ATTACHMENT H: HIPAA QUESTIONNAIRE

As a covered entity, it is the responsibility of the North Carolina State Health Plan (Plan) to ensure its Members' health information is protected from use and disclosures not allowed under the Health Insurance Portability and Accountability Act (HIPAA), as well as applicable state and federal laws. The Plan takes this responsibility very seriously.

The purpose of this HIPAA Questionnaire is to allow the Plan to evaluate the HIPAA compliance of a prospective or current vendor who may request or require Member data containing protected health information (PHI). As a threshold to being considered to do business with the Plan, the Vendor must demonstrate that it meets the Plan's expectations for HIPAA compliance. The information provided below will be used by the Plan to determine the Vendor's level of understanding of HIPAA privacy and security rules, as well as its compliance status.

The Vendor is encouraged to thoroughly respond to all questions to the best of its ability and provide copies of all requested documentation. The Plan encourages the Vendor to have its privacy officer or other compliance specialist complete this questionnaire. Any incomplete responses may negatively impact the Plan's evaluation of the Vendor's HIPAA compliance, including a determination that the Vendor does not meet the Plan's expectations.

All responses must be typed. Handwritten responses will not be accepted.

If the Vendor maintains that any information contained in requested documentation is proprietary or otherwise confidential, the Vendor may redact these portions and supply the un-redacted portions for review.

Vendor Information:

Company name: UMR, Inc.

Address (city, state, and zip code): 115 W. Wausau Ave. Wausau, WI 54401-2875

Website URL: www.umr.com

Name of person completing form, and role: Jeff Giadone

Email address: jgiadone@uhc.com

Phone number: (714) 226-4108

Fax number: Not applicable

HIPAA compliance person's name, title, phone number, and email address, if different than person completing form:
Brian DuPerre

Chief Privacy Officer, Deputy General Counsel, Senior Vice President
UnitedHealthcare

(860) 702-7095

Brian_Duperre@uhc.com

Date you are completing this form: 9/14/2022

***** Please note that you must update the contact information provided in this questionnaire within 30 days of any change in personnel. *****

For all questions, if more detail is needed than the space provided allows for, please attach a separate page.

Compliance Questionnaire

1. **Details of the individual responsible for HIPAA Compliance (if this designated position does not exist, provide the details of the employee who typically handles HIPAA privacy and security issues within your company or organization).**

   Name: Brian DuPerre

   Title: UnitedHealthcare Chief Privacy Officer, Deputy General Counsel, Senior Vice President

   Address: 185 Asylum Street, Hartford CT 06103

   Phone number: (860) 702-7095

   E-mail address: Brian_Duperre@uhc.com

   Certification designation (e.g., CHC, CISSP, CIPP, CHP, CHPSE, etc.): Certified Information Privacy Professional (CIPP)

   Date certified: 10/19/2009

2. **If they are not certified, provide detailed information regarding training that has been provided to the person responsible for HIPAA compliance (e.g., date last received training, name of company or person that provided training, etc.).** Not applicable.

Employee HIPAA Training

3. **Which employees receive HIPAA training? How frequently is their training refreshed?**

   All full-time and part-time new hires and applicable contractors are required to complete UnitedHealth Group's Information Security and Privacy training as part of the onboarding process and annually.

   All UMR employees undergo initial and annual Health Insurance Portability and Accountability Act (HIPAA) training to ensure they understand the policies and procedures that support HIPAA compliance. The training covers a variety of topics, such as transmitting protected health information (PHI) safely and securely, by either electronic or paper-based means; appropriate conduct when discussing PHI with a co-worker or supervisor; protecting PHI at their workstations; and appropriate storage of PHI data. We also have extensive safeguards in place to protect our facilities and IT systems to ensure safe transfer and storage of PHI-related data.

4. **Do all the above employees receive comprehensive training (i.e., training which covers the privacy and security of PHI; both physical and technical)? Yes** X **No** ☐

   a. If no, provide details of the level of training made available to employees.

   Not applicable.

5. **When was HIPAA training last updated? When is the next planned update?**

   We implement necessary actions for timely compliance with the American Recovery and Reinvestment Act (ARRA) provisions. To the extent that the law requires modifications to our current practices, policies, training or systems, we effectively adopt and implement revised practices, policies, training and systems to meet the various compliance effective dates outlined in the law and subsequent regulations. We also closely monitor Health and Human Services (HHS) Office for Civil Rights (OCR) on the ARRA for additional guidance from provisions and to make appropriate adjustments to our practices, policies, training and systems.

6. **Are there internal HIPAA privacy policies and procedures in place which govern the privacy practices of the organization and its employees? Yes** X **No** ☐

7. **Attach a copy of all internal/employee-facing privacy policies and procedures.**

   Please refer to the document titled: UnitedHealth Group - Privacy – UHGPrivacyPolicyManual.

   a. Note when the privacy policies were last reviewed or updated:

May 2022

8. **Are employees trained on the privacy policies and procedures? Yes** X **No** ☐

9. **Are employees required to sign an agreement stating they have read and understand the privacy policies and procedures? Yes** X **No** ☐

10. **Are there internal HIPAA security policies and procedures in place which govern the security practices of the organization and its employees? Yes** X **No** ☐

11. **Attach a copy of all internal/employee-facing security policies and procedures.**

    Please refer to the documents titled:

    - UnitedHealth Group - Policies - Information Security - Enterprise Information Security Policy
    - UnitedHealth Group - Policies - Information Security - 1A Security Program Management

    a. **Note when the security policies were last reviewed or updated:**

       These documents were updated on 1/5/2022 and 7/31/2022, respectively.

12. **Are employees trained on the security policies and procedures? Yes** X **No** ☐

13. **Are employees required to sign an agreement stating they have read and understand the security policies and procedures? Yes** X **No** ☐

14. **Can you provide documentation that all employees have completed training? Yes X No** ☐

15. **Has your organization received any certifications regarding HIPAA compliance? (If yes, please provide copies of the certification and the date when the certification was awarded.)**

    Our last Health Information Trust Alliance (HITRUST) certification was April 30, 2021 and is valid for two years. Please refer to the documents titled:

    - Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
    - Optum_2021-_HITRUST_Interim_Letter
    - UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

16. **When was the last time your company was audited to determine HIPAA compliance? Provide date the audit was performed and the name of the company who performed it. Provide copies of the audit findings.**

    We have a continuous/revolving HIPAA audit model. Our Enterprise Information Security staff is continuously making HIPAA security assessments. HITRUST is annual, and we have over 70 SOC audits each year. Internal audit has various areas tested each year, Deloitte does baselines as a part of their certification of our financials, and we do regular HIPAA program maturity assessments. CMS and the Departments of Insurance (and some self-insured customers) test various elements regularly, and for special purposes, we engage Price Waterhouse Coopers (PWC) and others to conduct reviews.

    The results of most assessments are confidential to UnitedHealth Group and are not typically shared outside the company.

    Our last HITRUST certification was April 30, 2021 and is valid for two years. Please refer to the documents titled:

    - Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
    - Optum_2021-_HITRUST_Interim_Letter
    - UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

Data Security

17. Provide details of the methods the company employs to secure and render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

At all times, employees are required to apply the Minimum Necessary rule when using, sending, or sharing PHI to perform business functions. UnitedHealth Group requires business associates to appropriately safeguard individually identifiable health information and have established HIPAA compliant contractual agreements with our trading partners and other business associates.

The Minimum Necessary rule applies when sending or sharing PHI internally within our organization and externally with customers and their trading partners. We limit the disclosure of PHI to that which is permitted or required by law and is necessary to administer our business, provide quality service, and meet regulatory requirements. UnitedHealth Group's offshore vendors use the same systems as domestic sites and have access to the same information. UnitedHealth Group employs a number of access control features to secure systems and information including:

- User authentication by ID and password
- User access on a need-to-know basis
- Prescribed network and application-level security.

These safeguards are reviewed on a regularly scheduled basis by our internal auditors, as well as, independent auditors. Managers are responsible for determining access levels required for the end-user to perform his/her job function. Inactive/terminated users are purged. Platform level access is revoked immediately if a user is terminated for cause or on the last day of employment. Policies and standards require that user IDs, date/time for logoff, successful/unsuccessful system, data, and resource access attempts are logged and retained.

CONFIDENTIALITY OF INFORMATION

With respect to confidentiality, UnitedHealth Group employs the same standards used in our onshore sites to govern our offshore sites (both UnitedHealth Group sites and those of third-party vendors). UnitedHealth Group's training, quality, and management personnel are a frequent on-site presence at global locations to ensure that operations meet our standards for security and decorum. Offshore personnel receive the same training provided to our domestic employees. The curriculum includes a detailed unit on confidentiality, security, and privacy concerns. Additionally, in compliance with HIPAA regulations, the following training is provided based on job type to all offshore staff:

- HIPAA overview
- HIPAA protected health Information (PHI) course
- HIPAA privacy individual rights process
- HIPAA privacy clarifying scenarios
- Handling HIPAA calls in Intelligent Desktop (IDT)
- Review of confidentiality job aid

BACKGROUND CHECKS AND EMPLOYEE SCREENING

Just as in UnitedHealth Group's domestic hiring process, all offshore resources, whether UnitedHealth Group employees or third-party vendors must undergo background screenings prior to receiving an offer of employment.

OTHER SECURITY CONTROLS

UnitedHealth Group's security controls are designed to satisfy best business practices and regulatory and business requirements to ensure protection of information and business process efficiencies. These security controls include:

- Firewall management
- Intrusion detection
- Vulnerability assessments
- Policy and standard definitions and refinements
- Encryption
- Security administration management tools

Ongoing audits initiated internally or by customers and/or regulatory agencies provide the checks and balances to identify gaps and plan for remediation.

18. Describe security procedures – physical, technical, and administrative – in place to ensure the confidentiality of PHI internally, and when transmitting data externally to the Plan or to Plan vendors.

Optum complies with all applicable HIPAA rules, including the current applicable HIPAA privacy requirements. We implement appropriate and reasonable controls to protect the privacy and security of confidential and sensitive information, including PHI and ePHI. In addition, Optum continues to follow all applicable federal and state laws that affect the confidentiality of consumer information. We continually assess and enhance our HIPAA privacy and security program to the controls and safeguards as necessary. For additional details please refer to the document titled: UnitedHealth Group - Policies - Information Security - 13A Data Classification and Protection.

TRANSMITTING DATA EXTERNALLY

UnitedHealth Group's Information Security Policies and Standards require that standard encryption solutions and protocols be employed in the external transmission of confidential and proprietary information. This includes but is not limited to:

- SSH
- SFTP (FTP over SSH)
- HTTPS (HTTP over SSL)

Information Security Policies, standards, procedures, technical protocol, and operation protocols ensure the control of secured information transmissions. Selected encryption algorithms used to protect data must be industry tested and peer-reviewed according to best practice standards (i.e. Advanced Encryption Standard (AES)-256). This provides verification of strength against known attacks along with validation of sufficient key length and random key distribution to minimize brute force attack and mathematical analysis of keys.

In addition, UnitedHealth Group encryption technology standards require a minimum key length of 256-bits for secret (symmetric) encryption and 2048-bits for public/private (asymmetric) encryption. These are the minimum standards. Longer key lengths may have been implemented within specific environments, based on risk. Secure hash algorithms are used to create a message digest with a minimum length of 256 bits.

19. Do you have procedures to identify and respond to suspected or known security incidents; mitigate (to the extent possible) harmful effects of known security incidents; and document incidents and their outcomes? Please describe.

Yes. UnitedHealth Group's Security Incident Response Team provides oversight in the handling of security and privacy related incidents across the enterprise. Forensic investigation and preservation of evidence are included as part of this team's responsibilities. Each UnitedHealth Group business segment Information Security Officer and Privacy Officer serves as members of the Security Incident Response Team.

The Security Incident Response Team has the following responsibilities:

- Coordinating incident detection, analysis, containment, mitigation, recovery, and final reporting efforts to assure timely resolution of all security and privacy incidents upon identification.
- Coordinating any/all notification to required entities as an outcome of a security/privacy related incident.
- Participating in the activities and decisions across cross-functional workgroups in developing the security/privacy incident response requirements, conducting gap-analysis, recommending compliance action plans, reporting, tracking security and privacy incident trends, and providing process improvement recommendations.

Please refer to the document titled: UnitedHealth Group - Incident Response - Incident Response Process Overview - Customer Copy.pdf

20. Has the company conducted a risk assessment and gap analysis to address any findings?
Yes X **No** ☐

If yes: Date: Performed by:

The company's IT environment is audited by various internal and external entities. UnitedHealth Group contracts with various third party vendors to perform assessments on behalf of management of its internal IT controls via ICFR (Internal Controls over Financial Reporting) and SSAE (Statement on Standards for Attestation Engagements) audits. These audits are inclusive of platform and application controls and are performed continuously to ensure operating effectiveness throughout each year.

UnitedHealth Group's businesses self-assess their control environment (both IT and operational controls, where applicable) via Internal Audits and HITRUST assessments, which are spread throughout each year. Various regulatory agencies, as well as, UnitedHealth Group customers perform audits of UnitedHealth Group throughout each year, which include a review of key IT and operational controls.

The results of most assessments are confidential to UnitedHealth Group and are not typically shared outside the company, with the exception of, but not limited to SSAE SOC 1 Type 2 reports, where allowed and penetration test result summaries. SSAE SOC 1 Type 2 is the audit standard under which our independent auditor issues our SSAE SOC 1 Type 2.

21. Can you provide a copy of a SOC2, Type 2 security assessment report or a report performed under another security framework that can be cross-walked to the appropriate NIST-800-53 security control requirements (e.g., ISO 27001, HITRUST) for each service component used/involved in the proposed services? Yes (*please attach*) X **No** ☐

Please refer to the documents titled:

- Optum_2021-_HITRUST_CSF_Cert._Ltr._1020-1574_(Final)
- Optum_2021-_HITRUST_Interim_Letter
- UnitedHealthcare E&I 2022 - HITRUST r2 Cert.Ltr. Final (2)

a. How often does the company conduct these types of audits?

HITRUST certification is issued by HITRUST – an independent organization, and is valid for a two-year period with annual validations for ongoing compliance. We maintain several HITRUST certifications to cover different in-scope systems/environment.

22. Provide the number of HIPAA violations reported to the Office of Civil Rights (OCR) in the last five years, the details of the violation, and include the amount of the fine incurred (if any).

We have not responded to any HIPAA complaints from the Office of Civil Rights that would make us unable to perform services described in this proposal.

For confidentiality reasons we are unable to disclose detailed information. We understand the sensitivity and seriousness of a privacy or security incident, regardless of the cause. We also recognize that not all

reported incidents are actual incidents and that not all actual incidents are the result of an inappropriate or malicious intent. Our commitment is to make sure that we appropriately manage and thoroughly investigate all reported incidents.

23. Does the company have in place procedures for the destruction of PHI compliant with the standards set forth in NIST Special Publication 800-88 Revision 1 (or most recent update) located at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf? Yes X No ☐

a. If yes, please describe the procedure for that destruction.

UnitedHealth Group's media destruction policy and control standards align with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization or U.S Department of Defense (DoD) manual 5220.22:

- Overwrite all addressable locations with a seven pass process
- Verify and document that the overwrite has been performed
- Physically destroy media which cannot be properly overwritten

Domestically, all vendors and third parties that UnitedHealth Group utilizes for destruction services are either National Association for Information Destruction (NAID) certified or certify that their operational process exceeds requirements of NAID certification. In addition, vendors are screened and evaluated for strict compliance to our security requirements. Vendors are required to attest that all Electronic media and/or Memory are sanitized or destroyed according to their process.

UnitedHealth group has the right to review a vendor's sanitization/destruction of electronic media/memory process at any time. Upon request by UnitedHealth Group, the vendor is required to provide evidence of design and effectiveness for their sanitization/destruction of electronic media/memory processes.

From a media perspective the following occurs:

- Hard drives:
  - All hard drives are subject to the seven pass DoD wipe
  - If the hard drives will not be re-used after complete sanitization they are shredded onsite as witnessed by an employee
  - Serial numbers of hard drives are documented and retained as a destruction record
- Tape media:
  - Tapes are not reused
  - Tapes are degaussed and shredded
  - The tape management system is updated to reflect status and a destruction record retained
- Removable media:
  - Utilization is by exception only via a formal process
  - All media is shredded when no longer required

Subcontractor Information

24. Do you outsource work to Subcontractors who would have access to Plan data and PHI and who may qualify as Business Associates as defined by HIPAA? Provide the names of the companies, contact information, and details of what they are contracted to do.

Yes. We provide most of our core services directly through the UnitedHealth Group family of companies. This enables us to offer affordable solutions through integrated data elements and systems, streamlined implementations and unified account management support. While most services are performed in-house or through sister companies, there are times we partner with external vendors for certain services. In these cases, we will remain fully responsible for these services and for the performance of these vendors or subcontractors. We hold our vendors and subcontractors to the same standards and requirements that we accept under our agreement with The Plan.

[redacted]

Below is a partial list of subcontractors. Because of the broad spectrum of UnitedHealth Group businesses and vendor relationships, we are unable to provide a complete list of proposed vendors/subcontractors and/or the level of detail you are requesting. Where vendors/subcontractors are required to support a customer relationship,ould typically select the vendors/subcontractors based upon the customer's specific requirements.

25. Have you entered into Business Associate Agreements (BAAs) with all Subcontractors who may qualify as Business Associates to your company or the Plan for this work? If yes, provide copies of the executed BAA(s).

Yes. We include a business associate agreement (BAA) in our Master agreement with suppliers. The Enterprise Supplier Risk & Performance Management Program provides the structure and framework to consistently identify, document and mitigate third-party supplier risks and to enforce contractual obligations and performance standards.

While we can identify the names of subcontractors, the actual subcontractor arrangements are considered proprietary. UMR will be responsible for services performed by our affiliates or subcontractors to the same extent that we would have been had the services been performed by us.

While the contracts signed between UMR and our subcontractors are considered proprietary and are not available for proposal purposes, upon award of business, The Plan will be permitted to conduct an on-site, closed door, white-room review of the contracts, at our office. UMR will schedule the appropriate visit upon request.

In addition, the UnitedHealth Group external facing website, **https://www.unitedhealthgroup.com/suppliers**, contains publicly available information related our organization's expectations and requirements for suppliers.

26. How do you enforce and monitor HIPAA policies with Subcontractors and Business Associates? What penalties or fixes are in place for violations?

Prior to selecting subcontractors, UMR completes a thorough review of qualifications. In order to contract with us, vendors must agree to and meet specific service-level expectations for quality, security, accuracy and pricing. We conduct both physical and electronic security checks of the vendors' facilities to ensure compliance with HIPAA regulations as well as our own security standards. Additionally, our standard contract requires vendors to file a business continuity plan to demonstrate how they would continue operating should a disastrous event occur.

UNITEDHEALTH GROUP ENTERPRISE INFORMATION SECURITY ASSESSMENT

UnitedHealth Group requires that effective information security controls be in place for External Parties. External Parties are defined as contractors, vendors, suppliers, business venture parties, auditors or assessors, cloud service providers, research agreements, government entities, or others who are involved in this Scope of Services.

External Parties must be assessed by Enterprise Information Security (EIS) prior to initiating any Scope of Services. EIS will utilize a risk and location-based approach to determine the level of information security assessment required. External Parties must demonstrate sufficient information security controls based on the Scope of Services, risks, locations, and relevant factors.

EIS may directly assess an External Party, and/or may accept the certification(s) achieved by External Parties to satisfy this requirement. The following are some of the certifications or third party assessments that will be considered:

- HITRUST certification
- International Standards Organization (ISO)-27001
- Service Control Organization 2 (SOC2) Type 2 mapped to HITRUST
- Third party or certification standard as contractually required

Certifications must be maintained for the duration of the relationship with the UnitedHealth Group. Remediation activities required by EIS or required to maintain the accepted certification must be implemented by the External Party within the timeframes prescribed.

External parties must acknowledge their responsibility for safeguarding the UnitedHealth Group's information technology (IT) systems and information assets via a formally written and legally binding agreement. Such agreements must follow applicable UnitedHealth Group policies, including Enterprise Sourcing & Procurement and Delegation of Authority policies. UnitedHealth Group maintains a standardized Security Exhibit template when Protected Information is in scope for the business engagement. Any negotiated modifications to the Security Exhibit must be approved by the UnitedHealth Group's Corporate Legal Department and Enterprise Information Security (EIS).

Where applicable, a Business Associate Agreement (BAA) is also required when a Business Associate (BA) of any of UnitedHealth Group's covered entities will create, receive, maintain, or transmit electronic Protected Health Information (ePHI) for or on behalf of UnitedHealth Group.

If the BA requires connectivity to the UnitedHealth Group information technology (IT) systems, information assets, or information entrusted to

UnitedHealth Group, modifications to the BAA must also be approved by the Enterprise Information Security (EIS) Organization.

Additional agreements other than a BAA may be required depending on business or legal requirements.

Please refer to the document titled: **UnitedHealth Group - Policies - Information Security - 10A External Party Security**

27. Have you conducted an audit of any Subcontractors or Business Associates? Can you provide information as to whether they are HIPAA complaint at this time? Include all available SOC2, Type 2 or substitute reports for Subcontractors and Business Associates.

UMR and UnitedHealth Group conduct both physical and electronic security checks of the vendors' facilities to ensure compliance with HIPAA regulations as well as our own security standards. UnitedHealth Group supports HITRUST, an expansion of the health care industry's use of the Common Security Framework (CSF) Assurance Program. In support of that objective we require third-party suppliers with access to our information systems and/or customer or health plan member data to adhere to the requirements listed in HITRUST to ensure proper security controls.

Please refer to the document titled: **UMR Claim Administration Processing System_CPS 2021 SOC 1 Type 2 Report**

Emergency/Contingency Plans

28. Describe the company's disaster recovery plan for data backup, data recovery, and system testing should a disaster occur (e.g., flood, fire, or system failure).

UnitedHealth Group developed an Enterprise Resiliency & Response Program that minimizes customer impact from disrupted service in a significant event or disaster, while aiding compliance to published regulatory guidelines. As a UnitedHealth Group company, UMR has plans to address all natural and human-caused disasters (i.e. hurricanes, floods, fires, terrorism, and pandemics).

The business continuity plans focus on critical business functions and planning for the worst-case scenario so that we can react quickly and efficiently, adding value to our business and customers through effective risk reduction, compliance with industry, contractual or regulatory standards, and safeguarding of operations and assets.

UnitedHealth Group's business impact analysis and subsequent business continuity plans are written to accommodate the following four scenarios:

- **Loss of Facility:** Complete interruption of facilities without access to its equipment, local data, and content. The interruption may impact a single site or multiple sites in a geographic region. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical People**: Complete interruption with 100% loss of personnel within the first 24 hours and 50% loss of personnel long-term. The interruption may impact a single site or multiple sites in a geographic area. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical Systems**: Complete interruption and/or access of critical systems and data located at the various UnitedHealth Group data centers for an extended period of time. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical Vendor:** Complete interruption in a service or supply provided by a third-party vendor. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

The impact of the operational loss due to one, or all, of these scenarios is assessed as part of the original Business Impact Analysis and annually thereafter. The business continuity plans are updated

quarterly and exercised annually.

Business continuity plans are leveraged as needed to address all forms of emergencies, which may impact business operations including short and long-term events. Examples of short-term events include power outages and winter weather office closings. These plans also address more severe, long-term situations, such as building fires and major hurricanes.

Business functions classified as critical generally provide for near immediate failover of core services by leveraging geographically dispersed, redundant operations and maintaining a recovery time objective of 72 hours or less. The plans are written to respond to a disaster lasting a minimum of 90 days.

In the event a disaster impacts our members, we will comply with any and all emergency orders mandated by the state Department of Insurance, Centers for Medicare and Medicaid Services (CMS), or Health and Human Services (HHS). The Event Management Team continually monitors for natural disasters and the potential impact on healthcare delivery services. If the situation warrants it, emergency provisions may be provided, even if not mandated.

An overview document is available, which describes the governance, strategy, and controls for the entire program. This document is not intended to replace the business continuity or disaster recovery plan review, but does provide the reassurance that UnitedHealth Group has a well-defined program in place to make sure customer impact is minimized during a disaster. Please refer to the document titled: **UnitedHealth Group - BCP-DR - Enterprise Resiliency and Response Customer Response Document.pdf.**

a. Provide the details of any incident that that has required activating the disaster recovery plan within the last two years, and any changes to the plan that were made as a result.

To maintain the confidentiality of our member and employee information, as well as, the integrity of our business operations, UnitedHealth Group considers this information proprietary and confidential.

Additionally, a post-event assessment is performed after any situation, which results in activation of the business continuity plans. This assessment is performed to learn from the experience and enhance business function preparedness and capabilities to respond and recover more effectively and efficiently. The results of our post-event assessments are also considered proprietary and confidential and are not provided to customers.

29. Describe the company's business continuity plan in the event of a disaster (e.g., flood, fire, power failure, system failure).

UnitedHealth Group developed an Enterprise Resiliency & Response Program that minimizes customer impact from disrupted service in a significant event or disaster, while aiding compliance to published regulatory guidelines. We have plans to address all natural and human-caused disasters (i.e. hurricanes, floods, fires, terrorism, and pandemics).

The business continuity plans focus on critical business functions and planning for the worst-case scenario so that we can react quickly and efficiently, adding value to our business and customers through effective risk reduction, compliance with industry, contractual or regulatory standards, and safeguarding of operations and assets.

UnitedHealth Group's business impact analysis and subsequent business continuity plans are written to accommodate the following four scenarios:

- **Loss of Facility:** Complete interruption of facilities without access to its equipment, local data, and content. The interruption may impact a single site or multiple sites in a geographic region. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical People**: Complete interruption with 100% loss of personnel within the first 24 hours and 50% loss of personnel long-term. The interruption may impact a single site or multiple sites in a geographic area. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical Systems**: Complete interruption and/or access of critical systems and data located at the various UnitedHealth Group data centers for an extended period of time. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

- **Loss of Critical Vendor:** Complete interruption in a service or supply provided by a third-party vendor. Recovery from anything less than complete interruption will be achieved by using appropriate portions of the plan.

The impact of the operational loss due to one, or all, of these scenarios is assessed as part of the original Business Impact Analysis and annually thereafter. The business continuity plans are updated quarterly and exercised annually.

Business continuity plans are leveraged as needed to address all forms of emergencies, which may impact business operations including short and long-term events. Examples of short-term events include power outages and winter weather office closings. These plans also address more severe, long-term situations, such as building fires and major hurricanes.

Business functions classified as critical generally provide for near immediate failover of core services by leveraging geographically dispersed, redundant operations and maintaining a recovery time objective of 72 hours or less. The plans are written to respond to a disaster lasting a minimum of 90 days.

In the event a disaster impacts our members, we will comply with any and all emergency orders mandated by the state Department of Insurance, CMS or HHS. The Event Management Team continually monitors for natural disasters and the potential impact on healthcare delivery services. If the situation warrants it, emergency provisions may be provided, even if not mandated.

An overview document is available, which describes the governance, strategy, and controls for the entire program. This document is not intended to replace the business continuity or disaster recovery plan review, but does provide the reassurance that UnitedHealth Group has a well-defined program in place to make sure customer impact is minimized during a disaster. Please refer to the document titled: **UnitedHealth Group - BCP-DR - Enterprise Resiliency and Response Customer Response Document.pdf.**

a. Provide the details of any incident that that has required activating the business continuity plan within the last two years.

UnitedHealth Group has never needed to implement our disaster recovery plans in response to a catastrophic outage of technology at our production data centers.

To maintain the confidentiality of our member and employee information, as well as the integrity of our business operations, UnitedHealth Group considers this information proprietary and confidential.

I hereby certify that the information provided above and attached hereto is true and correct to the best of my knowledge and belief.

Scott Hogan

Name (Type)

Signature

09/16/2022

Date