



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

**NFP Health Services Administrators  
Rhode Island**

For the Period July 1, 2025 – June 30, 2026



*Proprietary and Confidential; Distribution without permission is prohibited.*



## CONTENTS

|           |                                                                              |      |
|-----------|------------------------------------------------------------------------------|------|
| Section 1 | Independent Service Auditor's Report                                         | 1-1  |
| Section 2 | Management of NFP Health's Assertion                                         | 2-1  |
| Section 3 | NFP Health's Description of Its System                                       |      |
|           | Overview of Services Provided                                                | 3-1  |
|           | Relevant Aspects of the Control Environment, Risk Assessment, and Monitoring | 3-2  |
|           | Control Objectives and Related Control Activities                            | 3-6  |
|           | New Customer Setup and Modifications                                         | 3-7  |
|           | Billings                                                                     | 3-8  |
|           | Transaction Processing                                                       | 3-9  |
|           | Cash and Suspense Reconciliation                                             | 3-11 |
|           | Refund Setup, Authorization, and Processing                                  | 3-12 |
|           | Reporting                                                                    | 3-13 |
|           | Backups                                                                      | 3-15 |
|           | Information Systems Overview                                                 | 3-16 |
|           | Logical Security                                                             | 3-18 |
|           | Change Management                                                            | 3-20 |
|           | Significant Changes During the Examination Period                            | 3-21 |
|           | User Control Considerations                                                  | 3-22 |
|           | Subservice Organization Control Considerations                               | 3-23 |
| Section 4 | Information Provided by BDMP Assurance, LLP                                  |      |
|           | Purpose and Scope of the Report                                              | 4-1  |
|           | Understanding the Control Environment                                        | 4-1  |
|           | Description of Tests of Controls and Results Thereof                         | 4-2  |
|           | Tests Performed and Results of Tests                                         | 4-3  |

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 NFP Health Services Administrators' (NFP Health) description of its Core Premium Billing Services (CPBS) system entitled "NFP Health's Description of Its System" for processing HealthSource Rhode Island (HSRI) transactions throughout the period July 1, 2025 to June 30, 2026 (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 Nutanix infrastructure, 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 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 organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

### SERVICE ORGANIZATION'S RESPONSIBILITIES

In Section 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. 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 AICPA. 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, 2025 to June 30, 2026. 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 objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, 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 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 user entities' 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 presented in the section of our report titled "Description of Tests of Controls and Results Thereof."

## OPINION

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

1. The description fairly presents the system that was designed and implemented throughout the period July 1, 2025 to June 30, 2026.
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, 2025 to June 30, 2026, 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, 2025 to June 30, 2026.
3. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2025 to June 30, 2026 if complementary subservice organization and user entity controls assumed in the design of NFP Health's controls operated effectively throughout the period July 1, 2025 to June 30, 2026.

## 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 management of NFP Health, user entities of NFP Health's system during some or all of the period July 1, 2025 to June 30, 2026, and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have 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.

*BDMP Assurance, LLP*

Portland, Maine  
August 13, 2026

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 "NFP Health's Description of Its System" for processing user entities' transactions throughout the period July 1, 2025 to June 30, 2026 (description) for user entities of the system during some or all of the period July 1, 2025 to June 30, 2026, 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 subservice organizations and user entities themselves, when assessing the risks of material misstatements 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 Nutanix infrastructure, host production 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 in the description can be achieved only if complementary subservice organization controls assumed in the design of our 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 organization. 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, 2025 to June 30, 2026 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, when 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 carve-out method or the inclusive 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 and complementary subservice organization controls assumed in the design of the service organization's controls.
  - viii. Other aspects of our control environment, risk assessment process, information and communication systems (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 service organization's system during the period covered by the description.
  - c. Does not omit or distort information relevant to the service organization's system, while 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 operated effectively throughout the period July 1, 2025 to June 30, 2026 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of NFP Health's controls throughout the period July 1, 2025 to June 30, 2026. 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, as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
  - c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Signed by:

*Laura Wood*

6B536EC2F0814D5...

Laura Wood, Chief Operating Officer  
NFP Health Services Administrators  
August 13, 2026

SECTION 3

# 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 (HIX) 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.

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 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
- 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. Emphasis 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:

- Helping ensure 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 helping ensure maximum client satisfaction
- Securing and protecting the organization's assets

Additionally, the Executive Management Team is responsible for determining the competency levels required for each position 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 to help ensure that current and new employees are qualified for their position.

Several Teams help to support the solution, including:

- **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 development meetings, and tracking the status using a Microsoft Project Plan. Risks and issues are immediately identified and addressed. Additionally, best-practice and industry-standard ticketing and project management applications are 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 that 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 development meetings at least monthly led by the Release Management Lead. These meetings are held for the purpose of communicating requirements, discussing change requests and reporting progress. Developers, testers, business specialists, infrastructure and operations attend these mandatory meetings. Members in attendance communicate project statuses 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 IT 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 annually. 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

employees, and the procedures to be followed are also clearly defined and available to 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, references are required. An Executive Management Team member authorizes new hires and internal promotions. Staff are professionally qualified and engage in training to receive and maintain relevant knowledge and skills needed for the job.

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 and/or Managers are required to evaluate and document the performance of employees. The annual performance review meeting provides an opportunity for the Supervisor and/or 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 to prevent changes such as 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 there are no performance and response issues, 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. Technology monitoring 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:

- **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
- **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 HIX 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 strives 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 in the 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 the CPBS system 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 the CPBS system. The unique customer ID is transferred to the CPBS system using the above-mentioned EDI files.

Individual enrollments are added to the UHIP application via creation of a unique customer and member IDs in the portal and used as the common reference between the portal and CPBS.

## BILLINGS

### CONTROL OBJECTIVE

**Control Objective 2:** Controls provide reasonable assurance that customer billing statements are generated for customers by the Financial Operations Team and are made accessible to clients daily and monthly.

### 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 Automated Clearing House (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 ACH payments and any previous day 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 payment received, payment rejected, plan changes, addition or termination of individuals 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. NFP Health performs a quality check on the XML to help ensure that dollar amounts generated on the XML match amounts in the CPBS system and resolves any discrepancies prior to transmitting the XML file to the mail house vendor used by NFP Health to print and mail the statements via a shared Secure File Transfer Protocol (SFTP) site. The mail house is notified of the transmission of the XML file. A request is generated to transform the statements into an electronic portable document format (PDF) file and then create hard copies. 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 the CPBS system to the mail house and back from the mail house to the CPBS system. A quality check is performed by NFP Health Operations personnel prior to authorizing the mail house to mail the statements to customers. The PDF statements are uploaded into the CPBS system 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 the CPBS system 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 HIX bank account. The second step is the application of 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 p.m. ACH process is 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 the CPBS system 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 the CPBS system (typically the next business day in the case of initial enrollment), an automated process either applies the payment out of the suspense account to the identified customer account or applies it directly to the account if enrollment data exists within the CPBS system 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 the CPBS system are monitored and compared to 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 toward 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 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, funds are not transmitted to the carrier to trigger ongoing insurance coverage.

The paid through field is automatically updated and calculated in the CPBS system based upon execution of the daily Paid Through Date (PTD) 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 PTD) and internally, that the CPBS system 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 Financial and Technical Operations staff. Correcting entries are either made through the coordination of changes with UHIP or via manual changes made directly by the CPBS system (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 designated schedule (daily/weekly/monthly). Job completeness and accuracy are tracked using the daily Operations Daily Batch Process Log. In the event of a failure, the issue is documented for subsequent review and resolution by a member of the Financial Operations Team using the Operations Daily Batch Process Log.

## CASH AND SUSPENSE RECONCILIATION

### CONTROL OBJECTIVE

**Control Objective 4:** Controls provide reasonable assurance that cash is completely and accurately reconciled between the CPBS system and the State's 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. Payments can go into suspense for several reasons (including, but not limited to):

- 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 the CPBS system (disallowing the ability to automatically link payments with enrollment records).
- 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. The process clears 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 daily 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 the CPBS system 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 unresolvable accounts. 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 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 the CPBS system 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) research further in an effort to help ensure it is resolved.

## 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 prequalifies 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.

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 the CPBS system 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 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 status is known.

When a refund request is submitted, the CPBS system must be checked to confirm the details. If the check is successful, the Billing Support Manager sends a spreadsheet that batches the weekly 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 does not exceed the credit balance available.

The Financial Operations Team sets up a refund request in the CPBS system 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 the CPBS system 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. The Financial Operations Team reviews the refunds monthly 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 timely.

### REPORTING TO CARRIER

The Financial Operations Team runs a monthly process to determine what payments received by UHIP should be submitted to the carrier, using the 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 EDI 820 files to the Office of the CFO of HSRI for review before sending them to carriers. The Financial Operations Team holds the EDI 820 files 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 EDI 820 file includes customer code, subscriber code, plan code, customer name, PTD, 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 EDI 820 file total to the carrier's expected sum.

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

The read-mode EDI 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 EDI 820 files to carriers comes from the CFO for the HIX via email prior to releasing the funds. Once approved, the EDI 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 EDI 820 files relevant to their business, are fielded via email by the Financial 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 HIX 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 the CPBS system 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 are available for restoration in the event of processing errors or unexpected processing interruptions.

### 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 (Disaster Recovery Site):** Asynchronous data volume replication to the Highlands Ranch, Denver, Colorado (CO) data center every 10 minutes.
- **Off-site:** Daily, NFP Health's Nutanix volumes are backed up (snap-vaulted) to a third-party service, HYCU, where backups are kept indefinitely or until the number of maximum snap-vaults is reached (256).

Full backups are scheduled to run automatically daily and are replicated off-site for added security. The Technology Operations Team monitors backups through email alerts and by reviewing backup logs. The status of backups (success or failure) is documented daily using a checklist maintained by the Technology Operations Team. If a failure occurs, the issue is documented on the checklist. Where applicable, the issue is also documented and tracked in the ticketing system and is expected to be resolved within 24 hours. Additionally, the Technology Operations Team uses a daily checklist to document their monitoring of systems hosted in the third-party data center for any system-triggered alarms, uptime status, and data center connectivity issues.

Backup restoration procedures are in place to help ensure NFP Health's ability to restore data from backups. In addition, the Technology Operations Team performs backup restoration testing annually by restoring a production virtual machine snapshot. Once restored, The Technology Operations Team confirms the success of the restore by checking for file integrity and consistency to the production virtual machine.

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 the CPBS system. Additionally, team members are responsible for granting and revoking access to the CPBS system, securing client, and company data, and overseeing the change management and release management processes.

### 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 ACH and lockbox payments, and aggregating premium for payment to the appropriate carriers to which premium is due. It also includes a web-based user interface for use by Call Center and Financial Staff to research enrollment and billing transactions and process reversal of payments, reallocation of payments, and the setup of refunds.

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

### LOCATION

NFP Health's infrastructure is located in data centers managed by two subservice organizations, TierPoint, LLC and Centersquare. The primary data center is located in Marlborough, Massachusetts (MA), while the secondary data center is located in Highlands Ranch, Denver, 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
- Nutanix HCI for compute, storage and virtualization
- HYCU Storage Area Networks (SAN) to provide network storage

**Operating Systems, Virtualization, and Network Domain**

NFP Health uses Nutanix within the majority of its server infrastructure running Windows Server operating system. Internet Information Services 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. To provide management and monitoring of its MS SQL instances, NFP Health leverages the services of Rackspace Technology Inc. (San Antonio, TX). 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 access to applications, operating systems and databases 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.

When a new employee is onboarded at NFP Health or a change in access is required for an existing employee, access to the CPBS system, 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 the date the access change is needed to be made by must be defined along with the signature of the employee's direct report requesting access. The Technology Operations Department is responsible for granting permissions for the CPBS system, 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 employee's access is updated based on their job functions and responsibilities.

When an employee leaves or is terminated, access to the CPBS system, databases, and networks are revoked upon the employee's manager completing the end-user access form and submitting it to the Technology Operations Department. The Technology Operations Department is responsible for revoking permissions for the CPBS system, database, and network access timely.

Administrative access to AD, the CPBS system, and CPBS database is restricted to appropriate personnel based upon role and responsibility. Password parameters for the network and the CPBS system are configured per the IT 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 the CPBS system, databases, and the network.
- That active employee access is accurate and appropriate based on their role/responsibilities.
- That terminated employee access has been revoked and their accounts removed from the CPBS system, databases, and the network.

### NETWORK SECURITY

NFP Health leverages multiple layers of security to protect its infrastructure and applications at the network layer; Cisco ASA firewalls and Cisco Intrusion Detection System (IDS/IPS) maintain perimeter security. Firewall rule sets are configured to limit and control inbound and outbound Internet traffic. Triggers are configured to send alerts. F5 Big-IP Application Security Managers (ASM) 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 network is provided to the authorized personnel by secure Virtual Private Network (VPN) using Cisco's VPN Client.

## OPERATING SYSTEM SECURITY

Operating system 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. Administrative access to operating systems is restricted to authorized personnel. Authorized personnel belong to the domain administrators' security group.

## DATABASE SECURITY

Databases inherit the AD security settings for authorization and authentication, such that database users' privileges are defined by AD group membership. These AD security groups include read-only, read and write, and SQL 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

The CPBS system 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 system changes and upgrades are documented, tested, and approved prior to implementation.

### CHANGE MANAGEMENT

Internal system and application changes are governed by a change management procedure, which prescribes infrastructure and application changes authorized by the Senior Manager overseeing infrastructure and application development. NFP maintains separate development, testing (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 Azure DevOps (DevOps) tickets. DevOps tickets track 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. Tickets also document formal approval of the change and acceptance of the change, confirming that it was implemented successfully.

For application development and infrastructure changes, changes are first implemented and tested in the following environments: development, quality assurance, and staging. 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 employee duties.

Once changes have been internally approved, 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 workflow in DevOps, 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 as needed. 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.

## **SIGNIFICANT CHANGES DURING THE EXAMINATION PERIOD**

There were no significant changes to NFP Health's CPBS system provided to HSRI during the examination period.

## USER CONTROL CONSIDERATIONS

In all processing environments, there are certain procedures and controls that users should be responsible for performing to help ensure the quality of service and integrity of the processing. The controls in place at NFP Health represent only a portion of the overall internal controls of the user entities, and NFP Health has designed its controls under the assumption that certain controls are implemented by the user entities. The implementation of certain controls at the user entities is necessary to enhance the efficacy of the controls and to achieve certain control objectives.

This Section describes certain internal controls that the user entities should consider to achieve the controls identified in Section 4. The user control considerations presented below should not be regarded as a comprehensive list of all the controls that should be employed by the user entities.

| NFP Health's Control Objectives                                                                                                                                                               | Complementary User Controls                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Control Objective 1:</b> Controls provide reasonable assurance that new customers are set up completely and accurately in the CPBS system.                                                 | HSRI is responsible for completing requested information at enrollment and for providing NFP Health with the correct information to complete their enrollment.                                        |
| <b>Control Objective 3:</b> Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.                                                     | HSRI is responsible for providing notification to NFP Health in case of personal information changes.                                                                                                 |
|                                                                                                                                                                                               | HSRI is responsible for their own third-party representatives to review payments and eligible customers prior to the release of the funds to carriers.                                                |
| <b>Control Objective 4:</b> Controls provide reasonable assurance that cash is completely and accurately reconciled between the CPBS system and the State's bank account in a timely manner.  | HSRI is responsible for regularly reviewing their bank accounts, including monthly bank statements.                                                                                                   |
| <b>Control Objective 5:</b> Controls provide reasonable assurance that insurance premium refunds are authorized and recorded accurately.                                                      | HSRI is responsible for providing notification to NFP Health of approval and denial of refunds.                                                                                                       |
| <b>Control Objective 8:</b> Controls provide reasonable assurance that logical access to applications, operating systems and databases is restricted to authorized and appropriate personnel. | 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. |

## SUBSERVICE ORGANIZATION CONTROL CONSIDERATIONS

NFP Health's services were designed with the assumption that certain procedures and controls are implemented by applicable subservice organizations to help ensure the quality of service and integrity of the processing. The controls in place at NFP Health represent only a portion of the overall internal controls relied upon by the user entities, and NFP Health has designed its controls under the assumption that certain controls are implemented by the subservice organization. The implementation of certain controls at the subservice organization is necessary to enhance the efficacy of the controls and to achieve certain control objectives.

This Section describes certain controls that should be in place to achieve the control objectives identified in Section 4. The Complementary Subservice Organization Controls presented below should not be regarded as a comprehensive list of all controls that the subservice organization should employ.

| NFP Health's Control Objectives                                                                                                                                                                                                                                                                                          | Complementary Subservice Organization Controls                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Control Objective 3:</b> Controls provide reasonable assurance that transactions are processed and recorded completely and accurately.</p> <p><b>Control Objective 9:</b> Controls provide reasonable assurance that system changes and upgrades are documented, tested, and approved prior to implementation.</p> | <p>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.</p> |
| <p><b>Control Objective 8:</b> Controls provide reasonable assurance that logical access to applications, operating systems and databases is restricted to authorized and appropriate personnel.</p>                                                                                                                     | <p>Rackspace Technology, Inc. is responsible for providing 24/7/365 monitoring and management of NFP Health's databases.</p>                                                                                                             |
|                                                                                                                                                                                                                                                                                                                          | <p>AWS is responsible for providing server-side encryption for the off-site backups of NFP Health's Nutanix virtualization platform.</p>                                                                                                 |
|                                                                                                                                                                                                                                                                                                                          | <p>HYCU is responsible for managing network storage and orchestrating backup activities to AWS.</p>                                                                                                                                      |
| <p><i>Data center hosting services at NFP Health are not in scope as there are no on-prem systems. There is therefore no corresponding control objective for these CSOCs.</i></p>                                                                                                                                        | <p>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.</p>                                                            |
|                                                                                                                                                                                                                                                                                                                          | <p>Centersquare is responsible for colocation data center services, specifically for the hosting of NFP Health's backup IT infrastructure and CPBS system and data.</p>                                                                  |

SECTION 4

# INFORMATION PROVIDED BY BDMP ASSURANCE, LLP

## 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 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.

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.

## DESCRIPTION OF TESTS OF CONTROLS AND RESULTS THEREOF

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, 2025 to June 30, 2026.

Our tests of the operating effectiveness of controls were designed to cover a representative number of transactions throughout the period July 1, 2025 to June 30, 2026, 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                                                                                                                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inquiry        | Inquired with management and/or process owners to develop an understanding of the processes in place and to confirm the existence of procedures or matters discussed.                                                                                                             |
| 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 in the CPBS system.

| No.  | NFP Health Control Activities                                                                                  | Tests Performed by BDMP Assurance, LLP                                                                                                                                       | Results of Tests                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.1  | NFP Health processes batches of new and existing customer activity upon receiving information from RI UHIP.    | Inspected the daily exchange log for a selection of dates to determine that NFP Health processed new and existing customer activity upon receiving it from RI UHIP.          | No deviations noted.                                                                                                                                            |
| 1.2  | Each business day, carriers are notified via an 834 file of enrollments/changes to activate or amend a policy. | Inspected confirmation emails for a selection of dates to determine that carriers were notified via the "834" file of enrollments and changes to activate or amend a policy. | No deviations noted.                                                                                                                                            |
| 1.3a | A QC script is run daily to identify failures in the enrollment process. Identified errors are resolved.       | Observed QC script success and failure notifications to determine that the script was run to report on enrollment results and errors were resolved, if identified.           | No deviations noted.                                                                                                                                            |
| 1.3b |                                                                                                                | Inspected QC script reports for a selection of dates to determine that the script was run daily to identify enrollment process failures.                                     | No deviations noted.                                                                                                                                            |
| 1.3c |                                                                                                                | Inquired and confirmed with management to determine that there were no errors identified in the daily QC script run during the examination period.                           | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |

| No. | NFP Health Control Activities                                                                                                                       | Tests Performed by BDMP Assurance, LLP                                                                                                                                            | Results of Tests     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 1.4 | EDI batch job failures are reported to the Financial Operations Team via notifications. Errors are researched and resolved by the Development Team. | Inspected an EDI batch job failure notification and evidence of resolution for a selection of EDI failures to determine that EDI batch job failures were identified and resolved. | No deviations noted. |

## Billings

**Control Objective 2:** Controls provide reasonable assurance that customer billing statements are generated for customers by the Financial Operations Team and are made accessible to clients daily and monthly.

| No.  | NFP Health Control Activities                                                                                                                                       | Tests Performed by BDMP Assurance, LLP                                                                                                                                                      | 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 the CPBS system. | Inspected initial billing statements for a selection of new customers to determine that new customers' billing statements were generated and uploaded to the CPBS system each business day. | No deviations noted.                                                                                                                                            |
| 2.2a | Invoices are generated monthly and any discrepancies are researched and resolved prior to billing activities for statement generation.                              | Inspected internal communications for a selection of months to determine that invoices were generated monthly and subscriber plan and previous balance (PB) transaction amounts reconciled. | No deviations noted.                                                                                                                                            |
| 2.2b |                                                                                                                                                                     | Inquired and confirmed with management to determine that there were no monthly invoicing discrepancies identified during the examination period.                                            | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 2.3  | Billing activities to generate monthly statements for customers are run according to the schedule agreed upon by RI.                                                | Inspected internal communications for a selection of months to determine that billing activities were run on the date agreed upon with RI.                                                  | No deviations noted.                                                                                                                                            |

| No.  | NFP Health Control Activities                                                                                                                                                                                                                              | Tests Performed by BDMP Assurance, LLP                                                                                                                                                          | Results of Tests                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4a | A Statement QC script is run both daily and monthly to help ensure that dollar amounts generated on the XML match amounts in the CPBS system. Anomalies are researched and resolved prior to sending the XML to the print vendor for statement generation. | Observed the Statement QC process to determine that a script was run to help ensure dollar amounts on the statement XML file matched amounts in the CPBS system.                                | No deviations noted.                                                                                                                                            |
| 2.4b |                                                                                                                                                                                                                                                            | Inspected QC script reports for a selection of dates to determine that the script was run daily to compare dollar amounts in the XML to amounts in the CPBS system.                             | No deviations noted.                                                                                                                                            |
| 2.4c |                                                                                                                                                                                                                                                            | Inspected research and resolution for a selection of dates to determine that statement errors identified by the daily QC script were resolved.                                                  | No deviations noted.                                                                                                                                            |
| 2.4d |                                                                                                                                                                                                                                                            | Inspected confirmation messages in Microsoft Teams for a selection of months to determine that the script was run monthly to help ensure that dollar amounts generated matched the CPBS system. | No deviations noted.                                                                                                                                            |
| 2.4e |                                                                                                                                                                                                                                                            | Inquired and confirmed with management to determine that there were no anomalies with the daily and monthly statement QC process during the examination period.                                 | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |

| No.  | NFP Health Control Activities                                                                                                     | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                             | Results of Tests     |
|------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 2.5a | NFP Health reconciles the total amount of statements sent to the print vendor versus statements received from the print vendor.   | Observed the monthly customer statement reconciliation process to determine that NFP Health verified that the total amount of statements received back from the print vendor matched the amount sent.              | No deviations noted. |
| 2.5b |                                                                                                                                   | Inspected monthly statement reconciliation confirmations for a selection of months to determine that NFP Health verified that the total amount of statements sent to the print vendor matched the amount received. | No deviations noted. |
| 2.6  | A sample of statements are spot checked for accuracy prior to uploading the statements to the CPBS system.                        | Observed the monthly customer statement reconciliation process to determine that statements sent back from the print vendor were reconciled before being uploaded to the CPBS system.                              | No deviations noted. |
| 2.7  | Monthly, customer statements are posted to the CPBS system by the Financial Operations Team where they are accessible to clients. | Inspected the customer statements on the CPBS system for a selection of months to determine that customer statements were posted to the CPBS system by the Financial Operations Team.                              | No deviations noted. |

## 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 BDMP Assurance, LLP                                                                                                                                                                    | Results of Tests                                                                                                                                                |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1a | Batch payments are processed and uploaded to the CPBS system each business day. Issues are tracked and resolved by the Financial Operations Team.                                                                                                                                                                                                               | Inspected the daily batch process log for a selection of dates to determine that batch payments were processed and uploaded to the CPBS system daily.                                                     | No deviations noted.                                                                                                                                            |
| 3.1b |                                                                                                                                                                                                                                                                                                                                                                 | Inquired and confirmed with management to determine that there were no batch payment errors that required manual resolution during the examination period.                                                | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 3.2  | 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 automated batch ACH job is run, or the next business day otherwise. | Observed the process for initial payments received via ACH to determine that the payment was processed the same day if received prior to the automated batch ACH job, or the next business day otherwise. | No deviations noted.                                                                                                                                            |

| No.  | NFP Health Control Activities                                                                                                                                                         | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                       | Results of Tests     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 3.3a | 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. |
| 3.3b |                                                                                                                                                                                       | Observed a payment being made which was not automatically posted to determine that the activity was posted to the suspense account.                                                                          | No deviations noted. |
| 3.3c |                                                                                                                                                                                       | Inspected payment configurations to determine that payments were automatically applied based upon unique client identifiers.                                                                                 | No deviations noted. |
| 3.3d |                                                                                                                                                                                       | 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. |
| 3.4a | If a payment is received in excess of the amount due, the excess amount is automatically applied as a credit balance toward the next month's billing.                                 | Observed an overpayment to determine that the excess amount was automatically applied as a credit balance toward the next month's billing.                                                                   | No deviations noted. |
| 3.4b |                                                                                                                                                                                       | Inspected payment configurations to determine that if the payment received was in excess of the amount due, the excess amount was automatically applied as a credit balance toward the next month's billing. | No deviations noted. |

| No.  | NFP Health Control Activities                                                                                                                                                                              | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                                                                                 | Results of Tests     |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 3.5a | If a received payment is under by 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 under by 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. |
| 3.5b |                                                                                                                                                                                                            | Observed a payment that was under by 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. |
| 3.5c |                                                                                                                                                                                                            | Inspected payment configurations to determine that if the received payment was under by 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. |
| 3.6a | After payments are uploaded, the paid through field is automatically updated and calculated in the CPBS system based upon execution of the PTD batch process each business day.                            | Observed the daily PTD batch process to determine that the system automatically updated and calculated the paid through field each business day.                                                                                                                                       | No deviations noted. |
| 3.6b |                                                                                                                                                                                                            | Inspected the daily batch process logs for a selection of dates to determine that the paid through batch process was executed daily after payments were uploaded.                                                                                                                      | No deviations noted. |
| 3.7a | 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. |
| 3.7b |                                                                                                                                                                                                            | Inspected QC script reports for a selection of dates to determine that any identified errors were resolved.                                                                                                                                                                            | No deviations noted. |

| No.   | NFP Health Control Activities                                                                                                                                                                                          | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                              | Results of Tests                                                                                                                                                |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.8a  | 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 the CPBS system each business day.                                                                   | No deviations noted.                                                                                                                                            |
| 3.8b  |                                                                                                                                                                                                                        | Inspected Daily ACH NSF emails for a selection of dates to determine that batch ACH returns were processed and uploaded to the CPBS system each business day and issues were tracked and resolved by the Financial Operations Team. | No deviations noted.                                                                                                                                            |
| 3.9   | Returned payments are tracked through resolution via the monthly bank reconciliation performed by the Financial Operations Team to help ensure data is entered completely and accurately.                              | Inspected reconciliations for a selection of months to determine that the Financial Operations Team reconciled the daily returns between the CPBS system and State of RI's Webster Bank account and resolved any issues.            | No deviations noted.                                                                                                                                            |
| 3.10a | 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 the CPBS system on an ad hoc basis.                                                                                 | No deviations noted.                                                                                                                                            |
| 3.10b |                                                                                                                                                                                                                        | Inquired and confirmed with management to determine that there were no issues related to lockbox returns during the examination period.                                                                                             | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |

## 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's bank account in a timely manner.

| No.  | NFP Health Control Activities                                                                                                                                                                 | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                                       | 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 monthly.                         | 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 the COO, and/or designee, reconciled the daily deposits between the CPBS system and the State of RI's Webster Bank account to the customer payments monthly.           | No deviations noted. |
| 4.2b |                                                                                                                                                                                               | Inspected reconciliations and 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 to determine that suspense accounts were automatically searched for matches to an account by ACH or 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 BDMP Assurance, LLP                                                                                                                                                                               | Results of Tests     |
|------|-------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 5.1a | The Financial Operations Team sets up a refund request in the CPBS system only upon an authorized request from the HIX. | Observed a refunded payment to determine that corresponding authorization from the HIX 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 or PMO only set up refund requests in the CPBS system after receiving the authorization from the HIX. | No deviations noted. |
| 5.2  | The Financial Operations Team reviews refunds monthly to help ensure that they are authorized and recorded properly.    | Inspected the combined refunds report and emails for a selection of months 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 timely.

| No. | NFP Health Control Activities                                                                                                                                                                                                                                         | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                                                            | Results of Tests     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 6.1 | EDI 820 files are generated following the end of the monthly billing process, according to the schedule agreed upon by RI.                                                                                                                                            | Inspected EDI 820 files for a selection of months and all carriers to determine that EDI 820 files were generated at the end of the monthly billing process and on the date agreed upon with RI.                                                                  | No deviations noted. |
| 6.2 | QC scripts are run for each carrier monthly to confirm transactions have been imported completely and accurately.                                                                                                                                                     | Inspected the QC script configuration and output to determine that the script ran monthly for each carrier to confirm transactions were imported.                                                                                                                 | No deviations noted. |
| 6.3 | Monthly, the Operations Team sends the EDI 820 files 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 EDI 820 files to the RI Office of the CFO for approval.                                                                                                   | No deviations noted. |
| 6.4 | Monthly, the Financial Operations Team issues and uploads the EDI 820 files to the carriers FTP servers once approved.                                                                                                                                                | Inspected the email communications to the carriers' FTP servers for a selection of months to determine that the Financial Operations Team issued and uploaded the EDI 820 files to the carriers' FTP servers once approved.                                       | No deviations noted. |
| 6.5 | Monthly, NFP 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 compared to amounts in the monthly bank reconciliation. | Inspected 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 BDMP Assurance, LLP                                                                                                                                                                                             | Results of Tests     |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 6.6a | 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 the COO, and/or designee, reconciled the daily deposits between the CPBS system and the State of RI's Webster Bank account to the customer payments monthly. | No deviations noted. |
| 6.6b |                                                                                                                                                                                               | Inspected reconciliations and 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 are available for restoration in the event of processing errors or unexpected processing interruptions.

| No.  | NFP Health Control Activities                                                                                                                                                                                          | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                                                    | Results of Tests                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.1  | Full backups are automatically scheduled daily and replicated off-site.                                                                                                                                                | Inspected backup configurations to determine that full backups were configured to run daily 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 compliance status report for a selection of dates to determine that automated backup compliance status reports were sent for successes and failures to the 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.                                                                                                                                   | Inquired and confirmed with management to determine that there were no changes to backup job schedules during the examination period.                                                                                                                     | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |

| No. | NFP Health Control Activities                                                                                                                                                                              | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                 | Results of Tests     |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 7.5 | The systems hosted in third-party data centers are monitored daily by a Technology Operations Engineer. This review includes system-triggered alarms, uptime status, and connectivity of the data centers. | Inspected the Technology Operations Checklists for a selection of dates to determine that hosted systems, alarms, uptime status, and data center connectivity was monitored daily by a Technology Operations Engineer. | No deviations noted. |

## Security

**Control Objective 8:** Controls provide reasonable assurance that logical access to applications, operating systems and databases is restricted to authorized and appropriate personnel.

| No. | NFP Health Control Activities                                                                                                                                          | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                              | 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 ticket for a selection of terminated employees to determine that the manager notified IT of the employee's termination, and that IT removed access timely.                                       | No deviations noted.                                                                                                                                            |
| 8.3 | For transferred employees, the manager sends a notification form to IT and employees' access is updated based on their job function and responsibilities.              | Inquired and confirmed with management to determine that there were no transferred employees during the examination period.                                                                                                         | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 8.4 | Administrative access to AD, the CPBS system 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 BDMP Assurance, LLP                                                                                                                                                                                                                                   | Results of Tests     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| 8.6 | Password parameters for AD and the CPBS system are configured in accordance with the IT Policy.                                                                                                                                                     | Inspected the network and CPBS password parameters to determine that password parameters were configured to meet or exceed requirements of the IT Policy.                                                                                                                | No deviations noted. |
| 8.7 | Annually, the IT department conducts a user access review for the AD and the CPBS system 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 the AD and the CPBS system 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 system changes and upgrades are documented, tested, and approved prior to implementation.

| No. | NFP Health Control Activities                                                    | Tests Performed by BDMP Assurance, LLP                                                                                                            | Results of Tests                                                                                                                                                |
|-----|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.1 | Change requests are documented and authorized prior to the start of development. | Inquired and confirmed with management to determine that there were no BizApps or CPBS changes during the examination period.                     | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 9.2 | Change requests are tested prior to implementation to production.                | Inquired and confirmed with management to determine that there were no BizApps or CPBS changes during the examination period.                     | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 9.3 | Separate development, QA, and production environments are in place.              | Inspected communication connection attempts to determine that development, QA, and production environments were in place and logically separated. | No deviations noted.                                                                                                                                            |

| No.  | NFP Health Control Activities                                                                                                                                                                                                                                                                                                   | Tests Performed by BDMP Assurance, LLP                                                                                                                                                                                                                                                                                                       | Results of Tests                                                                                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.4  | Change requests are approved prior to implementation to production.                                                                                                                                                                                                                                                             | Inquired and confirmed with management to determine that there were no BizApps or CPBS changes during the examination period.                                                                                                                                                                                                                | Because no instances requiring the operation of the control occurred during the examination period, we were unable to perform tests of operating effectiveness. |
| 9.5a | Users with ability to update changes to the CPBS system are based on users' roles and properly authorized and monitored.                                                                                                                                                                                                        | Inspected the CPBS user list to determine that users with the ability to update changes to the CPBS system 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 a selection of production access tickets to determine that when developers required temporary administrator access, an IT ticket was created for access request and tacked to completion.                                                                                                                                          | No deviations noted.                                                                                                                                            |
| 9.6  | The Release Management Team organizes development meetings at least monthly, 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 development meeting minutes for a selection of months to determine that the Release Management Team met at least monthly 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.                                                                                                                                            |

*"BerryDunn" is the brand name under which Berry, Dunn, McNeil & Parker, LLC and BDMP Assurance, LLP, independently owned entities, provide professional services in an alternative practice structure in accordance with the AICPA Code of Professional Conduct. BDMP Assurance, LLP is a licensed CPA firm that provides attest services, and Berry, Dunn, McNeil & Parker, LLC, and its subsidiary entities provide tax, advisory, and consulting services.*

*Berry, Dunn, McNeil & Parker, LLC leases professional and administrative staff to BDMP Assurance, LLP. These individuals work under the direct control and supervision of BDMP Assurance LLP, which is solely responsible for their performance.*

*The entities falling under the BerryDunn brand are independently owned and neither entity is liable for the services provided by the other entity. Our use of the terms "our Firm" and "we" and "us" and terms of similar import denote the alternative practice structure of Berry, Dunn, McNeil & Parker, LLC and BDMP Assurance, LLP.*

*This report is the work of BDMP Assurance, LLP.*

©2026 BerryDunn | All rights reserved.



With offices and employees located in 40+ states—  
wherever you are based, we look forward to working together.

**berrydunn.com**