6. Management Information System (Section 15 Management Information System)

a. Provide a detailed description, diagrams and flowcharts of the Management Information System (MIS) the Vendor will use to support all aspects of Kentucky's Medicaid managed care program including the following subsystems:

i. Enrollee Subsystem;

ii. Third Party Liability (TPL);

iii. Provider Subsystem;

iv. Reference Subsystem;

v. Claims Processing Subsystem (to include Encounter Data);

vi. Financial Subsystem;

vii. Utilization/Quality Improvement Subsystem; and

viii. Surveillance Utilization Review Subsystem (SURS).

As part of the response, include information about the following:

i. Required interfaces, how the system will share and receive information with the Department, how the Vendor's system will use files provided by the Department, Subcontractors, providers, and other supporting entities.

To accommodate large, frequent and complex interface, transmission, acceptance and submission protocol and processes, we rely on our Electronic Communication Gateway (ECG) for interface and data file exchanges. Our ECG provides a secured and security-compliant electronic transport mechanism for internal and external business customers to exchange data files on demand or via scheduled integration with job automation and control services, including transmission validation audit reporting. Our systems are designed to support electronic data interchange (EDI) using batch and real-time services that allows for fast, easy integration with state and federal information technology (IT) systems and data sources, real-time services route through either a Layer 7 or StarGate gateway.

How Our Systems Use Files from the Commonwealth and Other Entities

We will implement and manage the Kentucky MCO program on our shared strategic platform, Community Strategic Platform (CSP). The systems composing the platform are shared across UnitedHealthcare states, and some systems, like our portals, business-to-business EDI framework, and utilization management platform, are shared across UnitedHealthcare segments, products and customers. We do this to manage costs, share common services and supports, and exercise best standard practices gathered globally from the industry and across our states and products.

Our flexible interface architecture can support changing file formats and data elements with little or no change needed by the sending systems. While industry standards are preferred, we can support proprietary or need-specific interfaces. We will comply with the requirement to have a Business Associates Agreement in place before implementing any interfaces with subcontractors, providers and other entities. All of our interfaces with the Commonwealth will comply with requirements contained in 42 C.F.R. 438. Aligning with the unique data set being used or exchanged for the intended internal or external operational or business purpose, we support numerous types and levels of information processing and data exchange, including:

- ***Claims/Encounters:*** We accept EDI claims through our clearinghouse in all standard formats. We create and submit encounter files in the required formats: 837P

(professional), 837I (institutional), 837D (dental), NCPDP PAH (pharmacy) using NEMIS, our encounter data submission and reporting system. We will collect, validate and submit encounter data regularly through established interfaces with the Commonwealth. We process acknowledgment files (999, 277CA, TA1 and pend/denied files [277CA, 277U]).

- ***Reporting:*** For a typical Medicaid partner, we produce more than 70 standard reports from various systems. Our management information systems (MIS) enable us to be fully prepared to meet the data element and format requirements to provide all Kentucky MCO program required management reports.
- ***Enrollee/Enrollment:*** We process 834 enrollment daily, and weekly/monthly reconciliation data, from all of our state partners. We process this data through our real-time Electronic Eligibility Management System (EEMS) enrollment engine and load it into CSP with little manual intervention. Enrollment data is passed on to subcontractors daily.
- ***Finance:*** Our revenue reconciliation system accepts the Commonwealth's capitation files through HIPAA-compliant 820 transactions. If discrepancies are identified, detailed reports are provided to the Commonwealth.
- ***Providers:*** Our National Provider Database allows for the setup of networks, provider demographics, and the storage of national and state (Commonwealth) provider identifiers (e.g., NPI) using the state's provider files. Our contracted providers can use our online provider portal, *Link*, to view, edit and attest to their demographic information. Providers may use our real-time HIPAA standard 270/271, 276/277 and 278 services for eligibility and benefits, claims and prior authorizations, and 835 for remittance advices. Our ACQH CORE-certified real-time 270/271 service alone responds to more than 20 million eligibility searches every month across our 31 Medicaid states.
- ***Reference Files*:** We process and use all other reference files, including provider records/profiles, procedure tables and fee schedules. We accept provider and profile reference files so they can be used by our claims platform for editing and resolving provider data discrepancies.

ii. Capability to store and use large amounts of data, to support data analyses, and to create standard and adhoc reports.

Supporting Kentucky's Medicaid MCO program, we will use an array of traditional and modern reporting and storage tools, comprehensive of both traditional structured query language (SQL) relational data marts and our on-premises cloud-based Hadoop "Big Data" repository. We have the capability and storage necessary to produce standard and ad hoc reports required under this Contract. Our integrated reporting and data analytics solution, SMART, is Oracle Exadata-based, providing a scalable, comprehensive, integrated analytical environment that holds all Medicaid and Medicare relevant information. Storing over 140 terabytes today, this scalable system comprehensively integrates claims data (e.g., medical, behavioral, pharmacy, financial, demographic, socioeconomic, vision and lab), as well as enrollee, provider, authorizations, subcontractor, predictive modeling information and HEDIS gaps in care data and results for all our enrollees. Our big data environment allows for unlimited storage and processing capacity.

MIS Storage and Record Retention Capabilities

We recognize that with a Medicaid managed care program as complex as Kentucky's, the importance of implementing and maintaining sufficient MIS capability and storage capacity is critical to the program's current and future success. Continuously, UnitedHealthcare proactively identifies needed expansion or upgrades to support our enrollees, providers and the Commonwealth with expedient and continuous IT operations. We assess system capability and capacity needs using predictive modeling to forecast 18 months of anticipated changes, in

combination with constant machine learning (ML)-based performance monitoring of key system indicators. Our ML monitor is capable of not only raising alerts but also taking key preemptive actions to prevent outages. We use this information to create plans to increase capacity proactively, before it is needed. Our flexible and scalable systems architecture enables us to expand capacity without risk or material operational impact quickly. In addition, we employ powerful, proven data collection, storage and analytics systems to meet the reporting and analytics requirements outlined in the Contract Appendix D. Reporting Requirements and Reporting Deliverables. We describe our reporting capabilities in detail in Attachment C.6.a. UnitedHealthcare Management Information System.

Supreme Storage Capacity
Storage capacity across our information systems environment is currently over 100 petabytes. One petabyte is equivalent to all of the content in the U.S. Library of Congress — by its claim the most extensive library in the world — multiplied by 50. Through our parent organization, UnitedHealth Group, we employ more than 20,000 technology professionals responsible for computing hardware, software and communications; these resources are committed to maintaining the highest quality of service.

For the Kentucky Medicaid MCO program, in compliance with the Contract and in accordance with 42 C.F.R. 438.2 and 907 KAR 1:672, or as amended or until all issues are resolved, whichever is later, we will maintain and make available all records for review by authorized personnel of the Commonwealth, state and federal personnel for a period of 10 years after termination of this Contract. On behalf of our client, the Commonwealth, we retain all records in our secure and redundant archival systems. We run incremental backups daily and full backups weekly. We comply with offsite storage and remote backup requirements, including operating instructions, procedures, reference files, system documentation and operational files.

Records retention procedures also will follow our enterprisewide policy on records retention and contract requirements. Training on provider medical record requirements will follow the current process for training and educating providers on record keeping expectations through functional partners.

Analysis and Reporting Capabilities

The SMART Analytics Toolset stores multiple years of detailed transactions to enable trend analysis and full drill down from aggregate data to detailed data, such as specific claims and authorizations. SMART allows us to meet the Commonwealth's standard and ad hoc reporting requirements. For analytics, we use our MicroStrategy data mining and multi-dimensional analysis tool to define key metrics. Using MicroStrategy, our analysts view these metrics at the most macro level, such as per member per month (PMPM) costs, utilization and rates by product, geography (e.g., county or ZIP code). Tableau, our Hotspotting tool, allows us to identify enrollees with high needs or high costs (medical, behavioral, health-related resource needs) quickly to better address their complex needs and social determinants of health in our ongoing efforts to the total cost of care. Our "Big Data" investments have introduced Tableau, MarkLogic, BusinessObjects, Splunk, MapR, and other software tools into our reporting and analytic subsystems. These analytics tools provide online analysis, drilling to details, sorting, pivoting, exporting and printing. We integrate data into our data repositories from sources external to our core operations systems, including provider and encounter data from our subcontractors (e.g., vision and dental) and pharmacy encounter data.

iii. Extent to which these systems are currently implemented and integrated with other systems, internal and external, and the Vendor's approach for assuring systems that are not fully implemented and integrated will be ready to begin operations on required timeframes.

Diagrams and flowcharts should show each component of the MIS and the interfacing support systems used to ensure compliance with Contract requirements.

Diagrams and flowcharts of our MIS, including systems and subsystems that comply with 42 C.F.R. 438.242 and that we will be using to support all aspects of Kentucky's MCO program and Attachment C – Draft Medicaid Managed Care Contract, are located in Attachment C.6.a. UnitedHealthcare Management Information System.

C.6.a.iii Extent to which our Systems are Integrated with Others

Our MIS is fully implemented in more than 30 states. We will use our integrated core system and set of tools for Kentucky using the same platform that supports our Medicaid managed care contracts. Our systems architecture accommodates scalable expansion, allowing us to introduce routine upgrades quickly with the latitude to plan for significant increases in computing needs without risk or material operational impact. We have broad and recent systems implementation experience with 16 successful implementations and the transition of almost 2 million individuals between January 2016 and December 2018. In 2019, we completed five projects, successfully transitioning nearly 800,000 Medicaid program members.

How We Assure Systems are Operational by Required Time Frames

As detailed in our implementation work plan, by DMS's readiness review and implementation due dates, we will have deployed our project governance approach and Project Management Body of Knowledge (PMBOK)-driven project management principles and techniques. We will ensure internal and external systems integration; interface and functionality tasks have been completed and tested according to DMS's readiness and implementation requirements. Our MIS director, Glenn Walsh, will collaborate with our implementation and readiness lead, Sharon Slotnick, to confirm system readiness and integration with internal and external systems. In addition, they will oversee our systems capacity, testing and configuration activities to accommodate all contractual requirements and enable a seamless transition with uninterrupted access to services for enrollees and timely payment for providers. Our approach will build on our mature, existing platform and environments and use our existing interfaces with current customers and vendors. Wherever possible, we will use standard and existing formats and adapt them to the specific business needs for Kentucky.

b. Provide a description for and list of potential risks and mitigation strategies for implementing new information systems and changes to existing systems to support the Kentucky Medicaid managed care program.

Experience has taught us that an organized, thorough and collaborative approach to program implementation is the key to mitigating and avoiding risks. Our risk mitigation strategy for implementing our IT systems and performing change management of our existing systems that will support the Kentucky Medicaid managed care program are described next.

Potential Risks and Mitigation Strategies

A sampling of some common potential risks, based upon our extensive experience and recent health plan implementations, is presented in the table herein. Our implementation and MIS leads (Ms. Slotnick and Mr. Walsh) will work with the Commonwealth to verify risks are appropriately identified, managed, and have an agreed-upon risk mitigation strategy.

Potential Risk	Risk Mitigation Strategy
Timing of the First 834-Enrollment File	Loading the initial 834 enrollment file correctly and confirming enrollment information flows to the appropriate systems correctly so enrollee materials are mailed timely is critically important. To overcome this risk, we build in additional time to upload this first file compared to subsequent files. Receiving the first 834 file at least 30 days prior to the go-live date is preferable and

Potential Risk	Risk Mitigation Strategy
	enables us to perform downstream enrollee outreach activities timely. Receiving ID cards in advance of their effective date will be especially important for enrollees served through the Kentucky Medicaid MCO program, particularly for enrollees currently receiving services, needing prescriptions filled and those who have scheduled appointments. Sending and loading the 834 file earlier will enable us to produce and distribute ID cards in batches and to manage the related influx of calls that ensue when enrollees receive new ID cards and transition to this new program. Our implementation and MIS leads will work with the Commonwealth to develop the file timing for this program.
New IT Systems Implemented	When a state updates or introduces new programs that require connections and sharing of data, we must confirm the systems interface flawlessly and correctly before the changes are implemented. A good example of this is the requirement to implement an Electronic Visit Verification (EVV) system. We mitigate this risk through proactive and frequent communications with the state agency's IT systems support staff or vendor, produce and distribute well thought out and clear system documentation, emphasize system integration testing, and the coordination of the data exchange processes. Our implementation and MIS leads will work with the Commonwealth to ensure a seamless transition to any new system the Commonwealth implements.
Mismatch of Provider Data due to Multiple Sources of Record	States usually maintain their provider data, which they collect and enumerate by certain categories or with multiple data elements using homegrown or industry-recognized codes or taxonomy (e.g., NPI, specialty, type, rural, urban). When the state's provider data must align with ours, the potential risk is that our systems will not recognize or match the providers appropriately, thus compromising provider data integrity. We mitigate this risk by understanding the state's requirements and provider enumeration processes, employ knowledgeable resources familiar with provider data that work extensively on this type of exchange, and tightly coordinate and test data exchanges required.
Data File Transmission	We receive data from external entities that we cannot open, read or use as intended. To mitigate this risk, we clearly understand and document the expected data exchange and frequency, we perform system integration testing directly with each external entity that will be submitting data to us before the go-live date, and employ balance, control and alerting in our systems when the data exchange occurs. In this way, we can identify, alert, and correct the issue or apply an appropriate workaround solution to enable the data to be used as intended.
Changing implementation schedules (i.e., go-live or contract execution date)	While at times unavoidable, implementation delays can be costly for both health plans and state agencies. We mitigate this risk by acknowledging and understanding the need for the change, communicating and jointly modifying plans, and putting those new plans into action. Due to our national presence and size, we will scale and reassign resources as needed to meet and exceed tight implementation schedule changes.

In every Medicaid state we serve, MIS risk mitigation starts with making sure everyone on our implementation and MIS team serving the state understands the state's expectations, goals and contract requirements. For Kentucky, our teams have studied these items and they have not found a substantial list of concerns at this stage. As the teams carry out the implementation and readiness activities, they deploy a series of project management exercises, including systems testing during the readiness review cycle, to address and resolve any identified issues relating to systems installment and functionality.

Implementing New Systems and Making Changes to Existing Systems

We are leveraging an existing system that we use in our Medicaid managed care plans as the core system for this project. As such, the system will require minimal customization and will be configured as needed for specific Kentucky rules that are not already present in the core business rules. After we complete requirements validation with DMS, we will follow our standard change management process for configuration of the system and any development required.

For any changes to our proposed solution for Kentucky, based upon requirements validation efforts, we will employ an industry standard approach to MIS change management, known as IT Service Management (ITSM) model. This model continuously improves IT services to our customers and simplifies customer interactions with IT using processes, tools, metrics and reporting. UnitedHealth Group's ITSM model is based upon the Information Technology Infrastructure Library. Our incident and problem management processes are part of our ITSM framework. Systems and applications that we will implement receive continuous monitoring and support to proactively identify and address issues, such as interfaces and batch processes, or internal hardware and software system issues. Our operations teams provide 24 hours a day, 365 days a year onsite support and monitoring of system consoles and batch cycles to make sure critical system availability and expected service levels are met.

c. Describe the Vendor's current and planned use and support of new and existing technology in health information exchange (HIE), electronic health records (EHR), and personal health records (PHR).

As described in detail in our response to Section C.8, we will support and connect to strategic health information exchanges (HIEs) such as the Kentucky Health Information Exchange (KHIE). After hearing and meeting with Andrew Bledsoe, Kayla Rose and others from his staff, we look forward to partnering to help the Commonwealth meet its KHIE goals to "Hardwire the Triple Aim: Better Healthcare, Better Health and Reduced Costs." We generally require HIE vendors we work with to be HITRUST certified. If the HIE vendor does not have HITRUST certification; our security professionals will work through our multipage security checklist to verify the HIE vendor has appropriate security safeguards in place. Periodically, we will revisit and update this checklist with the HIE to confirm their continued adherence to our security requirements and policies.

Supporting Expanded Use of Electronic Health Records (EHR)

We are investing in our Point of Care Assist™ by integrating directly into a provider's electronic medical record system. Point of Care Assist™ is also our tool for integrating directly with EHR vendors. It will allow providers to get information such as real-time patient eligibility and enrollment at the point of appointment scheduling, enabling real-time chart exchange at the time of encounter, and reducing or eliminating chart requests and real-time gaps in care information. In Kentucky, we will introduce health systems that have not yet adopted the use of EHRs to UnitedHealthcare's vendors. While we are not a party to agreements between physician groups and EHR vendors, these vendors can bring our real-time data to physicians who engage with UnitedHealthcare vendors.

Point of Care Assist's Nationwide Reach

Several large national vendors, such as Cerner and Epic onsite platforms, can now supply more real-time information to providers. Our Point of Care Assist™ tool integrates with these vendors, which help patients achieve better clinical results.

Supporting Expanded Use of the Enrollee's Personal Health Record (PHR)

Our Integrated Health Record (IHR) tool is central to delivering a user-friendly and meaningful PHR for provider use in achieving quality and cost-efficient patient care. The IHR is a

patented, dynamic, easy-to-use longitudinal accounting of each individual's historical and current health status. It offers patients and clinicians secure access to personalized health information through a desktop or mobile application. The centerpiece of the IHR from a provider's perspective is the Patient Summary, which acts as a dashboard of patient information. The IHR aggregates data sourced from medical claims, laboratory results, pharmacy benefit management systems, electronic medical records, health information exchanges and other sources to create an organized clinical record centered on the individual and is available when needed most — at the time-of-care. The IHR tool is designed to assist providers in proactively managing care before the enrollee's health status deteriorates and requires intense care management and costly interventions. The same health record used by providers is available to the enrollee in an understandable format. The appearances may be very different, but the presentations are based upon the same record and rules, and form the same "system of care," for the individual.

We are also actively involved with CMS's efforts to advance interoperability in conformance with the Office of the National Coordinator for Health IT (ONC) Proposed Rule designed to facilitate the essential exchange of health care clinical data and end information blocking. Empowering consumers with access to health care information and improving care coordination is one of our main goals. Once the rule is finalized, we will partner with DMS to implement the required changes to enable the exchange of information and end information blocking.

d. Describe the Vendor's approach to assessing integrity, accuracy, and completeness of data submitted by providers and Subcontractors.

The vast majority of data we receive from providers and subcontractors is either claims or claims related (e.g., prior authorization, enrollment, billing codes, other coverage, participation status, encounter data). This data can affect the integrity and accuracy of information fed into downstream systems. Therefore, we thoroughly test, quality check and validate the **integrity, accuracy and completeness** of the data we receive from providers, subcontractors and other external entities before it is loaded into our systems. Wherever we connect interfaces between subsystems, applications and platforms, we implement triggers and controls to monitor the interfaces for the end-user, job (or web service) success, record counts extracted and loaded, fallout to error reports or work queues, and a variety of other data uses and applications for day-to-day operations. Except for interfaces to analytical stores and tools, interfaces are typically daily batch files or real-time services. Interfaces are required to include and evaluate file balances and control totals, and to send response files to ensure data is received and loaded. We perform additional validations after the data has been loaded into our systems, such as CSP claims editing, to confirm accurate, complete claims and manual data validations.

To assess the integrity of claims data received, we apply data validations and edits to verify all HIPAA 837 required fields are present and in the correct format and meet the Commonwealth's claims and encounter submission requirements. Claims passing the standard edits and validations enter the claims processing system for adjudication and payment. We submit all claims that pass these validations to our encounter processing system for final preparation for submission to the Commonwealth. Claims that do not pass the validations receive an error submitted flag on the finalized claim tables, and the error reason is written to an error table for research and inclusion in future submissions. We evaluate adjusted claims to determine the status of the original claim. Appropriate action is taken to either hold the encounter for a response or submit the encounter as a void or replacement, based upon the adjusted claim's status,

We assess the integrity of encounter data using our NEMIS encounter data submission and reporting system, which performs automated edits and validations to confirm the accuracy and completeness of encounter data using processed claims data from CSP and our subcontractors.

NEMIS edits can mirror DMS's edits. We apply additional edits to our encounters prior to submission to the Commonwealth. The edits and processes will confirm that our data meets integrity, accuracy and completeness checks in use by DMS for encounter processing.

Other data integrity checks we perform include validations such as credentialing checks to confirm accurate provider and contract data; data validations that identify enrollment data or load errors; and HIPAA compliancy checks for claims data received from the clearing house.

e. Provide a description of the Vendor's data security approach and how the Vendor will comply with Health Insurance Portability and Accountability Act (HIPAA) standards including the protection of data in motion and at rest, staff training and security audits.

All of our MIS systems have been built around data security and HIPAA privacy rules, regulations and standards. We manage our MIS systems on a real-time, continual 24-hour basis to confirm ongoing data security and compliance with HIPAA standards. In our security approach to protecting data in motion and at rest, our Medicaid health plan security and privacy team works with UnitedHealth Group's Enterprise Resiliency & Response (ER&R) group to deploy response mechanisms as soon as we detect an event that may disrupt our systems or indicate a data security threat. Within minutes of identifying risk or threat, we open a bridge line for technical leads to discuss what is happening, understand how it will affect our customers and stakeholders, determine what options are available for responding and set recovery priorities.

To manage our MIS system in Kentucky, and to confirm compliance with MIS-related requirements in the Contract, we will employ a Kentucky-based MIS director who will report any security breach in the system to the Commonwealth within the time frame established. The Commonwealth will have direct access to the incident response team via a toll-free number staffed in the United States 24 hours a day, seven days a week. Additionally, DMS will have the personal mobile and office numbers of the information security officers for direct contact.

UnitedHealthcare's Data Security Approach

We operate a comprehensive data protection framework to protect customer data. This framework includes applied technology, security operations and services that reduce the risk of data breaches for all health plans owned and operated by UnitedHealth Group, including UnitedHealthcare. We use many network, security monitoring and encryption technologies to protect our environment and maintain the confidentiality and integrity of our data, and routinely test and validate our systems' security. Across UnitedHealth Group, we employ more than 1,000 security professionals dedicated to protecting and securing data entrusted to us. We expect our standards, frameworks, policies and practices will be well aligned to the Commonwealth. Still we operate in a shared commercial environment; we follow our policies, so some exceptions are expected for sensitive and proprietary concerns, such as sharing detailed reporting of vulnerabilities, Commonwealth approval of security assessments and strategies, detailed artifacts related to the Software Development Life Cycle and so forth. We welcome the opportunity to review our standards, policies and practices with the Commonwealth.

To protect its health plans against data security breaches while also complying with HIPAA rules, regulations and standards, UnitedHealth Group uses frameworks from two organizations. Leidos, which provides a cyber defense framework and the Health Information Trust Alliance (HITRUST), which provides a health-industry risk management framework:

- ***Leidos:*** The Leidos Intelligence Driven Defense® framework is used to guide and benchmark our cyber defense program. Our current cyber defense rating is among the top three of 133 companies assessed by Leidos. We are rated well above the health care industry and Fortune 500 company average scores.

- ***HITRUST:*** HITRUST provides a security-management maturity score using a Prisma process. We score well above health-industry certification requirements. This certification provides evidence of our compliance with federal health care requirements, including HIPAA and HITECH. Furthermore, HITRUST is supported by the U.S. government as the implementation guidance for the NIST (National Institute of Standards and Technology) Cybersecurity Framework for the health/public sector. HITRUST is also aligned to validate the inclusion of additional industry controls such as ISO, NY Cyber Regulation, other state and federal regulations, and international standards. This framework provides the Commonwealth with the assurance that we meet our regulatory expectations and practices recommended to defend our data against cyber risks. We apply the HITRUST framework and applicable standards to our internal programs and our external vendors.

Our data loss prevention program encompasses both data in motion and endpoint data at rest.

- ***Data in Motion:*** We actively scan web and email data leaving the UnitedHealth Group network. The automated scan uses techniques and rules to scan for content based upon requirements for HIPAA, Gramm-Leach-Bliley, Payment Card Industry Standards, confidential/proprietary information and other data protection requirements. If the scan identifies content that matches a rule, we block the content from leaving our network, and we notify the sender of the block. We monitor blocked events for certain signatures and patterns to identify activities that may be outside of normal business activity.
- ***Endpoint Data at Rest:*** We scan workstations using similar rules and techniques as described for data in motion scanning. This process focuses on individual workstations to scan, flag and present the workstation owner with files that require remediation. The flagged content is reviewed for certain signatures and patterns that may be outside of normal business activity. The workstation owner remediates the identified files, and progress is tracked until all files have been remediated. If our program recognizes suspected abnormal business activity, we escalate the issue for investigation, and then to our security incident response team if support is necessary to resolve the event. In nearly all cases, the issue is resolved simply through user education.

The systems and applications where we hold the Commonwealth's Medicaid plan data entrusted to us have employee role-based access controls that prevent unauthorized users from accessing the data. Furthermore, any use of any Commonwealth's Medicaid data is strictly limited to proper uses and disclosures permitted by applicable law, our contract, our policies and procedures, and, as appropriate, at the explicit direction of DMS. As such, we can assure our Kentucky Medicaid enrollees with confidence that their data will only be used properly and will be treated with the utmost confidentiality and security.

Staff Training Regarding Data Security and HIPAA Compliance

All employees, contractors and subcontractors are required to comply with HIPAA rules and regulations and to report privacy and security breaches, whether it involves one or thousands of individuals. All employees receive training upon hire and at least annually thereafter regarding our policies, processes, and company resources specific to HIPAA compliance, data security and data privacy. Training includes how to spot security risks, how to protect, receive and share data securely, when and how to report data risks or breaches, and the responsible handling and protection of personally identifiable information (PII) and protected health information (PHI). Our privacy office provides overall direction for enterprisewide privacy-compliance activities, including the oversight of formal administrative functions per the HIPAA Privacy Rule, compliance requirements from Commonwealth laws and regulations, data protection and

privacy incident management across the company, including the Commonwealth and its subcontractors.

UnitedHealthcare's Approach to Data Security Audits

We conduct risk assessments annually and monitor risk mitigation activities throughout the year. These risk assessments and activities help determine our data security audit approach. Our enterprise risk management (ERM) team creates an annual business segment, platform and enterprise risk profiles. The ERM works with the leadership in each business and major corporate function to assess risk. Based upon the annual risk assessment and management requests, ERM performs detailed risk assessments for the businesses to identify where risk is present in major initiatives, projects, change events and other business activities. UnitedHealth Group discloses material risk factors in the annual 10K statement.

We will implement Kentucky's Medicaid managed care program on our shared common platforms — the same systems we use to run Medicaid and D-SNP plans in 31 states. These shared resources provide our organization economies of scale, enabling us to implement best practices and policies across our enterprise.

Security Audits and Risk Assessment Program

Our Information Security Risk Management and Privacy Program align with NIST 800-37 Risk Management Framework requirements. We use the risk management framework to make risk-informed decisions through structured reviews of information security risks. Policies are based upon industry best practices such as NIST 800-37, HITRUST and applicable and appropriate state and federal regulatory obligations. We welcome the opportunity to review our standards, policies, frameworks and practices (which align with HITRUST) with the Commonwealth. Our frameworks and those of the Commonwealth's will be well aligned. We also consider the U.S. Department of Health & Human Services, Office of Civil Rights, and Office of eHealth Standards & Services, Department of Insurance, Federal Trade Commission, State attorneys general, International Implications (EU 95/46EC), CMS and others. The Information Security Risk Management and Privacy programs provide input to the ERM program. The ER&R program manages the process of identifying and managing risks associated with natural and fabricated threats. These programs will work directly with our Kentucky-based MIS director and the Commonwealth.

f. Describe any proposed system changes or enhancements that the Vendor is contemplating making during the anticipated Contract Term, including subcontracting all or part of the system. Describe how the Vendor will ensure operations are not disrupted.

We plan to make system changes or enhancements to our core platform during the term of the contract. We maintain short- and long-term systems and capability roadmaps that align with business needs. For example, our CSP core claims platform is scheduled to be updated twice per year when releases are made available from our software vendor. We maintain this upgrade schedule to take advantage of any new enhancements while ensuring we remain on supported software versions.

Systems Enhancements in Progress

We are also simplifying, modernizing and transforming our provider subsystems over the life of the contract. We are automating provider onboarding, digitizing workflows, eliminating paper processes, automating transactions, and moving toward near-real-time interfaces in the next few years. We are modernizing our claims subsystems to move away from scheduled processes to real-time interfaces. We are investing in machine learning to improve our

adjudication rates, deploying chatbots to assist our member service advocates, and accelerating our prior authorization processes. As CMS's interoperability rules are placed into operation, we are modernizing our clinical subsystems to support real-time information exchange both internally and externally. We will continue to advance and invest in new technologies as they become available.

Our teams are adopting the United Scalable Agile Methodology (USAM), while other teams will continue to use the sequential design process of the Waterfall Methodology. The USAM methodology is built on Agile principles and values that provide a streamlined software delivery framework. The USAM is a scalable, lean, metrics-driven approach that fosters faster software deployment.

Ensuring Continuous Operations during Systems Enhancements

With any systems upgrade or enhancement, our IT teams take great care to schedule the enhancement to occur during times that will have the least effect on enrollees, providers, staff and other system users. Regardless of the software development methods used, our systems analysts, business analysts, product owners and plan executives consider HIPAA regulations, the Commonwealth's requirements and the effect to users, when reviewing changes, enhancements and upgrades to systems. Our Software Change Management Policy and Procedure governs all changes. We demonstrate compliance with this policy by our HITRUST certification and during annual internal audits based upon regulatory requirements.

As we identify externally and internally driven system changes, we have the full support of local and national resources to respond to the Commonwealth's needs proactively. We will partner with DMS on emerging system changes through our change management process and throughout implementation in collaboration with the Commonwealth's MIS team.

All changes to UnitedHealth Group's environment follow our Change Management Policies and Procedures to validate that standardized methods and procedures are used to handle all changes efficiently and promptly. Changes to an application or the infrastructure include clear requirements, a back-out plan, appropriate test plans and IT owner approval. We apply industry best practices to confirm any system changes are free from defects.

Release Cycles

UnitedHealth Group continuously upgrades and enhances its systems. Comprehensive enhancements deploy on a monthly or quarterly schedule, coordinated across platforms as needed. We schedule change windows to avoid impact on enrollees, providers and other system users. The change management team works with system stakeholders and the operations team to determine release timing and change windows when there will be minimal and ideally no effect on system availability. We communicate any change that may result in enrollee or customer impact through appropriate customer contacts and they will adhere to the notification requirements.

This Page Intentionally Left Blank