP site is used to securely pass the data files from CPBS to the mail house and back from the mail house to CPBS. A quality check is performed by NFP Health operations personnel prior to authorizing the mail house to mail the statements to the customers.

The PDF statements are uploaded into CPBS and linked to the relevant customers account information for access by customers/clients, NFP Health staff and UHIP staff who may be assisting customers with enrollment or simple billing issues.

3. **Transactions Processing**

Batch payments are processed and uploaded to CPBS daily and any issues are tracked and resolved by the Financial Operations Team so that data is entered completely and accurately.

Payments are handled in two steps. The first step is the receipt of a payment via ACH or a lockbox deposit to the exchange bank account. The second step is the application of a payment to the appropriate customer account. Payments are automatically applied based upon unique client identifiers. Initial payment may come over during the enrollment process, if customers choose to pay their first payment using a one-time ACH payment. If such a payment is provided, the payment is processed that same day if received with sufficient time to process prior to the daily 5pm ACH process run, or the next business day. Upon receipt of payment from a customer, that payment may go into a suspense account if the corresponding full enrollment information has not yet been provided to CPBS in the daily batch.

NFP Health integrates with inComm Inc. ("inComm") and CVS Pharmacy ("CVS") to facilitate in person cash and credit/debit card payments at CVS locations. This integration is peer to peer, meaning both organizations have separate contracts with HSRI and are directed to work together to execute the integration. Neither party is directly contractually bound to the other. NFP Health imports unique identifiers from inComm to attach to each existing and new accounts in CPBS and used this information to create a bar code that allowed a CVS clerk to scan the code in with the payment. Each day, inComm remits the sum of payments to Webster Bank, and delivers a report with the code and amount of each payment. This report is processed by CPBS and the payment is applied to the appropriate customer account.

When the necessary/required enrollment data is transmitted by UHIP to CPBS (typically the next business day in the case of initial enrollment), an automated process either applies the payment out of the suspense account to the identified customer account, or it is applied directly to the account if enrollment data exists within CPBS prior to the ACH batch process being run.

Checks or money orders that are processed by the bank through the lockbox and remote scanner processes follow a similar process to ACH. If the scanning process finds a customer ID (whether written or through the Optical Character Recognition ("OCR") scanline on the payment coupon), the resulting lockbox/scan files and the transactions within the file representing each payment received automatically matches the incoming payments to the enrollment data, applying payments to the appropriate customer accounts. If lockbox/scan files do not contain clearly identifying information for the customer, such as the unique customer ID, those payments are placed into suspense for manual research and assignment of payments (which is covered in the payment reconciliation section).

Payments that have been processed within CPBS are monitored and compared to the bank statements to help ensure that data representing customer payments have been received and applied as expected. This is accomplished by running standard reports, queries, and consulting daily dashboards, displayed as a result of checks run against the system. As part of processing and applying payments to accounts, if a payment is received in excess of the amount due, the excess amount is automatically applied as a credit balance towards the next month's billing for the respective customer.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

12

For an initial payment (the first month's premium) that is not within $5 of the total amount due, the customer is not considered paid in full and is not transmitted to the carrier to initiate their insurance coverage. For ongoing customers (after their first month of fully paid coverage), if a received payment does not bring them within $10 of the balance due, then funds are not transmitted to the carrier to trigger ongoing insurance coverage.

The "Paid Through" field is automatically updated and calculated in CPBS based upon execution of the daily Paid Through Date batch process, after payments are uploaded to the system. These fields are used to indicate to carriers and UHIP that customers have paid for insurance (effective through the "Paid Through" date) and internally, that CPBS is tracking the status as to how far into the future a customer has been billed. The automated updating of these fields helps ensure that account activity is stated correctly on customer statements.

Daily, a Quality Control ("QC") script is run to uncover potential data errors in enrollment and the receipt and application of payments. Identified errors are resolved through CPBS Financial and Technical Operations staff. Correcting entries are either made through the coordination of changes with UHIP or via manual changes made directly by CPBS (with coordination and authorization of UHIP and/or the State of Rhode Island).

System batches are monitored to help ensure completeness and accuracy of posting. In the event that an error occurs, the issue is tracked to resolution in a timely manner. Batch jobs are run on a schedule (daily/weekly/monthly). Job completeness and accuracy is tracked using a daily checklist (Operations Daily Batch Process Log). In the event of a failure, the issue is documented by a member of the Financial Operations Team using the Operations Daily Batch Process Log and is resolved in a timely manner.

4. **Cash and Suspense Reconciliation**

If a payment has been made and it is not specified which account it should be applied to, the payment goes into a suspense account. A payment can go into suspense due to a number of reasons. For example, if the account number on a check or money order is not readable or it is incorrect, there are delays in enrollment from UHIP to CPBS (disallowing the ability to automatically link payments with enrollment records). Another example of payment going into suspense is when the customer omits a payment coupon or lack of other identifying information with payment, or other situations where a single payment may be issued that applies to multiple accounts (and, hence, must be applied manually).

Suspense accounts are automatically matched daily, excluding weekends and holidays, to enrollment accounts via a batch process. When a match occurs (i.e., the account number associated with a payment matches the enrollment data of a customer account), the amount is automatically applied to the matched account.

Suspense entries that are a result of ACH transactions are most often due to the normal and expected process of a one-time ACH payment being provided by a customer on one day, and the corresponding enrollment information being processed the following business day. Such transactions are automatically re-processed with each new enrollment batch that is run, clearing those suspense entries automatically, by applying payments until the amount owed is paid in full, or the payment amount is depleted, with any additional monies being applied to unapplied cash for each respective customer.

The lockbox and scan file are manually checked every day for payments that are in suspense and copies are pulled of these checks. A screenshot of the check shows the name and address of the customer who has paid. The Vice President ("VP") of Operations (or designee) then searches CPBS for corresponding information from a client, and the payment is then transferred from suspense to the matching account if one is found. If no account is matched to a payment in suspense after 30 days, it is added to the list of accounts that NFP Health is unable to resolve. Monthly, the suspense accounts are reviewed again by the VP of Operations (or designee) to help ensure amount discrepancies are resolved completely and accurately. Then, the VP of Operations (or designee) sends a list of the unresolved accounts to the State of Rhode Island and their authorized representatives for further research and helps ensure that suspense accounts are resolved in a timely fashion.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

13

In addition to the monitoring of the suspense account, NFP Health also helps ensure that monies automatically applied to customer accounts are accounted for accurately and completely. On a monthly basis, the COO (or designee) reconciles the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to customer payments. The bank account is matched with customer payments to see if there are any discrepancies. If there are discrepancies, the COO (or designee) researches further into the situation, so it is resolved in a timely manner.

5. **Refund Setup, Authorization and Processing**

Refunds are requested by customers through the UHIP Call Center. There is a HSRI priority team that "pre-qualifies" refund eligibility. The escalation team includes representatives of the State of Rhode Island and the Billing Support Manager for NFP Health, who serves as the refund escalation point of contact at NFP Health.

Ultimately, refunds are approved or denied by the State of Rhode Island. NFP Health's role in the refund process is simply to flag accounts that have requested refunds, with the date, customer name, customer account number and dollar amount. NFP Health also monitors when the State of Rhode Island has finished their due diligence and approved or denied the refund request, on what date the decision was made or a check sent to the customer, and the amount of the check, to help ensure that CPBS always represents the current and valid state of any given account.

NFP Health performs a level of interim due diligence when a refund request is received to confirm that customers are, from all evidence available, eligible for a refund. In order for a customer to be qualified for a refund, they must be disenrolled and have a credit on their account. If customers are pre-considered eligible for a refund, a request for it is processed for the existing credit amount. If customers are pre-considered not eligible, clarification emails are sent so that the parties are aware of the credit balance and that the current status of the account is known.

When a refund request is submitted, CPBS must be checked to confirm the details just described. If the check is successful, the Billing Support Manager sends a spreadsheet that batches together the refund requests for the week. That spreadsheet is sent to the VP of Operations (or designee) with the customer code, customer name, and refund amount. The system helps ensure that the refund amount requested cannot exceed the credit balance available.

The Financial Operations Team then sets up a refund request in CPBS only upon an authorized request through the process mentioned above. These requested refunds are reviewed by the State of Rhode Island and their support staff to help ensure that the refund requests were entered completely and accurately. The State of Rhode Island has access to the current list of unissued refunds on a 24/7 basis through access to reports within CPBS that are available through their UHIP log in credentials. Monthly, the Office of the Chief Financial Officer ("CFO") for HSRI provides the VP of Operations (or designee) with a spreadsheet of requested refunds and whether they have been approved or denied. This data is transmitted to NFP Health through a shared SFTP location. The Office of the CFO is the only entity capable of deciding whether a refund request is approved or denied. If a request is approved, the Office of the CFO issues a check for the customers refund.

The Financial Operations Team finalizes the process by capturing the approval, denial or cancellation of refunds. Monthly, the Financial Operations Team reviews the refunds to help ensure that they were authorized and recorded properly.

6. **Reporting**

   Reporting to Carrier

   A monthly process is run by operations, to determine what payments received by UHIP should be submitted to the carrier, using industry standard EDI file, "820" format. EDI "820" files are a standard format for payment transactions that are transmitted to the carriers to indicate the payments that are received. This process is run after the due date cut-off for the month (the 23rd of the month), and at the end of the monthly billing process (the 25th of the month). This carrier payment process summarizes payments and payment reversals (rejected payments) that have occurred prior to the run date of the process, and to determine effective day of coverage for each customer. Monthly, the Financial Operations team issues "820" reports to the Office of the CFO of HSRI for review prior to sending to carriers. The Financial Operations team holds the "820" reports from the carriers until written approval from the CFO's office.

   QC scripts are run for each carrier to confirm transactions have been imported completely and accurately prior to creating the EDI "820" files.

   The information provided in an 820 file includes customer code, subscriber code, plan code, customer name, paid through date, and premium. There are separate reports created and QC scripts run for each carrier; each one sums the premiums so that discrepancies can easily be found by matching the "820" total to the carrier's expected sum.

   Corresponding "read-mode" "820" files are generated for review by the State of Rhode Island, who ultimately is responsible for releasing the payment from the Exchange to each carrier.

   The "read-mode" "820"s are shared with the State of Rhode Island by the VP of Operations (or designee) using an SFTP location shared specifically for these purposes. The State of Rhode Island representatives are notified of the file being posted via email.

   Authorization to send the machine readable 820s to carriers comes from the CFO for the Exchange via email prior to the release of the funds. Once approved, the "820"s are uploaded to the carriers FTP servers.

   Any questions or concerns raised by the carriers, based on receipt of the machine or human readable 820s that are relevant to their business, are fielded via email by the operations team and resolved/reconciled as the need arises.

   Reporting to the State of Rhode Island

   On a monthly basis, NFP Health prepares journal entries covering invoices generated and write-offs, cash receipts and returned payments, accounts receivable, refunds and premium payments to carriers. The journal entries are in a specifically designed Excel format to enable the Exchange financial team to import directly into their accounting system, QuickBooks.

   In addition, files are generated showing the detail customer activity corresponding to each journal entry. The details include the customer code, subscriber code, plan code, payment id, payment method, transaction date and amount. These files are uploaded to the Exchange's Sharefile server.

   NFP Health prepares the report which reconciles the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to customer payments on a monthly basis. Any discrepancies are investigated and resolved.

7. **Backups**

   NFP Health uses a multi-tiered approach to system backups:

   • Local: snapshots of virtual machines are backed up locally and retained for 14 days rolling.

   • Denver: asynchronous data volume replication to the Denver colocation facility every 10 minutes.

   • Offsite: daily, NFP Health's NetApp volumes are backed up (snap-vaulted) to a third-party service, Net2Vault, where backups are kept indefinitely or until the number of maximum snap-vaults are reached (256).

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

15

Full backups are automatically scheduled on a daily basis and replicated offsite. Backups are monitored daily by email alerts and daily review of backup logs. Backup status (success / failure) is tracked on a weekly Technology Operations checklist. In the event of a failure, the issue is documented using the Technology Operations checklist and resolved within 24 hours.

Restore test is performed at least annually by restoring a production virtual machine snapshot (backup) to the Denver data center. Once restored, the virtual machine is checked for file integrity and consistency.

Access to backups is limited to appropriate users based on their role and responsibility with the organization.

8. **Logical Security**

When a new employee is on boarded at NFP Health or a change in access is required for an existing employee, access to CPBS, database and the network is granted after the employee's manager completes the new user access form and submits it to the Technology Operations Department. The form requires that the employee's level of access for each system and application to be defined. Additionally, the employee's start date or access change date must be defined along with the signature of the employee's direct report requesting the access. The Technology Operations Department is responsible for granting permissions for CPBS, database and network access and access is updated based on the employee's business unit and function.

When an employee leaves or is terminated at NFP Health, access to CPBS, databases and network are revoked after the employee's manager completes the end user access form and submits it to the Technology Operations Department. The Technology Operations Department is responsible for revoking permissions for CPBS, database and network access within one business day.

Administrative access to the Active Directory ("AD"), CPBS and CPBS database is restricted to appropriate personnel. Password parameters for the network and CPBS are configured in accordance with the Information Technology Policy.

Annually, the IT department conducts a user access review for the network, CPBS and database with department managers to help ensure access rights are still appropriate. As a result of the review, any access deemed to be inappropriate is modified. The review of user access is to determine the following:

- That only active employees have access to CPBS, databases and the network.

- That active employee access is accurate and appropriate based on their role / responsibilities.

- That terminated employee's access has been revoked and their accounts removed from CPBS, databases, and the network.

Network Security

NFP Health leverages multiple layers of security to protect its infrastructure and applications at the network layer, Cisco ASA firewalls and Cisco Intrusion Detection System ("IDS/IPS") maintain perimeter security. Firewall rule sets are configured to limit and control inbound and outbound internet traffic. Triggers are configured to send alerts. F5 Big IP Application Security Managers ("ASM/WAF") protect applications and databases from application layer attacks. Logs for these devices are monitored daily to track attempts to penetrate the network and web applications. Access to these devices is limited to the Technology Operations Manager and the Technology Operations System Engineer.

Penetration testing is conducted at least annually by a third-party network security contractor. The contractor issues their findings to the Technology Operations Manager who then oversees the remediation of any discovered vulnerabilities.

Remote access to NFP Health's networks is provided to the authorized personnel by secure Virtual Private Network ("VPN") using Cisco's VPN Client.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

16

Operating System Security

Operating systems security is managed through AD. Domain users' privileges are defined by membership to AD security groups, which allow users to access a specific area or application within the domain. Membership to security groups is determined by the user's job function and responsibilities. Administrative access to operating systems is restricted to authorized personnel. Authorized personnel belong to the domain administrators' security group.

Database Security

Databases inherit the AD security settings, for authorization and authentication, such that database users' privileges are defined by AD group membership. These AD security groups include read only, read and write, and SQL administrator. Membership to security groups is determined by the user's job function and responsibilities. Sensitive tables in the database, including those listing SSNs, are encrypted with a 1024-bit RSA key.

Application Security

CPBS is secured by application-based user management. User account information and sensitive data is stored and encrypted in the CPBS SQL database. User permissions are determined by an employee's role and responsibilities within the organization.

Webster Bank

The State of Rhode Island provides NFP Health with access to Webster Banks' SFTP portal to transfer ACH, Lockbox, non-sufficient funds ("NSF") and scanned check files. User access to the Webster Bank portal is restricted to appropriate personnel based on job responsibilities.

9. **Change Management**

Internal system and application changes are governed by a strict change management procedure, which prescribe infrastructure and application changes to be authorized by the senior manager overseeing infrastructure and application development. Requested changes are documented and authorized prior to commencement of development. The Technology Operations System Engineer or Vice President approves database and operating system changes; the Release Management Lead or Vice President approves application changes.

Authorized changes are documented using NFP Health's paper-based change management form. This form tracks change details that include the requesting party, the type of change (complex or non-complex), the application or systems that are changing, the details of the change and the level of risk associated with the implementation of the change. Additional details include a back-out plan, a verification plan, downstream impact and the quality assurance process. The form also documents formal approval of the change along with acceptance of the change confirming that it was implemented successfully.

For application development and infrastructure changes, changes are first implemented and tested in the following environments: development, quality assurance and staging. For infrastructure changes, changes are tested at the Denver (disaster recovery/secondary) data center before they are approved and implemented at the Marlborough (production/primary) data center. As changes are approved for production, a limited number of team members on the technology team are allowed to make approved changes. Responsibilities are segregated based on employees' responsibilities.

Once changes have been internally approved and documented in the NFP Health change management form, they are submitted via email and a Deloitte JIRA/Azure DevOps ticket is initiated and submitted to be reviewed by Deloitte and the State of Rhode Island Change Control Board ("CCB"). Once the change is approved by Deloitte and CCB, a formal maintenance window is scheduled; approved changes are then implemented and validated/accepted during that window. Individuals with development responsibilities cannot migrate changes to production environment.

In the event that a job schedule needs to be altered, the request to alter must follow the standard change management process. Leveraging the NFP Health Change Management form, changes to job schedules involves acceptance, testing and approval from the Technology Operations System Engineer or Vice President.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

17

NFP Health disables all developer accounts and only enable them on an as needed basis. If Admin access is needed, developers open an IT ticket stating what server access is needed, justification and duration of access. Ticket have a subject line of "Access Required", which is automatically filtered and grouped for ease of management. Once the time have elapsed the requested duration Infrastructure personnel disable the account, put a resolution note that state it is disabled or a note on the ticket itself that it was disabled. Infrastructure personnel reviews the grouped access tickets daily (except for holidays and weekends) to ensure access was granted and disabled as requested and required.

E. Additional Information about Management's Description

NFP Health has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives and related controls are presented within Section IV of this report, "Description of NFP Health Services Administrators' Control Objectives and Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results." and are an integral component of NFP Health's description of its system as described within this section.

F. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The accompanying description includes only the policies, procedures, and control activities at NFP Health and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control over financial reporting must be evaluated in conjunction with NFP Health's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Table 1

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Deloitte Consulting LLP	Responsible for development of the UHIP system technology, hosting services, ongoing maintenance, fulfilling requested enhancements, as well as payment processing through an integrated financial management system. The following control areas are critical to achieving the applicable control objectives: • IT General Computer Controls around the UHIP system provided to NFP Health; and • Reconciliation controls to ensure payment and refund information provided are complete and accurate. In addition, NFP Health has identified the following controls to help monitor the subservice organization: • On an annual basis, management reviews access to the third-party data centers; and • On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.	Control Objectives 1*, 2*, 3*, 4*, 5*, 7*, 9*, 10*

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Rackspace Technology Inc. (f/k/a TriCore Solutions)	Responsible for providing 24/7/365 monitoring and management of NFP Health's databases. The following control areas are critical to achieving the applicable control objectives: • IT General Computer Controls around NFP Health's system databases provided to NFP Health. In addition, NFP Health has identified the following controls to help monitor the subservice organization: • On an annual basis, management reviews logical access to the third-party data centers, and applications and databases; and • On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.	Control Objectives 7*, 8*, 9*
Net2Vault LLC	Responsible for providing offsite, encrypted SAN to SAN backups of NFP Health's NetApp storage platforms. The following control areas are critical to achieving the applicable control objectives: • IT General Computer Controls around the NFP Health's system back up processes and related data. In addition, NFP Health has identified the following controls to help monitor the subservice organization: • On an annual basis, management reviews logical access to the third-party NetStorage platform and data centers • On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.	Control Objective 7*
TierPoint, LLC	Responsible for colocation data center services, specifically for the hosting of NFP Health's production IT infrastructure and CPBS system and data. The following control areas are critical to achieving the applicable control objectives: • Controls around the physical security of the data center hosting the production IT infrastructure and CPBS system; and • Controls, including environmental controls, around the protection of the data center environment to support the production processes.	Control Objectives 1*, 2*, 3*, 4*, 5*, 6*, 7*, 8*, 9*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
	In addition, NFP Health has identified the following controls to help monitor the subservice organization:	
	• On an annual basis, management reviews logical access to the third-party data centers, and applications and databases; and	
	• On an annual basis, Management reviews TierPoint's SOC 2 attestation report to gain assurance over the TierPoint, LLC control environment.	
CenturyLink	Responsible for colocation data center services, specifically for the hosting of NFP Health's backup IT infrastructure and CPBS system and data.	Control Objectives 1*,2*,3*,4*,5*,6*,7*, 8*, 9*
	The following control areas are critical to achieving the applicable control objectives:	
	• Controls around the physical security of the data center hosting the backup IT infrastructure and CPBS system; and data and	
	• Controls, including environmental controls, around the protection of the data center environment to support the backup processes, IT infrastructure, CPBS system and data.	
	In addition, NFP Health has identified the following controls to help monitor the subservice organization:	
	• On an annual basis, management reviews logical access to the third-party data centers, and applications and databases; and	
	• On an annual basis, management evaluates the performance of the third-party organization to help ensure the compliance with commitments and agreed-upon service level agreements.	

* The achievement of design and operating effectiveness for this particular control objective assumes that complementary controls at this subservice organization are in place and are operating effectively to support and achieve this control objective.

G. User Entity Controls

NFP Health's controls relating to the system cover only a portion of the overall internal control structure of HealthSource RI. It is not feasible for the control objectives to be solely achieved by NFP Health. Therefore, the user entity's internal control over financial reporting must be evaluated in conjunction with NFP Health's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated control objective(s) are included within the table below.

Management has highlighted control objectives in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for HealthSource RI to rely on the controls reported on herein, HealthSource RI must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes HealthSource RI should consider in developing their internal controls over financial reporting that are relevant to the Company's controls detailed in this report; however, such control considerations are not required to achieve design or operating effectiveness for the control objective. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and HealthSource RI. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities that provide a basis for the assertions underlying the financial statements and control environments for HealthSource RI.

User Entity Controls	Associated Control Objective(s)
HealthSource RI is responsible for completing requested information at enrollment and for providing NFP Health with the correct information to complete their enrollment.	Control Objectives 1*, 2*, 3*
HealthSource RI is responsible for ensuring the robustness of their own finances for completion of enrollment.	Control Objective 1
HealthSource RI is responsible for regularly reviewing their bank accounts, including monthly bank statements.	Control Objectives 4, 5
HealthSource RI is responsible for providing notification to NFP Health in the case of personal information changes.	Control Objectives 1*, 2*, 5*
HealthSource RI is responsible for providing notification to NFP Health of approval and denial of refunds.	Control Objective 5*
HealthSource RI is responsible for their own 3rd party representatives to review payments and eligible customers prior to the release of the funds to carriers.	Control Objective 6
HealthSource RI is responsible for approving all program changes made to CPBS prior to release into production.	Control Objective 9*

* This is a complementary control and is required to achieve design and operating effectiveness for this particular control objective.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

21

IV. Description of NFP Health Services Administrators' Control Objectives and Related Controls, and the Independent Service Auditor's Description of Tests of Controls and Results

A. Types and Descriptions of the Tests of Operating Effectiveness

This report, when combined with an understanding of the controls at the user entity and subservice organizations, is intended to assist auditors in planning the audit of the user entity's financial statements or the user entity's internal control over financial reporting and in assessing control risk for assertions in the user entity's financial statements that may be affected by controls at NFP Health.

Our examination was limited to the control objectives and related controls specified by NFP Health in Sections III and IV of the report and did not extend to the controls in effect at the user entity and subservice organizations.

It is the responsibility of the user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the total internal control environment. If the internal controls are not effective at a user entity, NFP Health's controls may not compensate for such weaknesses.

NFP Health's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by NFP Health. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by NFP Health, we considered aspects of NFP Health's control environment, risk assessment process, monitoring activities, and information and communications. The following table clarifies certain terms used within this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control

In addition, when using information produced (or provided by) the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

B. Control Objectives, Control Activities, and Tests Performed

Control Objective 1		
Controls provide reasonable assurance that new customers are set up completely and accurately on Core Premium Billing Services system.		
Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
1.1 Daily, NFP Health receives batches of new and existing customer activity from the Rhode Island UHIP. Any identified issues are researched and resolved. Small group ("SHOP") enrollments come from HSRI for employers 2.0 system.	**Inspection:** Inspected the daily batch process log and email communications for a sample of days to determine that NFP Health received new and existing customer activity from the Rhode Island UHIP, and any identified issues were researched or resolved.	No exceptions noted.
1.2 Each business day, carriers are notified via a 834 file of SHOP enrollment/changes to activate or amend a policy.	**Inspection:** Inspected the business day batch process log for a sample of business days to determine that carriers were notified via 834 file of enrollment and changes to activate or amend a policy.	No exceptions noted.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying
Report of Independent Service Auditors.

23

	Control Objective 2		
	Controls provide reasonable assurance that customer billing statements are generated for customers on a daily and monthly basis by the Financial Operations Team and are made accessible to clients.		
	Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
2.1	New customers' initial billing statements are generated on a daily basis by the Financial Operations Team and are made accessible to clients.	**Observation:** Observed the customer billing statement configurations to determine that new customers' initial billing statements were configured to be generated daily for relevant customers and made accessible to clients through the CPBS web portal. Further, inquired of the Program Manager to determine that the customer billing statement configurations were in place to generated customer billing statements and make them available to clients daily throughout the specified period.	No exceptions noted.
		Inspection: Inspected the billing statements for new customers for a sample of days and to determine that new customers' billing statements were generated and made accessible to clients on a daily basis.	No exceptions noted.
2.2	Monthly, customer statements are posted to the UHIP website by the Financial Operations Team where they are accessible to clients and subsequently reconciled by the Financial Operations Team. Failures are tracked to resolution.	**Observation:** Observed the customer statement configurations to determine that customer statements were configured to be generated and automatically posted to the UHIP website on a monthly basis. Further, Inquired of the Program Manager to determine that customer statements configurations were in place to generate and poste the statements to the UHIP website on a monthly basis throughout the period.	No exceptions noted.
		Inspection: Inspected the customer statements on the UHIP website, email confirmations and reconciliation performed for a sample of months to determine that customer statements were uploaded and posted to the UHIP website by the Financial Operations Team and that a reconciliation was performed and failures were tracked.	No exceptions noted.

Control Objective 3			
Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.			
	Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
3.1	Batch payments are processed and uploaded to CPBS each business day. Any identified issues are tracked and resolved by the Financial Operations Team to ensure data is entered completely and accurately.	**Observation/Inquiry:** Observed the batch payment configurations to determine that batch payments were processed and uploaded to CPBS each business day. Further, inquired of the Program Manager to determine that batch payments were processed and uploaded to CPBS each business day throughout the period.	No exceptions noted.
		Inspection: Inspected the batch monitoring emails and logs for a sample of business days to determine that any identified issues were tracked and resolved by the Financial Operations Team to ensure data was entered completely and accurately.	No exceptions noted.
3.2	Payments on accounts are automatically applied based upon unique client identifiers. In the event that automated postings do not occur, the activity is posted to a suspense account.	**Observation/Inquiry:** Observed the payment configurations to determine that payments were automatically applied based upon unique client identifiers. Further inquired of the VP of Operations to determine that payments configurations were in place to automatically apply payments on accounts based upon unique client identifiers throughout the specified period.	No exceptions noted.
		Observation/Inquiry: Observed the suspense account configurations to determine that in the event that automated postings did not occur, the activity was posted to a suspense account. Further inquired of the Program Manager to determine that payment configurations were in place to post the activity to a suspense account in the event that automated postings did not occur throughout the specified period.	No exceptions noted.
3.3	If a payment is received in excess of the amount due, the excess amount is automatically applied as a credit balance towards the next month's billing.	**Observation/Inspection:** Observed the payment configurations and a sample of an overpayment to determine that if a payment received was in excess of the amount due, the excess amount was automatically applied as a credit balance towards the next month's billing. Further, inquired of the Program Manager to determine that the payment configurations were in place to apply excess amounts as credit towards the next month's billing throughout the specified period.	No exceptions noted.

Control Objective 3			
Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.			
	Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
3.4	If a received payment is short more than $10 (for ongoing customers) and more than $5 (for initial customers) of the balance due, then funds are not transmitted to the carrier for insurance renewal.	**Observation/Inquiry:** Observed the payment configurations to determine that if the received payment was short more than $10 for ongoing customers and more than $5 for initial customers of the balance due, the funds were not transmitted to the carrier for insurance renewal. Further, inquired of the Program Manager that the configurations for short payments were in place throughout the specified period.	No exceptions noted.
3.5	After payments are uploaded, the Paid Through field is automatically updated and calculated in CPBS based upon execution of the Paid Through Date batch process each business day.	**Observation/Inquiry:** Observed the Paid Through configurations and a sample of payment uploaded to determine that the system automatically updated and calculated the Paid Through field. Further, inquired of the Program Manager to determine that Paid Through configurations were in place throughout the specified period.	No exceptions noted.
		Inspection: Inspected the daily batch process logs for a sample of business days to determine that the Paid Through batch process was executed daily after payments were uploaded.	No exceptions noted.
3.6	A QC script is run to uncover potential data errors each business day. Identified errors are resolved.	**Observation/Inquiry:** Observed the QC script to determine that the script was run to uncover potential data errors each business day. Further, inquired of the Program Manager to determine that the QC script was configured to run each business day throughout the specified period.	No exceptions noted.
		Inspection: Inspected the QC script logs for sample of business days to determine that any identified errors were resolved.	No exceptions noted.
3.7	Batch ACH returns, including NSF, are processed and uploaded to CPBS each business day. Any issues are tracked and resolved by the Financial Operations Team to ensure data is entered completely and accurately.	**Observation/Inquiry:** Observed the ACH return upload configurations to determine that batch ACH returns were configured to be processed and uploaded to CPBS each business day. Further, Inquired of the VP of Operations to determine that batch ACH returns were configured to be processed and uploaded each business day throughout the period.	No exceptions noted.

Control Objective 3		
Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.		
Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
	Inspection: Inspected the Batch ACH returns processed in CPBS to determine that batch ACH returns were processed and uploaded to CPBS each business day, and that any issues were tracked and resolved by the Financial Operation Team.	No exceptions noted.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

27

Control Objective 4			
Controls provide reasonable assurance that cash is completely and accurately reconciled between the Core Premium Billing Services system and the State of Rhode Island's Webster Bank account in a timely manner.			
	Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
4.1	Monthly, suspense accounts are reviewed by the VP of Operations and/or designee to help ensure amounts are resolved completely and accurately.	**Inspection:** Inspected the end of month Suspense Accounts review for a sample of months to determine that suspense accounts were reviewed by the VP of Operations and/or designee to help ensure amounts were resolved completely and accurately.	No exceptions noted.
4.2	Monthly, the Chief Operations Officer ("COO") and/or designee reconciles the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to customer payments. Any discrepancies are investigated and resolved.	**Inspection:** Inspected the reconciliations and e-mail communications for a sample of months to determine that the COO and/or designee reconciled the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to the customer payments.	No exceptions noted.
4.3	Suspense accounts are automatically searched for matches to an account by ACH or check. When a match occurs, the amount is automatically applied to the matched account.	**Observation/Inquiry:** Observed the suspense payment configurations and the customer payment table to determine that suspense accounts were automatically searched for matches to an account by ACH check, and when a match occurred the amount was automatically applied to the matched account. Further, inquired of the Program Manager to determine that the suspense accounts configurations were in place to automatically apply to matched accounts throughout the specified period.	No exceptions noted.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

28

Control Objective 5			
Controls provide reasonable assurance that insurance premium refunds are authorized and recorded accurately.			
	Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
5.1	The Financial Operations Team sets up a refund request in CPBS only upon authorized request from the Exchange.	**Observation/Inquiry:** Observed an example refund request set up in CPBS to determine that the Financial Operations Team set up a refund request in CPBS after receiving an authorized request from the exchange. Further, inquired of the VP of Operations to determine that refund requests were only set up in CPBS after an authorized request was received throughout the period.	No exceptions noted.
		Inspection: Inspected the refund request and CPBS output for a sample refund requests to determine that the Financial Operations Team set up a refund request in CPBS only upon authorization from the Exchange.	No exceptions noted.
5.2	Monthly, the Financial Operations Team reviews all refunds to ensure that they were authorized and recorded properly.	**Inspection:** Inspected the Refund Requests and their review for a sample of months to determine that the Financial Operations Team reviewed all refunds to ensure that they were authorized and recorded properly.	No exceptions noted.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying
Report of Independent Service Auditors.

29

Control Objective 6		
Controls provide reasonable assurance that reporting to carriers and the HealthSource RI is performed completely, accurately, and on a timely basis.		
Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
6.1 On a monthly basis, QC scripts are run for each carrier to confirm transactions have been imported completely and accurately.	**Observation/Inquiry:** Observed the QC script to determine that the script ran monthly for each carrier to confirm transactions have been imported. Further, Inquired of the Program Manager to determine that the QC script was configured to run monthly throughout the specified period.	No exceptions noted.
	Inspection: Inspected the Monthly Batch process logs for a sample of months to determine that the QC scripts ran to confirm transactions were imported completely and accurately.	No exceptions noted.
6.2 On a monthly basis, the Operations team sends the "820" report to Rhode Island for approval by the Office of the CFO.	**Inspection:** Inspected email communications for a sample of months to determine that the report was sent to Rhode Island by the Operations team for approval from the Office of the CFO.	No exceptions noted.
6.3 On a monthly basis, the Operations team issues and uploads the "820" reports to the carriers FTP servers once it has been approved.	**Inspection:** Inspected the email communications to the carriers' FTP servers for a sample of months to determine that the Operations team issued and uploaded the "820" reports to the carriers FTP servers once it was approved.	No exceptions noted.
6.4 On a monthly basis, NFP prepares journal entries covering invoices generated and write-offs, cash receipts and returned payments, accounts receivable, refunds and premium payments to carriers.	**Inspection:** Inspected the QuickBooks journal entries for a sample of months to determine that NFP prepared journal entries that covered invoices generated and write-offs, cash receipts and returned payments, accounts receivable, refunds and premium payments to carriers.	No exceptions noted.
6.5 Monthly, the Chief Operations Officer ("COO") and/or designee reconciles the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to customer payments. Any discrepancies are investigated and resolved.	**Inspection:** Inspected the reconciliations and e-mail communications for a sample of months to determine that the COO and/or designee reconciled the daily deposits between CPBS and the State of Rhode Island's Webster Bank account to the customer payments.	No exceptions noted.

Control Objective 7		
Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.		

	Control Activity	Tests Performed By Service Auditor	Results of Testing
7.1	Full backups are automatically scheduled on a daily basis and replicated offsite.	**Observation/Inquiry:** Observed the SnapMirror and SnapVault backup configurations to determine that full backups were configured to run on a daily basis and replicate offsite. Further, inquired of the Manager of Technology Infrastructure to determine that SnapMirror and SnapVault backup were configured to fully backup and replicate daily throughout the period.	No exceptions noted.
7.2	Backups are monitored daily by the Technology Operations System Engineer and automated backup alerts are sent for successes and failures. In the event of a failure of a backup, the issue is tracked to resolution.	**Observation/Inquiry:** Observed the backup alert settings to determine that automated backup alerts were sent upon completion of the backup job for successes and failures. Further, inquired of the Manager of Technology Infrastructure to determine that the backup alerts were configured to automatically send the alerts upon completion of the backup jobs throughout the period.	No exceptions noted.
		Inspection: Inspected the Technology Operations Checklist for a sample of days to determine that backups were monitored by the Technology Operations System Engineer and any issues were tracked to resolution.	No exceptions noted.
7.3	Backups are tested at least annually to verify media reliability and data integrity.	**Inspection:** Inspected the backup restore process to determine that backups were tested at least annually to verify media reliability and data integrity.	No exceptions noted.
7.4	Changes to backup job schedules are documented and approved prior to implementation.	**Inspection:** Inspected the Change Request Control Form for a sample of backup job schedule changes during the specified period to determine that changes were documented and approved prior to implementation for each selected change.	The Service Auditor noted that this control activity did not operate during the specified period, as there were no changes to the backup job schedules during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
		Inspection: Inspected the Backup Job Schedule Changes logs produced SnapVault System to determine that no changes to backup jobs occurred during the specified period.	No exceptions noted.

Control Objective 8		
Controls provide reasonable assurance that logical security to applications, operating systems and databases that may affect user entities internal controls over financial reporting is restricted to authorized and appropriate personnel.		
Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
8.1	System access requests for new employees are submitted by the manager to the IT department. User access is updated based on the employee's business unit and function.	**Inspection:** Inspected the system access requests for sample of new hires to determine that access requests were submitted by the manager to the IT department, and that access was updated based on the employee's business unit and function.	No exceptions noted.
8.2	For terminated employees, the manager sends a system access termination form to IT with the employee's termination date. IT removes access within one business day.	**Inspection:** Inspected the employee termination forms and user access listings for a sample of terminated employees to determine that the manager notified IT of the employee's termination and IT removed access within one business day.	No exceptions noted.
8.3	For transferred employees, the manager sends a notification form to IT and employees' access is updated based on their functions and responsibilities.	**Inspection:** Inspected the transfer forms for a sample of transferred employees to determine that the manager notified IT and access was updated.	The Service Auditor noted that this control activity did not operate during the specified period, as there were no transferred employees during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
		Inspection: Inspected the employee transfer reports produced by the Human Resource Department to determine that no employees were transferred during the specified period.	No exceptions noted.
8.4	Administrative access to the AD, CPBS and CPBS database is restricted to authorized and appropriate personnel.	**Inspection:** Inspected the user access list for the AD to determine that administrative access to AD was restricted to authorized and appropriate personnel.	No exceptions noted.
		Inspection: Inspected the user access list for the CPBS to determine that administrative access to CPBS was restricted to authorized and appropriate personnel.	No exceptions noted.
		Inspection: Inspected the user access list for the CPBS database to determine that administrative access to the CPBS database was restricted to authorized and appropriate personnel.	No exceptions noted.

<table>
<tr>
<td colspan="4">**Control Objective 8**

Controls provide reasonable assurance that logical security to applications, operating systems and databases that may affect user entities internal controls over financial reporting is restricted to authorized and appropriate personnel.</td>
</tr>
<tr>
<th colspan="2">**Control Activity**</th>
<th>**Tests Performed
By Service Auditor**</th>
<th>**Results of Testing**</th>
</tr>
<tr>
<td>8.5</td>
<td>Access to backups is limited to appropriate individuals based upon their role and responsibility.</td>
<td>**Inspection:** Inspected the list of users with access to backups to determine that access was limited to appropriate individuals based upon their role and responsibility.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>8.6</td>
<td>Password parameters for the AD and CPBS are configured in accordance with the Information Technology Policy.</td>
<td>**Observation:** Observed the AD and CPBS password parameters and the Information Technology Policy to determine that password parameters for the AD and CPBS were configured to meet or exceed requirements of the Information Technology Policy.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>8.7</td>
<td>Annually, the IT department conducts a user access review for the AD, CPBS and CPBS SQL database with department managers to help ensure access rights are still appropriate. As a result of the review, any access deemed to be inappropriate is modified.</td>
<td>**Inspection:** Inspected the annual user access review for the AD, CPBS and the CPBS SQL database to determine that the IT department conducted a user access review with department managers to help ensure access rights were appropriate and any access deemed to be inappropriate was modified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>8.8</td>
<td>User access to the Webster Bank portal is restricted to authorized and appropriate personnel.</td>
<td>**Inspection:** Inspected the Webster Bank Access List and the NFP employee listing to determine that access to the Webster Bank portal was restricted to appropriate personnel.</td>
<td>No exceptions noted.</td>
</tr>
</table>

Control Objective 9

Controls provide reasonable assurance that changes or upgrades to applications and infrastructures are documented, tested, and approved prior to implementation to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting and to support user entities' internal control over financial reporting.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
9.1	Application and infrastructure change requests are documented and authorized prior to commencement of development.	**Inspection:** Inspected the application change approval list for sample of application changes to determine that application change requests were documented and authorized prior to commencement of development.	No exceptions noted.
		Inspection: Inspected the Information Technology Change Request Control forms for a sample of infrastructure changes to determine that infrastructure change requests were documented and authorized prior to commencement of development.	No exceptions noted.
9.2	Application and infrastructure change requests are tested prior to implementation to production.	**Inspection:** Inspected the application change tickets and release schedule for a sample of application changes to determine that application change requests were tested prior to implementation to production for each selected application change.	No exceptions noted.
		Inspection: Inspected the Information Technology Change Request Control forms for a sample of infrastructure changes to determine that infrastructure change requests were tested prior to implementation to production for each selected infrastructure change.	No exceptions noted.
9.3	Separate development, testing, and production environments are in place.	**Observation/Inquiry:** Observed the system to determine that separate development, testing, and production environments were in place. Further, inquired of the Systems Engineer to determine that separate environments were in place throughout the period.	No exceptions noted.
9.4	Application and infrastructure change requests are approved prior to implementation to production.	**Inspection:** Inspected the application change release log for a sample of application change releases to determine that application change releases were approved prior to implementation to production.	No exceptions noted.
		Inspection: Inspected the application change release log for a sample of infrastructure change releases to determine that infrastructure change releases were approved prior to implementation to production.	No exceptions noted.

Control Objective 9
Controls provide reasonable assurance that changes or upgrades to applications and infrastructures are documented, tested, and approved prior to implementation to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting and to support user entities' internal control over financial reporting.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
9.5	Users with ability to update changes to CPBS are based on users job responsibilities and properly authorized, and monitored.	**Inspection:** Inspected the users with the ability to update changes to CPBS and the employee listing to determine that users with the ability to update changes to CPBS had access based on job responsibilities and were properly authorized and monitored.	No exceptions noted.
		Observation: Observed the Netwrix Auditor tool settings to determine that the tool was configured to record and monitor activity of users in the production environment. Further, inquired of the Technology Infrastructure Manager to determine that access monitoring was in place effective November 2019.	No exceptions noted.
		Inspection: Inspected a sample of ticket for production access request by the development team member to determine that when Admin access was needed, developers opened an IT ticket stating what server access is needed, justification and duration of access.	No exceptions noted.
		Inspection: Inspected the IT daily checklist for a sample of days to determine that management reviewed tickets to help ensure there are production access to CPBS was disabled within timeframe that was requested and granted.	No exceptions noted.
9.6	The Release Management Team organizes bi-weekly development meetings, led by the Release Management Lead to communicate requirements, change requests and report progress. All members of the team, including developers, testers, business specialists, infrastructure and operations, attend these mandatory meetings.	**Inspection:** Inspected the change meeting minutes for a sample of weeks to determine that the change committee met to discuss change projects and releases and documented key decisions in the minutes at least biweekly.	No exceptions noted.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying
Report of Independent Service Auditors.

35

Grant Thornton