BerryDunn

NFP | Health

REPORT ON CONTROLS AT A SERVICE ORGANIZATION
SOC 1® TYPE 2 FOR

NFP Health Services Administrators Rhode Island

For the Period July 1, 2023 – June 30, 2024

BerryDunn

CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of
NFP Health Services Administrators
Braintree, MA

SCOPE

We have examined management of NFP Health Services Administrators' (NFP Health) description of its Core Premium Billing Services (CPBS) system provided to HealthSource Rhode Island (HSRI) entitled "Management of NFP Health's Description of Its System" for processing user entities' transactions throughout the period July 1, 2023 to June 30, 2024 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Management of NFP Health's Assertion" (assertion). The controls and control objectives included in the description are those that management of NFP Health believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

NFP Health uses subservice organizations to monitor and manage NFP Health's databases, encrypt off-site backups of NFP Health's VMware virtualization platforms, host production information technology (IT) infrastructure, host backup IT infrastructure, and aid in the development, hosting, and ongoing maintenance of the Unified Health Infrastructure Project (UHIP) system. The description includes only the control objectives and related controls of NFP Health and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by NFP Health can be achieved only if complementary subservice organization controls assumed in the design of NFP Health's controls are suitably designed and operating effectively, along with the related controls at NFP Health. 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 NFP Health's controls are suitably designed and operating effectively, along with related controls at the service organizations. 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 2, NFP Health has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Management of NFP Health 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 period July 1, 2023 to June 30, 2024. 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

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

INHERENT LIMITATIONS

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. 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 4.

OPINION

In our opinion, in all material respects, based on the criteria described in management of NFP Health's assertion,

1. the description fairly presents the system that was designed and implemented throughout the period July 1, 2023 to June 30, 2024.
2. 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, 2023 to June 30, 2024, and the subservice organizations and user entities applied the complementary controls assumed in the design of NFP Health's controls throughout the period July 1, 2023 to June 30, 2024.
3. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2023 to June 30, 2024, if complementary subservice organization and user entity controls assumed in the design of NFP Health's controls operated effectively throughout the period July 1, 2023 to June 30, 2024.

RESTRICTED USE

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of NFP Health, user entities of NFP Health's system during some or all of the period July 1, 2023 to June 30, 2024, and their auditors who audit and report on such user entities' 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 user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Berry Dunn McNeil & Parker, LLC

Manchester, New Hampshire
August 12, 2024

SECTION 2

MANAGEMENT OF NFP HEALTH'S ASSERTION

MANAGEMENT OF NFP HEALTH'S ASSERTION

We have prepared the description of NFP Health Services Administrators' (NFP Health) Core Premium Billing Services (CPBS) system provided to HealthSource Rhode Island (HSRI) entitled "Management of NFP Health's Description of Its System," for processing user entities' transactions throughout the period July 1, 2023 to June 30, 2024 (description) for user entities of the system during some or all of the period July 1, 2023 to June 30, 2024 and their auditors who audit and report on such user entities' 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 user entities themselves, when assessing the risks of material misstatement of user entities' financial statements.

NFP Health uses subservice organizations to monitor and manage NFP Health's databases, encrypt off-site backups of NFP Health's VMware virtualization platforms, host production information technology (IT) infrastructure, host backup IT infrastructure, and aid in the development, hosting, and ongoing maintenance of the Unified Health Infrastructure Project (UHIP) system. The description includes only the control objectives and related controls of NFP Health and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by NFP Health can be achieved only if complementary subservice organization controls assumed in the design of NFP Health's controls are suitably designed and operating effectively, along with the related controls at NFP Health. The description does not extend to 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 NFP Health's controls are suitably designed and operating effectively, along with related controls at the service organizations. The description does not extend to controls of the user entities.

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

1. The description fairly presents the system made available to user entities of the system during some or all of the period July 1, 2023 to June 30, 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
    a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
        i. the types of services provided, including, as appropriate, the classes of transactions processed;
        ii. 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 user entities of the system;
        iii. 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 user entities;

iv. how the system captures and addresses significant events and conditions other than transactions;

v. the process used to prepare reports and other information for user entities;

vi. services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them;

vii. the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the controls;

viii. 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.

b. Includes relevant details of changes to the system during the period covered by the description.

c. Does not omit or distort information relevant to the system, acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2023 to June 30, 2024 to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of NFP Health's controls throughout the period July 1, 2023 to June 30, 2024. The criteria we used in making this assertion were that:

a. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

b. 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.

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

Laura L. Wood

Laura Wood, Chief Operating Officer
NFP Health Services Administrators
August 12, 2024

SECTION 3

MANAGEMENT OF NFP HEALTH'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF SERVICES PROVIDED

NFP Health provides Core Premium Billing Services (CPBS) to the State of Rhode Island (RI) under a subcontract with Deloitte Consulting, LLP (Deloitte). Since January 2013, Deloitte has been engaged in delivering the Unified Health Infrastructure Project (UHIP) system on behalf of the State of RI. In delivering this project, Deloitte designs, develops, implements, and operates a technology platform and system to support a statewide Health Insurance Exchange under the Patient Protection and Affordable Care Act. The scope of this report is limited to NFP Health only; Deloitte's systems and services are not in scope of this report.

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

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

As part of this subcontract, NFP Health provides CPBS and staff to support financial management services. These services include:

- Processing system with batch and real-time integration with RI State Health Insurance Exchange (HIX). HIX is a service available in every state that helps individuals, families, and small businesses shop and enroll 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 the payments 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

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, AND MONITORING

CONTROL ENVIRONMENT

Executive Management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures. Management recognizes its responsibility for establishing and maintaining sound internal controls and promoting integrity and ethical values to all personnel.

NFP Health's 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. It is the foundation for all other components of internal control, providing both discipline and structure.

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.

Organizational Structure

NFP Health's 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), President, Chief Operations Officer (COO), and Chief Information Officer (CIO). The Executive Management Team's responsibilities 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

Additionally, 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 fulfill 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 specific job functions. As a result, each position at NFP Health has a pre-defined set of technical

expertise and personal skills needed for each level of employment. These competency requirements are communicated to personnel and candidate employees during the hiring process and help to ensure that current and new employees are qualified for their position.

Several teams help support the solution; they include:

- **Implementation Team:** The team is managed by the Implementation Lead. The Implementation and Project Management Office (PMO) is in constant contact with the client, determining requirements, reporting progress, and procuring feedback.
- **PMO:** The PMO is responsible for recording minutes of each meeting, including the bi-weekly development meetings, and tracking the status using a 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 the status of tickets through resolution.
- **Financial Operations Team:** The Financial Operations Team, consisting of Finance and Billing Specialists, the Call Center Team, Project Specialists, 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.
- **Product Development Team:** This team is responsible for working with the PMO to help ensure requirements are clearly documented and translated into well-functioning and secure software applications to support the solution.
- **Release Management Team:** The 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 to report progress. Developers, testers, business specialists, infrastructure and operations, attends these mandatory meetings. Each member may communicate status and report any issues encountered.
- **Technology Operations Team:** This team is led by the Technical Program Director, who oversees information security, privacy, and infrastructure. The team consists of the Director of Information Security, Risk and Compliance, and the Information Technology 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 the organization's data.
- **Call Center Team:** The team is governed by standard operating procedures established by the client, coupled with NFP Health best practices. Call recording is utilized for quality assurance.

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 also clearly defined and available to the employees.

When a new employee joins NFP Health, they participate in a series of training sessions on 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, appropriate references are 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 relevant knowledge and skills.

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 ongoing professional development opportunities. Both are encouraged to engage in ongoing performance feedback discussions and evaluations throughout the year.

RISK ASSESSMENT

Risk assessments 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 the risk assessment processes is on both the ongoing operations and maintenance of the current system and evaluating new enhancements, fixes, or other changes to the system in order to prevent placing core functionality and customer-facing capabilities at risk.

For Technical Operations, the 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 before the promotion of code into production to confirm that performance or response issues are not anticipated, and that the functionality provided produces the results expected by the client.

For Financial Operations, the risk assessment is conducted by using practices established by 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.

MONITORING

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 of systems for performance is handled through third-party distributed remote agents that provide real-time alerts of

any issues detected from outside of the data center. A second layer of monitoring is used to monitor internal networks, applications, and databases via independent third-party solutions.

System performance is tracked and reported to the client monthly, 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

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

SELECTION AND DEVELOPMENT OF CONTROL ACTIVITIES

Control activities are a part of the process by which NFP Health stive to achieve its business objectives. NFP Health has applied a risk management approach to the organization to select and develop control objectives. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

NFP Health's control objectives and related control activities are included below and in Section 4 of this report.

The description of the independent service auditor's tests of operating effectiveness and the results of those tests are also present in Section 4, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

NEW CUSTOMER SETUP AND MODIFICATIONS

CONTROL OBJECTIVE

Control Objective 1: Controls provide reasonable assurance that new customers are set up completely and accurately on CPBS system.

New Customer Setup and Modifications

NFP Health receives batches of new and existing customer activity from the RI 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 CPBS from UHIP, using Electronic Data Interchange (EDI) files.

These files are reviewed daily via a combination of quality control (QC) queries and by Financial Operations personnel, who look for known issues that are fixed upon identification. This helps ensure that customer data comes across completely and accurately for further payment and billing processing. If an error is noted, the event is tracked through resolution within 24 hours by sending an EDI 999 response file to UHIP. The EDI 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 identification (ID) is created by the 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 are split into separate systems and separate databases, where SHOP enrollments originate in the NFP Health SHOP enrollment portal. As with the 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 of any errors being sent to the Information Technology (IT) team.

The EDI 834 file is a benefits enrollment and maintenance file to add, remove, or update customer's enrollment information. For SHOP enrollments only, daily (excluding weekends and holidays), the carriers are notified via an EDI 834 file of new SHOP enrollment and changes to activate or amend the policy. This process includes identifying add/changes/terminations in the SHOP CPBS system, extracting them, and formatting them as 834 EDI files. EDI files are delivered to the carriers, with full logging and error notification enabled. File failures are researched and resolved by the IT team. Individual enrollments are sent to carriers directly by UHIP.

Daily emails indicating that EDI 834 files 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 EDI 834 files to carriers are analyzed each business day. Finally, SLA reporting is performed monthly to the client to

indicate EDI 834 files were sent daily, excluding weekends and holidays. This report also includes information indicating when an EDI 834 file was not sent to a carrier because no enrollment data needs existed on that business day.

BILLINGS

CONTROL OBJECTIVE

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.

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 initial enrollment, this initial statement shows the payment and current amount due. The billing statement further reflects the payment status and totals for the first month's premium lines. These are produced daily for the relevant customers only after the enrollment information is processed through the standard daily enrollment batches. 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 the State of RI directive or to match business days vs. calendar days. For example, if the 25th falls on a Saturday or Sunday, the State of RI can decide to bill on the Friday before or following Monday. 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 Extensible Markup Language (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. A request to transform the statements into electronic portable document format (PDF) file, and then a hard copy is generated. As part of the transformation, the mail house creates a unique scanline for 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.

TRANSACTION PROCESSING

CONTROL OBJECTIVE

Control Objective 3: Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.

Transaction Processing

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

Payments are handled in two steps. The first step is receiving 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 so long that it is received with sufficient time to process before the daily 5 pm. 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. However, 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. CPBS processes this report, 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 for 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 before the ACH batch process being run.

Checks or money orders that the bank processes through the lockbox and remote scanner 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 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. 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.

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 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 RI).

System batches are monitored to help ensure completeness and accuracy of posting. If an error occurs, the issue is tracked through resolution. Batch jobs are run on a schedule (daily/weekly/monthly). Job completeness and accuracy are 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.

CASH AND SUSPENSE RECONCILIATION

CONTROL OBJECTIVE

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 RI's Webster Bank account in a timely manner.

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. Payment can go into suspense due to several reasons. For example, suppose the account number on a check or money order is not readable or is incorrect. In that case, 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 a customer omits a payment coupon or lacks other identifying information with the payment or other situations where a single payment made may apply to multiple accounts (and 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 resulting from 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. That process clears those suspense entries automatically by applying for 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 files 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) searches CPBS for corresponding information from a client, and the payment is 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 cannot resolve. Monthly, the suspense accounts are reviewed again by the VP of Operations (or designee) to help ensure discrepancies are resolved completely and accurately. The VP of Operations (or designee) sends a list of the unresolved accounts to the State of RI and their authorized representatives for further research to help ensure that suspense accounts are resolved in a timely fashion.

In addition to monitoring the suspense account, NFP Health also helps ensure that monies automatically applied to customer accounts are accounted for accurately and completely. Monthly, the COO (or designee) reconciles the daily deposits between CPBS and the State of RI'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 in an effort to help ensure it is resolved in a timely manner.

REFUND SETUP, AUTHORIZATION, AND PROCESSING

CONTROL OBJECTIVE

Control Objective 5: Controls provide reasonable assurance that insurance premium refunds are authorized and recorded accurately.

Refund Setup, Authorization, and Processing

Customers request refunds through the UHIP Call Center. There is an HSRI priority team that pre- qualifies refund eligibility. The escalation team includes representatives of the State of RI 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 RI. NFP Health's role in the refund process is 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 RI has finished their due diligence and approved or denied the refund request, on what date the decision was made, a check sent to the customer, and the amount of the check, to help ensure that CPBS always represents the current and valid status 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. 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 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 account's current status is known.

When a refund request is submitted, CPBS must be checked to confirm the details. If the check is successful, the Billing Support Manager sends a spreadsheet that batches the week's refund requests 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 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 RI and their support staff to help ensure that the refund requests were entered completely and accurately. The State of RI 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 login 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 site. 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 customer's refund.

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

REPORTING

CONTROL OBJECTIVE

Control Objective 6: Controls provide reasonable assurance that reporting to carriers and the HSRI is performed completely, accurately, and on a timely basis.

Reporting to Carrier

The Operations Team runs a monthly process 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 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). The carrier payment process summarizes payments and payment reversals (rejected payments) that have occurred before the run date of the process and determines the 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 before 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 file total to the carrier's expected sum.

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

The read-mode 820 files are shared with the State of RI by the VP of Operations (or designee) using an SFTP site provided for these purposes. The State of RI representatives are notified of the file being posted via email.

Authorization to send the machine-readable 820 files to carriers comes from the CFO for the Exchange via email prior to releasing the funds. Once approved, the 820 files are uploaded to the carriers' file transfer protocol (FTP) servers.

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

Reporting to the State of RI

Monthly, 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 detailed 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.

NFP Health prepares the report that reconciles the daily deposits between CPBS and the State of RI's Webster Bank account to customer payments every month. Any discrepancies are investigated and resolved.

BACKUPS

CONTROL OBJECTIVE

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.

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.
- **Secondary Data Center:** Asynchronous data volume replication to the Highlands Ranch, Denver, CO data center every 10 minutes.
- **Off-site:** Daily, NFP Health's production servers are backed up to a third-party service, Amazon Web Services (AWS), where two sets of backups are kept in encrypted S3 buckets. One for traditional backup with industry-standard retention and an immutable backup to address risk related to such events as ransomware attacks. HYCU is the software platform that manages and orchestrates backup activity to AWS.

Full backups are automatically scheduled daily and replicated off-site. 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.

A Restoration test is performed annually by restoring a production virtual machine (VM) snapshot (backup) to the Highlands Ranch, Denver, CO data center. Once restored, the VM is checked for file integrity and consistency.

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

INFORMATION SYSTEMS OVERVIEW

NFP Health's Technology Operations Team 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. Additionally, team members are responsible for granting and revoking access to CPBS system, securing client, and company data, and overseeing the change management and release management processes. Refer to the paragraphs below for additional information.

Application Overview

The CPBS system is an application consisting of a database and core software modules that allow loading of enrollment data, creating bills, and processing 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 co-location data center facilities and is managed and monitored by the Product Development and Technology Operations Teams.

Location

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

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
- HYCU Storage Area Networks (SAN) to provide network storage
- VMware is used to provide a virtual server environment

Operating Systems, Virtualization, and Network Domain

NFP Health uses VMware ESXi within the majority of its server infrastructure running Windows Server operating system (OS). Internet Information Services (IIS) and .NET framework are used to host its applications. The network is managed through Windows Active Directory (AD).

Databases

NFP Health's applications leverage Microsoft (MS) SQL Server 2016 Enterprise. To provide management and monitoring of its MS SQL instances, NFP Health leverages the services of Rackspace Technology Inc. (Norwell, MA). Rackspace Technology, Inc. provides 24/7/365 monitoring and management of NFP Health's databases.

LOGICAL SECURITY

CONTROL OBJECTIVE

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.

Logical Security

NFP Health addresses the security of its systems by a defense in depth approach, securing each layer of the system. NFP's approach is outlined below:

When a new employee is onboarded 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 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; access is updated based on the employee's business unit and function. When an employee transfers departments, the manager sends a notification form to IT and the employees' access is updated based on their job functions and responsibilities.

When an employee leaves or is terminated at NFP Health, access to CPBS, databases, and networks 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 timely.

Administrative access to AD, CPBS, and the CPBS database is restricted to appropriate personnel based upon role and responsibility. Password parameters for the network and CPBS are configured per 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. FS 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.

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

Operating System Security

OS security is managed through the 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. Domain administrative access to operating systems is restricted to authorized personnel.

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 administrators. Membership to security groups is determined by the user's job function and responsibilities. In addition, sensitive tables in the database, including those listing SSNs, are encrypted with a 1024-bit Rivest-Shamir-Adleman (RSA) key.

Application Security

CPBS is secured by application-based user management. User account information and sensitive data are 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 RI 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.

CHANGE MANAGEMENT

CONTROL OBJECTIVE

Control Objective 9: Controls provide reasonable assurance that changes or upgrades 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.

Change Management

Internal system and application changes are governed by a strict change management procedure, which prescribes infrastructure and application changes authorized by the senior manager overseeing infrastructure and application development. NFP maintains separate development, testing/quality assurance (QA), and production environments to help segregate different change management functions. Requested changes are documented and authorized before the commencement of development. For example, the Technology Operations Manager or Technical Program Director approves database and operating system changes; the Release Management Lead or CIO approves application changes.

Authorized changes are documented using NFP Health's 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 QA process. The form also documents formal approval of the change and acceptance of the change, confirming that it was implemented successfully.

For application development and infrastructure changes, changes are implemented, tested and reviewed in the following environments: development, QA, and production. Changes are tested at the Highlands Ranch (disaster recovery/secondary) data center for infrastructure changes 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' duties.

Once changes have been internally approved and documented in the NFP Health change management form, they are submitted via email. A Deloitte Intelligent Risk Assistant (IRA)/Azure DevOps ticket is initiated and submitted to be reviewed by Deloitte and the State of RI Change Control Board (CCB). Once Deloitte and CCB approve the change, 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 the production environment.

If 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 involve acceptance, testing, and approval from the Technology Operations Manager or CIO.

NFP Health disables all developer accounts and only enables them on an as-needed basis. If privileged access is needed, developers open an IT ticket stating what server access is required, justification, and

duration of access. Tickets have a subject line of "Access Required," which is automatically filtered and grouped for ease of management. Once the time has elapsed the requested duration, the Technology Operations Team disables the account and adds a resolution note to the ticket stating that temporary access has been disabled. The Technology Operations Team reviews the temporary access tickets daily (except for holidays and weekends) to help ensure that access was granted and disabled as requested and required.

USER CONTROL CONSIDERATIONS

NFP Health's processing of transactions and the controls over the processing were designed with the assumption that certain controls would be placed in operation by the user entities. This section describes some of the controls that should be in operation at the user entities to complete the controls at NFP Health. The user entity auditors should determine whether the user entities have established controls to provide reasonable assurance that:

1. HSRI is responsible for completing requested information at enrollment and for providing NFP Health with the correct information to complete their enrollment.
2. HSRI is responsible for ensuring the robustness of their own finances for completion of enrollment.
3. HSRI is responsible for providing notification to NFP Health in case of personal information changes.
4. HSRI is responsible for providing NFP Health with access to Webster Bank's portal to help ensure user access to the bank portal is restricted to appropriate personnel based on job responsibilities.
5. HSRI is responsible for regularly reviewing their bank accounts, including monthly bank statements.
6. HSRI is responsible for providing notification to NFP Health of approval and denial of refunds.
7. HSRI is responsible for their own third-party representatives to review payments and eligible customers prior to the release of the funds to carriers.

SUBSERVICE ORGANIZATION CONTROL CONSIDERATIONS

NFP Health's controls related to the CPBS cover only a portion of overall internal control for each user entity of NFP Health. It is not feasible for the control objectives related to the CPBS to be achieved solely by NFP Health. Therefore, 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 detailed in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Deloitte

1. Deloitte is 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.

Rackspace Technology, Inc.

2. Rackspace Technology, Inc. is responsible for providing 24/7/365 monitoring and management of NFP Health's databases.

AWS

3. AWS is responsible for providing encryption of off-site backup of NFP Health's VMware virtualization platform.

TierPoint, LLC

4. TierPoint, LLC is responsible for colocation data center services, specifically for the hosting of NFP Health's production IT infrastructure and CPBS system and data.

Cyxtera

5. Cyxtera is responsible for colocation data center services, specifically for the hosting of NFP Health's backup IT infrastructure and CPBS system and data.

SECTION 4

INFORMATION PROVIDED BY BERRYDUNN

PURPOSE AND SCOPE OF THE REPORT

This report is intended to provide interested parties with information about NFP Health's controls that may affect the processing of user entity transactions, and to provide information about the operating effectiveness of the controls that were tested. The information contained in this report, when combined with an understanding of the controls in place at the user entities, is intended to assist the user entities' financial statement auditors in planning the audit of the user entities, and in assessing control risk for assertions in the user entities' financial statements that may be affected by controls at NFP Health.

The examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). It is the responsibility of each user of this report to evaluate the information contained in this report in relation to the controls in place at the user entities. If certain complementary controls are not in place at the user entities, NFP Health's controls may not compensate for such weaknesses.

UNDERSTANDING THE CONTROL ENVIRONMENT

The control environment represents the collective effect of various elements in establishing or enhancing the effectiveness of specific controls. In addition to tests of specific controls described below, our procedures included tests of, or consideration of, the relevant elements of NFP Health's control environment, including:

- NFP Health's organizational structure and its approach to segregation of duties;
- The control methods of management;
- HR policies and practices of NFP Health.

In order to obtain an understanding of the control environment, we included the following procedures, to the extent we considered necessary: (1) a review of organizational structure, including management controls, the segregation of functional responsibilities, policy statements, accounting and processing manuals, and HR policies; (2) discussions with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to, and applying controls; and (3) observations of personnel in the performance of their assigned duties.

Our assessment of the control environment was considered in determining the nature, timing, and extent of tests of operating effectiveness of certain controls relevant to achievement of the control objectives specified in this Section.

TESTS OF OPERATING EFFECTIVENESS OF SPECIFIED CONTROLS

Our examination of the operating effectiveness of certain controls of NFP Health was restricted to the control objectives and related control activities specified by NFP Health in this Section, and was not extended to controls in effect at the user entities. Our tests of the operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period July 1, 2023 to June 30, 2024.

Our tests of the operating effectiveness of controls were designed to cover a representative number of transactions throughout the period July 1, 2023 to June 30, 2024, for each of the controls listed in this Section, which are designed to achieve the specified control objectives. In selecting particular tests of the operating effectiveness of controls, we considered: (1) the nature of the controls being tested; (2) the types and competence of available evidential matter; (3) the nature of the control objectives to be achieved; and (4) the expected efficiency and effectiveness of the test.

Test procedures performed in connection with determining the operating effectiveness of internal controls detailed in this Section are described below. In addition, we evaluated whether the information provided by the service organization was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of the information, as required by AICPA, Professional Standards, paragraph .36 of AT-C section 205, Assertion-Based Examination Engagements (AICPA, Professional Standards), and paragraph .30 of AT-C section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

Test Procedure	Description
Observation	Observed the application or existence of controls within the service organization.
Inspection	Inspected documents and reports that contain an indication of performance of the internal control policy or procedure. This includes, among other things, review of statistical and accounting reports, review of policies and procedures, and review of other control documents.

New Customer Setup and Modification

Control Objective 1: Controls provide reasonable assurance that new customers are set up completely and accurately on the CPBS system.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
1.1a	Each business day, NFP Health receives batches of new and existing customer activity from the RI UHIP. Any identified issues are researched and resolved.	Inspected the daily exchange log for a selection of days to determine that NFP Health received new and existing customer activity from the RI UHIP.	No deviations noted.
1.1b		*There were no issues identified; therefore, this test was not performed.* Inspect email communications for a selection of days to determine that any identified issues identified in the daily exchange log are researched and resolved.	*There were no issues identified.*
1.2	Each business day, carriers are notified via an 834 file of SHOP enrollments/changes to activate or amend a policy.	Inspected confirmation emails for a selection of days to determine that carriers were notified via the 834 file of enrollments and changes to activate or amend a policy.	No deviations noted.

Billings

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.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
2.1	Each business day, new customers' initial billing statements are generated by the Financial Operations Team and are made accessible to clients via CPBS.	Inspected initial billing statements for a selection of new customers to determine that new customers' billing statements were generated and uploaded to CPBS each business day.	No deviations noted.
2.2a	Monthly, customer statements are posted to CPBS by the Financial Operations Team where they are accessible to clients and subsequently reconciled by the Financial Operations Team. Failures are tracked to resolution.	Inspected the customer statements on the CPBS and reconciliations performed for a selection of months to determine that customer statements were posted to CPBS by the Financial Operations Team.	No deviations noted.
2.2b		*There were no identified failures; therefore, this test was not performed.* Inspect the customer statements on the CPBS and reconciliations performed for a selection of months to determine that any identified failures are tracked to resolution.	*There were no identified failures.*

Transaction Processing

Control Objective 3: Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
3.1	Batch payments are processed and uploaded to CPBS each business day.	Inspected Daily Deposit reports for a selection of days to determine that batch payments were processed and uploaded to CPBS each business day.	No deviations noted.
3.2a	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.	Observed a payment being posted to determine that the payment on account was automatically applied based upon unique client identifiers.	No deviations noted.
3.2b		Observed a payment being made which was not automatically posted to determine that the activity was posted to the suspense account.	No deviations noted.
3.2c		Inspected payment configurations to determine that payments were automatically applied based upon unique client identifiers.	No deviations noted.
3.2d		Inspected suspense account configurations to determine that in the event automated postings did not occur, the activity was posted to a suspense account.	No deviations noted.
3.3a	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.	Observed an overpayment to determine that the excess amount was automatically applied as a credit balance towards the next month's billing.	No deviations noted.
3.3b		Inspected payment configurations 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.	No deviations noted.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
3.4a	If a received payment is short more than $10 (for ongoing customers) and more than $5 (for initial customers) of the balance due, the funds are not transmitted to the carrier for insurance renewal.	Observed a payment that was short more than $10 of the balance due for an ongoing customer to determine that the funds were not transmitted to the carrier for insurance renewal.	No deviations noted.
3.4b		Observed a payment that was short more than $5 of the balance due for an initial customer to determine that the funds were not transmitted to the carrier for insurance renewal.	No deviations noted.
3.4c		Inspected payment configurations to determine that if the received payment was short more than $10 of the balance due for ongoing customers, or short more than $5 of the balance due for initial customers, the funds were not transmitted to the carrier for insurance renewal.	No deviations noted.
3.5a	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.	Inspected the Paid Through configurations to determine that the system automatically updated and calculated the Paid Through field each business day.	No deviations noted.
3.5b		Inspected the daily batch process logs for a selection of days to determine that the Paid Through batch process was executed daily after payments were uploaded.	No deviations noted.
3.6a	A QC script is run to uncover potential data errors each business day. Identified errors are resolved.	Inspected the QC script and associated configuration settings to determine that the script was scheduled to run and uncover potential data errors each business day.	No deviations noted.
3.6b		Inspected QC script reports for a selection of days to determine that any identified errors were resolved.	No deviations noted.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
3.7a	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 help ensure data is entered completely and accurately.	Inspected ACH return upload configurations to determine that batch ACH returns were configured to be processed and uploaded to CPBS each business day.	No deviations noted.
3.7b		Inspected Daily ACH NSF emails for a selection of days 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 Operations Team.	No deviations noted.
3.8a	Lockbox returns are processed and uploaded to CPBS on an ad hoc basis. Any issues are tracked and resolved by the Financial Operations Team to help ensure data is entered completely and accurately.	Inspected the reconciliation of lockbox returns to determine that NFP processed and uploaded lockbox returns to CPBS on an ad hoc basis.	No deviations noted.
3.8b		*There were no identified issues regarding lockbox returns; therefore, this test was not performed.* Inspect evidence of communication to determine that issues with lockbox returns are resolved by the Financial Operations Team.	*There were no identified issues regarding lockbox returns.*

Cash and Suspense Reconciliations

Control Objective 4: Controls provide reasonable assurance that cash is completely and accurately reconciled between the CPBS system and the State of Rhode Island's Webster Bank account in a timely manner.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
4.1	Monthly, the VP of Operations (or designee) sends a list of unresolved accounts to the State of RI for further review.	Inspected the end of month suspense account report and corresponding emails for a selection of months to determine that unresolved suspense accounts were sent to the State of RI for further investigation on a monthly basis.	No deviations noted.
4.2a	Monthly, the COO and/or designee reconciles the daily deposits between CPBS and the State of RI's Webster Bank account to customer payments. Any discrepancies are investigated and resolved.	Inspected reconciliations for a selection of months to determine that on a monthly basis, the COO, and/or designee, reconciled the daily deposits between CPBS and the State of RI's Webster Bank account to the customer payments.	No deviations noted.
4.2b		Inspected emails for a selection of months to determine that any identified discrepancies in the corresponding monthly reconciliations were investigated and resolved.	No deviations noted.
4.3a	Suspense accounts are searched for matches to an account by ACH or check. When a match occurs, the amount is automatically applied to the matched account.	Observed a payment being posted to determine that the payment on account was automatically applied based upon unique client identifiers.	No deviations noted.
4.3b		Inspected 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.	No deviations noted.

Refund Setup, Authorization, and Processing

Control Objective 5: Controls provide reasonable assurance that insurance premium refunds are authorized and recorded accurately.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
5.1a	The Financial Operations Team sets up a refund request in CPBS only upon authorized request from the Exchange.	Observed a refunded payment to determine that corresponding authorization from the Exchange was obtained prior to processing the refund.	No deviations noted.
5.1b		Inspected the log of all refund requests from the RI ShareFile to determine that the Financial Operations Team only set up refund requests in CPBS after receiving the authorization from the Exchange.	No deviations noted.
5.2	The Financial Operations Team reviews refunds to help ensure that they were authorized and recorded properly.	Inspected the combined refunds report to determine that the Financial Operations Team reviewed all refunds to help ensure that they were authorized and recorded properly.	No deviations noted.

Reporting

Control Objective 6: Controls provide reasonable assurance that reporting to carriers and the HSRI is performed completely, accurately, and on a timely basis.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
6.1	On a monthly basis, QC scripts are run for each carrier to confirm transactions have been imported completely and accurately.	Inspected the QC script to determine that the script ran monthly for each carrier to confirm transactions were imported.	No deviations noted.
6.2	On a monthly basis, the Operations Team sends the 820 report to RI for approval by the Office of the CFO.	Inspected email communications for a selection of months to determine that the Operations Team sent the 820 report to the RI Office of the CFO for approval.	No deviations 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, in a timely manner.	Inspected the email communications to the carriers' FTP servers for a selection of months to determine that the Operations Team issued and uploaded the 820 reports to the carriers' FTP servers once it was approved, in a timely manner.	No deviations 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.	Inspected the QuickBooks journal entries for a selection 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 deviations noted.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
6.5a	Monthly, the COO and/or designee reconciles the daily deposits between CPBS and the State of RI's Webster Bank account to customer payments. Any discrepancies are investigated and resolved.	Inspected reconciliations for a selection of months to determine that on a monthly basis, the COO, and/or designee, reconciled the daily deposits between CPBS and the State of RI's Webster Bank account to the customer payments.	No deviations noted.
6.5b		Inspected emails for a selection of months to determine that any identified discrepancies in the corresponding monthly reconciliations were investigated and resolved.	No deviations noted.

Backups

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.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
7.1	Full backups are automatically scheduled on a daily basis and replicated off-site.	Inspected backup configurations to determine that full backups were configured to run on a daily basis and replicate off-site.	No deviations noted.
7.2a	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 reviewed and remediated.	Inspected the backup alerts for a selection of days to determine that automated backup alerts were sent for successes and failures to Technology Operations System Engineer.	No deviations noted.
7.2b		Inspected the Technology Operations Checklist for a selection of months to determine that backups were monitored by the Technology Operations System Engineer daily for the selected months, and that any identified issues were reviewed and remediated.	No deviations noted.
7.3	Backup restores are tested annually to verify media reliability and data integrity.	Inspected the backup restoration results to determine that backups were tested to verify media reliability and data integrity.	No deviations noted.
7.4	Changes to backup job schedules are documented and approved prior to implementation.	*There were no changes made to the backup job schedule; therefore, this test was not performed.* Inspect tickets for a selection of backup job schedule changes to determine that changes are documented and approved prior to implementation for each selected change.	*There were no changes made to the backup job schedule.*

Security

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.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
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.	Inspected system access requests for a selection 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 deviations noted.
8.2	For terminated employees, the manager sends a system access termination form to IT with the employee's termination date. IT timely removes access.	Inspected the employee termination forms and user access listings for a selection of terminated employees to determine that the manager notified IT of the employee's termination, and that IT timely removed access.	No deviations 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.	*There were no transferred employees; therefore, this test was not performed.* Inspect a notification form to IT for a selection of transferred employees to determine that transferred employees' access is updated based on their functions and responsibilities.	*There were no transferred employees.*
8.4	Administrative access to AD, CPBS and the CPBS database is restricted to appropriate personnel based upon role and responsibility.	Inspected the administrative user list to determine that administrative access to the network, application, and database was restricted to appropriate personnel based upon role and responsibility.	No deviations noted.
8.5	Access to backups is limited to appropriate individuals based upon their role and responsibility.	Inspected the HYCU backup user list and organization chart to determine that access was limited to appropriate individuals based upon their roles and responsibilities.	No deviations noted.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
8.6	Password parameters for AD and CPBS are configured in accordance with the Information Technology Policy.	Inspected the network and CPBS password parameters to determine that password parameters were configured to meet or exceed requirements of the Information Technology Policy.	No deviations noted.
8.7	Annually, the IT department conducts a user access review for AD and CPBS 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.	Inspected the annual user access review for AD and CPBS 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.	No deviations noted.

Change Management

Control Objective 9: Controls provide reasonable assurance that changes or upgrades 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.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
9.1	Change requests are documented and authorized prior to prior to implementation to production.	Inspected evidence for a selection of changes to determine that application and infrastructure change requests were documented and authorized prior to implementation to production.	No deviations noted.
9.2	Change requests are tested prior to implementation to production.	Inspected the change tickets and release schedule for a selection of changes to determine that application change requests were tested prior to implementation to production.	No deviations noted.
9.3	Separate development, QA, and production environments are in place.	Inspected the communication connection attempts to determine that development, QA, and production environments were in place and logically separated.	No deviations noted.
9.4	Change requests are approved prior to implementation to production.	Inspected the change release log for a selection of changes to determine that changes were approved prior to implementation to production.	No deviations noted.

No.	NFP Health Control Activities	Tests Performed by BerryDunn	Results of Tests
9.5a	Users with ability to update changes to CPBS are based on users' roles and properly authorized and monitored.	Inspected the CPBS user list and organization chart to determine that users with ability to update changes to CPBS were role based and authorized.	No deviations noted.
9.5b		Inspected the Netwrix Auditor configuration settings to determine that the tool was configured to record and monitor activity of users in the production environment.	No deviations noted.
9.5c		Inspected the ticket for a selection of developers requesting production access to determine that when developers required administrator access, an IT ticket was created stating the justification for access, the duration that administrator access was needed for, and what server they were requesting production access to.	No deviations 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.	Inspected the development meeting minutes for a selection of months to determine that on a bi-weekly basis, the Release Management Team met to discuss change requests and report progress, and that all members of the team, including developers, testers, business specialists, infrastructure, and operations, attended these mandatory meetings.	No deviations noted.