Oregon All Payer All Claims (APAC) Program

Application for Limited Data Files

APAC-3

This application is used to request limited data sets. If you would like to discuss APAC data in relation to your project prior to submitting this application, please contact apac.admin@odhsoha.oregon.gov with a brief description of the project and your contact information. OHA will have someone contact you to help determine if APAC is appropriate for your project and, if so, which data elements may be needed.

PROJECT INFORMATION

Project Title: An Examination of Competition and Access to Healthcare Services in the Portland Area

Principal Investigator: Subramaniam Ramanarayanan

Title of Principal Investigator: Senior Managing Director

Organization: NERA Economic Consulting ("NERA")

Address: 1166 Avenue of the Americas

City: New York State: NY Zip Code: 10036

Telephone: 1-212-345-0745

Email: subbu.ramanarayanan@nera.com

SECTION 1: PROJECT SUMMARY

1.1 Project Purpose: Briefly describe the purpose of the project. You may submit a separate document that details the project's background, methodology and analytic plan in support of your request for APAC data elements.

Please refer to the attached document ("APAC-3 application additional responses_NERA submission.pdf") for our complete responses.

1.2 Research Questions: What are the project's key research questions or hypotheses? If this project is research and has been approved by an Institutional Review Board (IRB), the research questions must align with the IRB approval documentation. If needed, a more detailed response may be submitted as a separate file.

- Note: APAC staff will use your response to this question to determine the minimum data elements necessary for this project, in accordance with the HIPAA minimum necessary standard. The research questions should be specific enough to justify the need for each data element beyond identifying it as a "potential confounding variable."

As described above, OHSU and Legacy filed a Notice of Material Change Transaction on September 26, 2024, and OHA is currently reviewing the transaction in the Comprehensive Review phase under the HCMO Analytic Framework. To the extent OHA relies on APAC data in its review, and asks questions of the Parties based on its review of that data, the Parties need access to the APAC data to be able to respond. The Parties are requesting access to the data through their agent NERA, the economic consulting firm the Parties have retained to perform any analyses of the APAC data that might later be demanded by OHA.

Please refer to the completed Data Elements Workbook submitted along with this application for the full list of data tables and fields that NERA is requesting, along with justification for each requested field.

1.3 Products or Reports: Describe the intended product or report that will be derived from the requested data and how this product will be used. If needed, a more detailed response may be submitted as a separate document with this application.

Please refer to the attached document ("APAC-3 application additional responses_NERA submission.pdf") for our complete responses.

1.4 Project Timeline: What is the timeline for the project?

Anticipated Start Date:

Anticipated Publication/Product Release Date:

Anticipated End Date:

Please refer to the attached document ("APAC-3 application additional responses_NERA submission.pdf") for our complete responses.

1.5 Data files may not be released or reused beyond the terms of the data use agreement resulting from this application regardless of funding source or other obligations of the principal investigator, organization or research team.

☒ I understand this limitation and agree that data files or work products will not be shared at less than an aggregated, de-identified level.

☐ I understand this limitation and request approval to share data files or work products at a potentially re-identifiable level as follows:

SECTION 2: PROJECT STAFF

2.1 Project Staff: Please list all individuals in addition to the principal investigator who will have direct or indirect access to the data. This must include any contractors or other third parties with access to the data.

Name: Yin Wei Soon Email: yinwei.soon@nera.com	Project role: Consultant
Name: Ian Pasinato Email: ian.pasinato@nera.com	Project role: Consultant
Name: Mirha Khan Email: mirha.khan@nera.com	Project role: Senior Analyst
Name: Samuel Cooley Email: samuel.cooley@nera.com	Project role: Senior Analyst
Name: Kayla Hreczuck Email: kayla.hreczuck@nera.com	Project role: Analyst
Name: Lauren Leonard Email: lauren.leonard@nera.com	Project role: Analyst
Name: Maroun Mezher Email: maroun.mezher@nera.com	Project role: Associate Analyst

Attach additional sheets as needed. (Please refer to the attached document for additional project staff.)

2.2 Technical Staff: Please list any additional staff who will be maintaining the data file(s) or otherwise assisting in the transfer or receipt of the data files. Files will not be transferred to anyone who is not listed on this application as either project staff or technical staff.

Name: Madawa Hewage Email: madawa.hewage@nera.com	Technical role: Systems Engineer
Name: Omasanjuwa Ofuya Email: omasanjuwa.ofuya@nera.com	Technical role: Computer Support Specialist

Attach additional sheets as needed.

SECTION 3: DATA REQUEST

3.1 Purpose of the Data Request:

a. Listed below are the purposes for which OHA may share APAC data. Please choose the category in which your project falls under (***choose only one***).

- ☐ Research (refer to 45 CFR 164.501 for definition)
- ☐ Public health activities as defined in 45 CFR 164.512(b) by the state or local public health authority
- ☒ Health care operations as defined in 45 CFR 164.501
  - Covered entity as defined in 45 CFR 160.103? ☐ Yes ☒ No
- ☐ Treatment of patient by health care provider as defined in 45 CFR 164.506 (c)(2)
  - Covered entity? ☐ Yes ☐ No
- ☐ Payment activities performed by covered entity or health care provider as defined in 45 CFR 164.506 (c)(3)
  - Covered entity? ☐ Yes ☐ No
- ☐ Work done on OHA's behalf by a Business Associate as defined in 45 CFR 160.103

b. Describe how the project falls into the category chosen above.

Planning for, managing, and general administrative activities such as responding to government inquiries about a Material Change Transaction fit squarely within the explicit definition of "Health care operations" under 45 CFR 164.501. Here, OHSU and Legacy filed a Notice of Material Change Transaction on September 26, 2024, and OHA issued its Preliminary Report and began its Comprehensive Review on November 4, 2024 and is currently reviewing the transaction under the HCMO Analytic Framework. OHA will rely on APAC data in its review, and to the extent it asks questions of the Parties based on its review of that data, the Parties need access to the APAC data to be able to respond. The Parties are requesting access to the data through their agent NERA, the economic consulting firm the Parties have retained to perform any analyses of the APAC data that might later be demanded of them by OHA.

3.2 Direct identifiers. What level of data identifiers are you requesting (***choose only one***)? Reference the Data Elements Workbook for the categorization of data elements.

- ☐ De-identified (as outlined in 45 CFR 164.514(e)) protected health information
- ☒ Limited, potentially re-identifiable data elements
- ☐ Restricted direct identifiers (member name, address, date of birth, etc.) *Please note:* Direct identifiers are only released under special circumstances that comply with HIPAA requirements, and will require specific approvals, such as IRB approval, patient consent and/or review by the Oregon Department of Justice.

3.3 Human Subjects Research: IRB protocol and approval are required for most research requests for limited data elements. Not obtaining IRB approval or waiver in advance may delay approval of the data request. **The research questions reported in 1.2 of this application must match the documentation supporting the IRB approval received or the IRB approval will not be accepted for this data application.**

The IRB application should indicate that APAC data contains sensitive personal health information and is subject to HIPAA regulations.

a. Does the project have IRB approval for human subjects research or a finding that approval is not required?

☐ Yes ☒ No

If no, briefly explain why you believe that this project does not require IRB review.

NERA is requesting the minimum justifiable set of APAC data elements OHA may use in its evaluation and, as noted earlier, NERA will share only aggregated findings. The vast majority of the data elements that NERA is requesting are de-identified. For the remaining data elements that are marked "sensitive," NERA is only requesting those OHA might use under the HCMO Analytical Framework.

If an IRB reviewed the project, include the IRB application and approval/finding memo with the submission of this APAC-3 and complete parts b-e below.

☐ IRB application and approval memo are attached.

b. Describe how this application is within the authority of the approving IRB.

N/A

c. Describe why the project could not be practicably conducted without a waiver of individual authorization (a waiver of individual authorization is provided by the IRB in cases in which the researcher does not need written authorization from participants to use their PHI):

N/A

d. On what date does the IRB approval expire? N/A

SECTION 4: DATA ELEMENTS

4.1 Narrowing Data Needs: Refer to the APAC Data Dictionary for detailed information about the data elements. In compliance with HIPAA regulations, you will only receive data elements that are adequately justified. This means APAC will only provide the minimum necessary data required for the project as represented in the research questions, protocol and IRB approval.

a. What years of data are requested? 2011 through 2022 are currently available.

2011 - 2022

b. What payer types are requested? Check all that apply

☑ Commercial ☑ Medicaid ☑ Medicare Advantage

c. What types of medical claims are requested? ☐ All

☑ Inpatient hospital ☑ Emergency department ☑ Outpatient
☑ Ambulatory surgery ☐ Ambulance ☐ Transportation
☐ Hospice ☐ Skilled Nursing Facility ☑ Professional

d. Demographic data limitations

1. Gender ■ All ☐ Male ☐ Female

2. Age ■ All ☐ Only 65+ ☐ Only 18 and younger ☐ Other (Specify age range)

e. Will data requested be limited by diagnoses, procedures or type of pharmaceutical? Add additional sheet if needed.

Diagnoses, indicate ICD 9 and ICD10 codes to include:

N/A

Procedures, indicate CPT to include:

N/A

Pharmaceuticals, indicate NDC or therapeutic classes to include:

N/A

f. APAC has a small number of out-of-state residents included, most often through PEBB or OEBB coverage. Do you want to include out-of-state residents? ■ Yes ☐ No

4.2 Data Element Workbook: Complete the Data Element Workbook to identify specific data requested.

Data Element Workbook completed and attached, including justifications for each element requested. ☑

SECTION 5: DATA MANAGEMENT & SECURITY

5.1 Data Reporting: APAC data or findings may not be disclosed in a way that can be used to re-identify an individual. Data with small numbers – defined as values of 30 or less (n≤30) or subpopulations of 50 or fewer individuals (n≤50) – cannot be displayed in findings or outputs derived from APAC data. Please describe the techniques you will use to prevent re-identification when findings or outputs result in small numbers or subgroups (e.g. aggregation, cell suppression, generalization, or perturbation).

As stated in Section 1.3, NERA will only share data or findings at an aggregate level. In no circumstance will NERA list any information pertaining to specific patients, inpatient discharges, or outpatient visits. Should any data summaries be reported at the cell level, NERA will abide by standards used by CMS and academics in analyzing health care data by masking statistics for cells with small sizes, i.e. those with 10 or fewer observations.

5.2 Data Linkage: OHA seeks to ensure that APAC data cannot be re-identified if it is linked or combined with data from other sources at the record, individual or address level. Requesters are strongly encouraged to consult with APAC staff regarding linking APAC data with other data prior to submitting a data request. Health Analytics prefers to conduct APAC data linking in-house and share only encrypted identifiers with data requesters.

a. Does this project require linking to another data source?

☐ Yes ■ No

If yes, please complete parts b-d below.

b. At what level will data be linked?

☐ Address ☐ Facility ☐ Individual person/member
☐ Individual provider

c. If required to link

☐ Authorized to provide data for linking at OHA
☐ Not authorized to provide data for linking at OHA
☐ Unknown

d. Describe and justify all necessary linkages, including the key fields in each data set, how they will be linked, the software proposed to perform the linkage and why it is necessary.

N/A

e. Describe in detail the steps will you take to prevent re-identification of linked data.

N/A

5.3 Data Security (required for all applications):

a. Attach a detailed description of your plans to manage security of the APAC data including:
   - Designation of a single individual as the custodian of APAC data, either the principal investigator or staff listed in Section 2 of this application, who is responsible for oversight of APAC data, including reporting any breaches to OHA and ensuring the data are properly destroyed upon project completion.
   - A security risk management plan applicable to APAC data that includes:
     - Secure storage in any and all mediums (e.g., electronic or hard copy)
     - Procedures to restrict APAC data access to only those individuals listed on the data use agreement
     - User account controls, i.e., password protections, maximum failed login attempts, lockout periods after idle time, user audit logs, etc.
     - Confirmation of training for personnel on how to properly manage protected health information in all formats
     - Protection of derivatives of APAC data at the re-identifiable level
     - If applicable, procedures for handling direct identifiers, such as allowing access on a 'need to know' basis only and minimizing risk by storing identifiers separately from other APAC data
     - Procedures for identifying, reporting and remedying any data breach
   - Statement of compliance with HIPAA and the HITECH Act
   - Electronic device protections, i.e., anti-virus or anti-malware software, firewalls, and network encryption

b. Record level or derivative data that can be re-identified must be destroyed within 30 days of the end of the data use agreement, in a manner that renders it unusable, unreadable or indecipherable. What are your plans for destruction of the dataset and any potentially identifiable elements of the data once the data use agreement has expired?

NERA maintains hardware asset management policies and procedures that require secure disposal of IT assets using industry standard methods: for example, electronic media, such as system hard drives, are sanitized before disposal using a multi-pass, random character overwriting procedure; other electronic media and portable devices may be physically destroyed through shredding, pulverizing, or secure wiping prior to disposal.

Please refer to the attached document titled "2024 MMC Information and Cyber Security Program_NERA submission.pdf" for more information.

SECTION 6: COST OF DATA

Because each data set is unique, cost can be determined only after the specific data elements are finalized. APAC staff will then review your request and estimate the number of hours required to produce and validate the data. APAC requires reimbursement for the cost of file transfer ($890 per request) and the total time spent by APAC staff on research and administrative activities. Payment must be received before the data will be provided. APAC staff will provide an invoice to facilitate payment. OHA's W-9 is available on request.

SECTION 7: CHECKLIST AND SIGNATURE

7.1 Checklist: Please indicate that the following are completed:

- ☒ I acknowledge that payment will not be refunded if OHA fulfills the data request, but the receiving entity does not have the capability to import or analyze the data
- ☒ All questions are answered completely
- ☒ Data Element Workbook is attached to email or printed application
- ☐ IRB application with approval/finding memo is attached to email or printed application, if applicable
- ☒ Data privacy and security policies for the requesting organization, and any third-party organizations, are attached to the email or printed application

7.2 Optional Racial Justice Addendum: Please see the last two pages of this form for options if data will be used to eliminate racial injustice.

- ☐ I am interested in this option
- ☒ This option does not apply to my data request

7.3 Signature: The individual signing below has the authority to complete this application and sign on behalf of the organization identified in Section 1. By signing below, the individual attests that all information contained within this data Request Application is true and correct.

Signature Ramanarayanan, Subramaniam Digitally signed by Ramanarayanan, Subramaniam Date: 2024.11.18 22:06:01 -05'00' Date 11/18/2024

Printed name Subramaniam Ramanarayanan

Title Senior Managing Director

Return the completed form with required attachments to APAC.Admin@odhsoha.oregon.gov.

Additional Responses

Oregon All Payer All Claims Program Application for Limited Data Files

Project Title: An Examination of Competition and Access to Healthcare Services in the Portland Area

1.1 Project Purpose: Briefly describe the purpose of the project. You may submit a separate document that details the project's background, methodology and analytic plan in support of your request for APAC data elements.

On September 26, 2024, Oregon Health & Science University ("OHSU") and Legacy Health System ("Legacy") (collectively "the Parties") filed a Notice of Material Change Transaction with the Oregon Health Authority (OHA) as required by Oregon Revised Statute ("ORS") 415.501. OHA is reviewing the transaction under the Health Care Market Oversight (HCMO) program and Analytic Framework.[1] On November 4, 2024, OHA issued its Preliminary Report and determined that the transaction will undergo a comprehensive review under OAR 409-070-0060.[2]

As outlined in the Preliminary Report, OHA will use the Oregon All Payer All Claims (APAC) dataset, among other data, during its Comprehensive Review.[3] OHA indicated that "additional analyses are required to determine the proposed transaction's impact on the market share."[4] OHA also stated that "during the comprehensive review, OHA will conduct additional analyses to better understand the potential impacts of OHSU's increased market share on health care costs, access, quality and equity."[5] These additional analyses of market share will require OHSU and OHA to analyze the APAC dataset as outlined in the "Health Care Market Oversight Analytic Framework" attached as Exhibit 1 with this application.

The Parties anticipate that OHA may request that the Parties respond to and conduct APAC based analyses in connection with the HCMO review. The Parties have retained NERA Economic Consulting (NERA) to perform any APAC based analyses demanded of them by OHA during the HCMO process. For that reason, NERA is submitting this application on behalf of OHSU and Legacy to ensure the Parties have timely access to the APAC data necessary to respond as may be required by OHA.

---

[1] See https://www.oregon.gov/oha/HPA/HP/Pages/039-OHSU-Legacy.aspx.

[2] See https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/039-OHSU-Legacy-Determination.pdf

[3] See https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/039-Preliminary-Report.pdf at 32; *see also* Table 1 in OHA, "Health Care Market Oversight Analytic Framework," October 2022, available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/OHA-HCMO-Analytic-Framework-FINAL.pdf (accessed November 5, 2024).

[4] See https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/039-Preliminary-Report.pdf at 25.

[5] See https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/039-Preliminary-Report.pdf at 28.

1.3 Products or Reports: Describe the intended product or report that will be derived from the requested data and how this product will be used. If needed, a more detailed response may be submitted as a separate document with this application.

As described above, the requested APAC data will be used only in connection with OHA's evaluation under the HCMO program of the Material Change Transaction notice filed by OHSU and Legacy on September 26, 2024, and the Parties retained NERA to perform any APAC data analyses demanded of them by OHA during the HCMO process.

Any report generated by NERA based on the APAC data will be treated as confidential work product, with strictly limited circulation for the sole purpose of communicating findings as required by OHA. Crucially, NERA will only present the analyses and results at an aggregate level, i.e. in no circumstance will NERA list any information pertaining to specific patients, inpatient discharges, or outpatient visits. Should any data summaries be reported at the cell level, NERA will abide by standards common in analyzing health care data by masking information for cells with small sizes, e.g. those with 10 or fewer observations.

Furthermore, to the extent NERA produces reports or summaries and analyses of APAC data to support the merging Parties in responding to questions by OHA in the HCMO review process, NERA will only do so consistent with all applicable confidentiality laws. More specifically, those materials will be designated "Confidential" under Oregon Administrative Rule 409-070-0070 and ORS 415.501(13), and therefore only be reviewed by OHA, unless OHA, after consultation with the Parties, determines that certain summary material is not "confidential" and can be disclosed in a "Public" version.

1.4 Project Timeline: What is the timeline for the project?

Anticipated Start Date: Immediately. OHA issued a determination to move to comprehensive review on November 4, 2024 and has sent its first batch of questions to the Parties.

Anticipated Publication/Product Release Date: None. The Parties do not anticipate the data or project will be Published or Publicly Released unless ordered by OHA.

Anticipated End Date: Dependent on OHA's review. The proposed effective date of the transaction is March 30, 2025. The comprehensive review lasts 180 days from the date OHA accepted a completed application (October 4, 2024) unless otherwise extended or tolled.

2.1 Project Staff: Please list all individuals in addition to the principal investigator who will have direct or indirect access to the data. This must include any contractors or other third parties with access to the data.

(Additional project staff, continued from the main application form.)

Name	Email	Project Role
Tomas Leonardo	Tomas.Leonardo@nera.com	Associate Analyst
Serena Chan	serena.chan@nera.com	Associate Analyst
Andrew Feng	andrew.feng@nera.com	Associate Analyst
Michael Tu	michael.tu@nera.com	Research Associate

Oregon All Payer All Claims Program Application for Limited Data Files

Project Title: An Examination of Competition and Access to Healthcare Services in the Portland Area

EXHIBIT 1

Health Care Market Oversight Analytic Framework

Overview

This framework describes the analytic approach of the Oregon Health Authority's Health Care Market Oversight program (HCMO) for conducting reviews of material change transactions pursuant to ORS 415.500 et seq. The framework is grounded in the goals, standards and criteria for transaction review and approval outlined in OAR 409-070-0000 through OAR 409-070-0085. This document outlines the analytic methods, performance measures, and sources of information HCMO expects to use for reviews of material change transactions.

This document provides the menu of potential analyses from which HCMO will choose in reviewing a particular material change transaction (hereafter, "transaction"). HCMO does not expect to complete every analysis described here for every transaction review. The specific facts of the proposed transaction, the availability of reliable data, and time constraints associated with preliminary and comprehensive review periods will affect the analyses included in HCMO's review of any given transaction. These considerations are further described in the section entitled "Application of the Framework." As the program matures, HCMO may update this framework as needed to reflect current practice, provide additional details on methodologies and measures, incorporate newly available data sources, and clarify implementation of the framework for specific transactions.

Contents

Please email hcmo.info@oha.oregon.gov with any questions regarding this document. You can get this document in other languages, large print, braille or a format you prefer free of charge. Contact us by email at hcmo.info@oha.oregon.gov or by phone at 503-385-5948. We accept all relay calls.

Nature of the Transaction and Characteristics of the Entities

Before starting the analysis, HCMO will review the Notice of Material Change Transaction form (hereafter, "notice") and proposed agreement or term sheet to extract key facts about the transaction, including:

Type of transaction: Merger, acquisition, affiliation (clinical, corporate, contracting), contract, partnership, joint venture, formation of Accountable Care Organization (ACO), parent organization, or management services organization.
Entities involved in the transaction: Type(s) of health care entities (hospital, health system, physician group, Coordinated Care Organization [CCO], insurer, etc.), service lines, facilities owned or operated, size (volume, revenue, capacity, employees), geographic area(s) of operation, patient demographics (including payer mix), existence of clinical or contracting affiliations, major contracting relationships, ownership/control of other businesses.
Ownership/governance/operational structure: Ownership type (public/private; for-profit/non-profit, LLC/corporate, etc.), governance, and operational structure of the parties to the transaction and any changes in ownership, governance, or operational structure resulting from the transaction.
Objectives: Rationale for the transaction; main benefits expected from the transaction.
Post-transaction plans: New investments, management or operational changes, including changes to services anticipated or planned to be implemented after the transaction closes.
Anticipated impact: Applicant's expectations for the impact of the transaction on access to affordable health care, health care cost growth, access to services in medically underserved areas, health inequities, and competition in health care markets.

If necessary, HCMO will consult with the Oregon Department of Justice (DOJ) on whether the transaction meets the criteria for a material change transaction under OAR 409-070-0005 through OAR 409-070-0025. For purposes of establishing these basic facts, HCMO may request supplementary information from the entities if the above information is not contained in the notice, proposed agreement, or term sheet.

Analytic Domains

HCMO analysis will focus on four domains: **cost, access**, **equity**, and **quality**. For each domain, HCMO will assess:

- The **current performance** of the entities involved in the transaction, based on relevant outcome metrics prior to the transaction. Current performance will be measured relative to performance of other comparable health care entities (see" Identifying Comparator Entities" for details on how comparator entities will be identified). When possible, multiple years of data will be used to assess current performance.
- The likely **impact of the transaction** on performance, given current performance, known details of the transaction, characteristics of the health care market(s) in which the entities operate, and the entities' goals and plans post-transaction. Impact analyses will seek to anticipate the entities' post-transaction performance and compare this to expected performance in the absence of the transaction. Focus will be on short-term (12-month) impacts of the transaction, although longer term impacts will also be considered. Impact analyses will be informed by academic research on the effects of similar transactions.

The Outcomes and Analysis section describes, for each domain, the key outcomes HCMO will assess and the methods HCMO may use to determine the likely impact of the transaction. Outcome metrics and analytic methods for a given transaction will depend on several factors, as described in the following section.

Application of the Framework

This section describes the main factors influencing the types of outcome measures and analyses HCMO will perform in reviewing a given transaction. These include the level of review (preliminary versus comprehensive), the characteristics of the entities, and the nature of the transaction.

Level of Review

Following a preliminary review, HCMO may determine that a comprehensive review is required if there are indications that the transaction may lead to significant adverse effects in any of the domains of cost, access, equity, or quality. (Please refer to HCMO sub-regulatory guidance: Criteria for Comprehensive Review of Material Change Transactions.[1]) Preliminary and comprehensive reviews may differ on multiple dimensions, including:

- **Quantitative analyses.** The number of outcome measures assessed, the level of granularity at which measures are calculated, the degree of adjustment of measures to account for provider- or population-specific factors, and the level of sophistication of statistical/econometric analyses.
- **Data sources.** The number of data sources used, reliance on confidential data and documents provided by the entities (subject to request), use of third-party proprietary databases.
- **Use of qualitative methods.** Qualitative analysis for preliminary reviews will be limited to review of publicly available documents, reporting, and any public comments submitted in response to the notice. Comprehensive reviews may include collection of qualitative information and in-depth analysis of documents obtained from the entities.

Table 1 provides an overview of HCMO analyses and data sources for preliminary and comprehensive reviews. The two left-hand columns list the data sources HCMO will use for preliminary reviews and the associated analyses. The two right-hand columns provide a menu of possible data sources and analyses for comprehensive reviews.

For current performance analysis during preliminary review, HCMO will examine a limited set of measures of cost, access, equity and quality using readily available administrative data (e.g., claims, hospital discharge data), existing reporting, and other publicly available information and documents. Additional information needed for preliminary analysis may be requested to supplement or clarify the contents of the notice, including details about the transacting entities, recent quantitative data, current policies and procedures, or narrative about patient and community engagement efforts. Please see Table 2 below for a list of supplemental items that may be requested during the preliminary review period.

For domains and outcomes identified as concerning during the preliminary review, HCMO will expand its analysis of current performance during comprehensive review by adding measures, using additional data sources for calculating measures, and calculating measures at a more granular level. For impact analysis, HCMO will generally employ more sophisticated statistical or econometric techniques during comprehensive review. To obtain additional data sources needed for more in-depth quantitative analysis, HCMO may request internal data from the entities or leverage third-party databases.

In addition to quantitative analyses, comprehensive reviews may include qualitative data collection and analyses, for example, input from community members as part of a Community Review Board (CRB), interviews with representatives of the entities and community groups, and review of internal documents requested from the entities relating to integration planning or quality improvement. (For more information on CRBs, please refer to HCMO sub-regulatory guidance: Criteria for Community Review Boards.[2])

[1] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/HCMO-Criteria-for-Comprehensive-Review.pdf.

[2] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/HCMO-Community-Review-Board-Criteria.pdf.

HCMO may retain outside advisors such as economists, accountants, actuaries, qualitative researchers, attorneys, and health care quality experts to carry out the more sophisticated and detailed analyses that may be required for a comprehensive review. HCMO does not expect to retain outside advisors for preliminary reviews, except on rare occasions where state agencies lack the necessary expertise. (Please refer to HCMO sub-regulatory guidance: Criteria for OHA Use of Outside Advisors for Material Change Transaction Review.[3])

Type of Entity

HCMO will review material change transactions involving any health care entity. Per OAR 409-070-0005, the types of entities meeting the definition of a "health care entity" include:

- Individual health professionals licensed or certified in Oregon.
- Hospitals.
- Health systems.
- Carriers offering a health benefit plan or Medicare Advantage plan.
- Coordinated care organizations.
- Other entities as defined in OAR 409-070-0005 (16)(f)-(g) and (17).[4]

The type(s) of entities engaging in the material change transaction will determine the measures HCMO uses to assess current performance and implementation of impact analyses in each domain. For example, in the access domain, measures of payer mix would be relevant for hospitals, health systems and physician groups. For carriers, HCMO would examine the size and composition of the provider network. In the cost domain, price, market share, and spending measures would be defined differently depending on the types of services offered by the entity.

Nature of the Transaction

HCMO's analytic approach will also differ based on the type of transaction (e.g., merger, acquisition, affiliation, partnership, joint venture, etc.) and the specific facts of the transaction (e.g., the associated change in ownership, governance, management, or operational structure). In addition to being relevant for the choice of analyses, these factors may affect the domains of focus (e.g., cost, access, quality, or equity) for impact analyses. For example, a contracting affiliation in which there are no changes in management or operations of either entity would be less likely to have implications for access than an acquisition in which the entities plan to integrate management and operations.

[3] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/HCMO-Outside-Advisors.pdf.

[4] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/HCMO-Entities-Subject-to-Review.pdf.

Table 1: Summary of Analyses and Data Sources for Transaction Reviews

	PRELIMINARY REVIEW		COMPREHENSIVE REVIEW	
Domain	**Data Sources**	**Analyses**	**Potential Additional Data Sources**	**Potential Additional Analyses**
Cost	- All Payer All Claims (APAC) data - Hospital discharge data - Audited financial statements - CCO/Hospital financial reporting - Cost growth target data - DCBS health insurer data - Publicly available data on hospital/health system characteristics (e.g., CMS, AHRQ) - Other information provided in notice	- Nature of the transaction - Characteristics of the entities (including entity ownerships and structure) - Market share/Market concentration analysis - Financial analysis (solvency, profitability) - Relative prices - Historical price growth - Total spending on health care services (absolute/relative, growth rate)	- Pricing/contract data - Interviews with representatives of transacting or comparator entities - Information on participation in value-based payment models - Documents relating to integration planning - Community Review Board (CRB) convening - Provider cost data	- Additional/more granular outcome measures - Diversion analysis - Willingness-to-Pay (WTP) analysis - Merger simulation - Synthesis of CRB opinions and recommendations - Analysis of interview transcripts/notes - Retrospective analysis of price changes following previous similar transactions - Assessment of potential efficiencies from integration - Qualitative analysis of interview transcripts/notes - Document review
Access	- APAC data - Hospital discharge data - CCO/Hospital financial reporting - Census data - Press releases and other public statements by the transacting entities - Other information provided in notice - Public comments submitted in response to notice	- Service volume (absolute and relative to service area/ comparator entity volume) - Number of providers/clinicians - Payer mix - Patient demographics	- CRB convening - Documents relating to integration planning - Workforce/capacity data - Enrollment data - Contract data (carriers) - Interviews with representatives of transacting or comparator entities - Emergency Department Information Exchange (EDIE)	- Additional/more granular outcome measures - Retrospective analysis of access outcomes following previous similar transactions - Analysis of service line profitability - Synthesis of CRB opinions and recommendations - Document review - Qualitative analysis of interview transcripts/notes
Equity	- APAC data - Financial reporting	- Community Benefit spending	- CRB convening - Enrollment data	- Synthesis of CRB opinions and recommendations

	PRELIMINARY REVIEW		COMPREHENSIVE REVIEW	
Domain	**Data Sources**	**Analyses**	**Potential Additional Data Sources**	**Potential Additional Analyses**
	- Health equity reporting - Census data - Community benefit reporting - Community health/equity assessments - Press releases and other public statements by the entities - Documents relating to integration planning - Public comments submitted in response to notice	- Patient demographics - Quality/access outcomes stratified by patient demographics - Document review	- Social needs screening/referral data - Interviews with representatives of priority population groups or community-based organizations - Health Care Workforce Reporting Program - Workforce directory/survey data - Traditional Health Worker/Health Care Interpretation registries	- Additional/more granular outcome measures - Provision of care coordination/social services referral - Qualitative analysis of interview transcripts/notes - Provision of translation/interpretation services - Utilization of traditional/community health workers - Workforce diversity/representation of community
Quality	- APAC data - Existing quality reporting (e.g., CCO metrics, hospital quality, Medicare, NCQA) - DCBS health insurer data - CAHPS survey data - Other relevant information provided in notice - Public comments submitted in response to notice	- Clinical quality measures - Patient outcome measures - Patient experience measures - Participation in national or statewide care delivery transformation efforts	- Documents relating to quality management/integration planning - Interviews with representatives of entities - Electronic health record extracts - Information on participation in value-based payment models - CRB convening - Grievance and appeals reporting - Entity-administered CAHPS results	- Additional/more granular outcome measures - Document review; assessment of potential quality improvements from integration - Qualitative analysis of interview transcripts/notes - Synthesis of CRB opinions and recommendations - Retrospective analysis of quality outcomes following previous transactions

Table 2: Supplemental information that may be requested for preliminary review

Area/Domain	Supplemental Information
Nature of the transaction and characteristics of the entities	- Chart showing all entities involved in the transaction and their relationships to one another (e.g., ownership stake, control, management) pre- and post-transaction; may involve a more detailed chart necessary for transaction review and a separate more redacted chart for public posting - Description of all entities involved in the transaction, their role in the transaction, and their connection to patient care - Annual national and Oregon revenue for all entities involved in the transaction in the previous year(s) - Business registration and/or incorporation documents (if business is primarily registered in another state) - Current investigations, regulatory action, fines, or formal complaints filed against any entity involved in the transaction
Cost	- For hospitals: Hospital Price Transparency Law-compliant data (if not readily available online), summarized or filtered as relevant - For carriers: Transparency in Coverage-compliant data (if not readily available online), summarized or filtered as relevant
Access	- For providers: patient payer mix from recent year(s), at minimum identifying patients covered by Medicare, Medicaid (Oregon Health Plan), commercial, and uninsured; may request coverage by specific carrier if relevant to the transaction - Patient/member demographic information from recent year(s), including race, ethnicity, language, age, sex, disability, gender identity, sexual orientation, zip code*Provider/staff demographic information from recent year(s) - Number of providers and/or full-time equivalent (FTE) and patient/staff ratios, by provider type as relevant to the transaction
Equity	- Documentation/description of culturally and linguistically appropriate services** provided or offered - Policy/procedure and patient-facing materials around provision of interpretation services - Policy/procedure and patient-facing materials around unpaid/charity care and patient financial assistance - Policies or action plans to identify and reduce health disparities and inequities across patient/member population - Documentation/description of community involvement in entity governance or decision-making - Documentation/description of programs, initiatives, or events intended to engage the community served and build relationships; examples include health fairs, patient education programs, or sponsored health-related events - Documentation/description of participation in community groups, including community organization boards, Coordinated Care Organization (CCO), participation in Regional Health Equity Coalitions (RHECs), support of county health department efforts or other local government activities (e.g., school districts, Parks and Recreation, Early Learning Hubs) - Community investments or benefits aimed at addressing health inequities and/or social determinants of health - For CCOs: most recent version of Health Equity Plan - For relevant entities: narrative around health equity strategy and/or specific elements related to health equity from most recent submission for accreditation to National Committee for Quality Assurance (NQCA), the Patient-Centered Primary Care Home (PCPCH) program, the Joint Commission, or other quality-related bodies - Consumer Assessment of Healthcare Providers and Systems (CAHPS) or other patient experience survey results and/or quality reporting data disaggregated by patient/member demographics

Area/Domain	Supplemental Information
Quality	- For carriers and providers: most recent quarterly/annual CAHPS or other patient experience survey results prior to transaction - For CCOs: most recent version of the Transformation Quality Strategy (TQS) and quality incentive metric performance - For Medicare certified providers: most recent quality reporting data prior to transaction that reflects performance on full patient population for all applicable CMS quality reporting program measures - For relevant entities: narrative around quality improvement strategy or projects and summary of performance on included quality indicators from most recent submission for accreditation to NCQA, PCPCH or Joint Commission - Most recent data on patient/member complaints and grievances

* HCMO promotes the collection of REALD-compliant data but will accept all demographic information currently collected.
** Culturally and Linguistically Appropriate Services (CLAS) are defined as effective, equitable, understandable, and respectful quality care and services that are responsive to diverse cultural health beliefs and practices, preferred languages, health literacy, and other communication needs. Information about national CLAS standards can be found on the Health and Human Services (HHS) website.

Decision Criteria

HCMO will adhere to the criteria for approval outlined in OAR 409-070-0055 and OAR 409-070-0060. Tables 3 and 4 below map these criteria to HCMO's analytic domains. Findings from analysis of each domain will be considered in unison, and no a-priori weights will be applied to domain-specific results when arriving at a decision.

Table 3: Domain Relevance to OAR Criteria for Approval following Preliminary Review

OAR Criteria for Approval following Preliminary Review	Domain Relevance			
At least ONE must apply:	Cost	Access	Equity	Quality
In the interest of consumers and is urgently necessary to maintain the solvency of an entity	●	●	●	●
Unlikely to substantially reduce access to affordable health care in Oregon	●	●	●	
Likely to meet the criteria set forth in OAR 409-070-0060*	●	●	●	●
Not likely to substantially alter the delivery of health care in Oregon	●	●	●	●
Comprehensive review is not warranted given the size and effects of the transaction	●	●	●	

Table 4: Domain Relevance to OAR Criteria for Approval following Comprehensive Review

OAR Criteria for Approval following Comprehensive Review	Domain Relevance			
	Cost	Access	Equity	Quality
ALL must apply:				
No substantial likelihood of anticompetitive effects not outweighed by benefits in increasing or maintaining services to underserved populations	●	●	●	●
No substantial likelihood of being contrary to law*				
No substantial likelihood of jeopardizing the financial stability of a health care entity involved in the transaction	●			
No substantial likelihood that the transaction would otherwise be hazardous or prejudicial to consumers or the public	●	●	●	●
At least ONE must apply:				
Reduces growth in patient costs in accordance with health care cost growth targets under OAR 442.386 or maintains a rate of cost growth that exceeds the target that the entity demonstrates is in the public interest	●	●	●	●
Increases access to services in medically underserved areas		●	●	
Rectifies historical and contemporary factors contributing to a lack of health equity or access to services		●	●	
Improves health outcomes for residents of this state		●	●	●

*HCMO may rely on an assessment by the Department of Justice during preliminary review of whether the transaction is likely to be contrary to law.

Outcomes and Analyses

This section describes, for each domain, the key outcomes HCMO will use to assess performance and provides an overview of the methods that may be used to determine the likely impact of the transaction. Where possible, the description distinguishes between analyses performed during preliminary review versus comprehensive review.

Market Definition

Definition of the primary service area (PSA) of each health care entity involved in the transaction is fundamental to subsequent analyses. HCMO will use the methodology described in Appendix C to determine the zip codes that comprise the PSA(s) of all relevant entities. This geographic definition is used to identify other competing service providers operating in the region and the Oregon population potentially impacted by the transaction. This information supports several subsequent analyses:

- **Market share.** What share of total patient volume or revenues across comparable health care entities in the geographic service area is attributable to each of the entities?
- **Market concentration.** Calculating the Herfindahl-Hirschman Index (HHI) from market shares, how concentrated or competitive is the market?
- **Impacted population.** What are the demographic and socioeconomic characteristics of the people living in the PSA? Does this population have unique health needs?
- **Market geography.** Does the geography of the region present barriers to accessing services?

Cost

HCMO will assess current performance and the likely impact of the transaction on four broad cost outcomes: market share, prices, spending, and financial condition. The below subsections describe the assessment questions and analytic methods HCMO expects to use for current performance and impact analyses, respectively.

Current Performance

- **Prices.** How do the entities' prices for health care services compare to similar entities or other reference datasets?
- **Spending.** How do the entities' total expenditures for health care services compare to similar entities?
- **Financial condition.** What is the financial condition of the entities, including revenues, profitability, and ability to meet financial obligations? Are any of the entities facing an immediate risk of insolvency?

A list of potential measures for each outcome is provided in Appendix A.

Market shares will be calculated in aggregate across all health care services offered by the entities and disaggregated by payer and type of service. For example, in the case of a hospital system, market shares may be calculated for inpatient versus outpatient services and by Major Diagnostic Category (MDC). For a physician group, market shares may be calculated by specialty (primary care, cardiology, oncology, etc.).

For preliminary reviews, prices will be calculated based on allowed and paid amounts from claims or other publicly available pricing data. For hospitals, HCMO may rely on existing Hospital Payment Reports (also known as SB 900 reports) for common inpatient and outpatient procedures. Where possible, relative prices will be calculated separately for each payer and standardized to account for differences in service volume, service mix, patient acuity, and insurance product type. HCMO will examine relative prices in aggregate across all services, by place of service, and by type of service. HCMO may request additional data on pricing (including bonus and performance payments) from the entities when carrying out a comprehensive review.

For price outcomes, HCMO's analysis will focus on the commercial market, where prices for health care services are determined by negotiations between payers and providers. While consolidation may affect pricing in other markets (e.g.,

Medicaid) as well, the commercial market is likely to be more directly impacted.

If any of the entities claim to be facing an immediate risk of insolvency, HCMO will perform an initial assessment of the financial condition of the entity in question as part of the emergency review (if requested) or preliminary review. In the absence of insolvency risk, comprehensive reviews are required by OAR 409-070-0060 to include an assessment of the likelihood that the transaction would jeopardize the financial stability of one of the health care entities.

Impact Analysis

Assessment of the cost impacts of the transaction will examine how each of the outcomes are likely to change due to the transaction.

- **Market share.** How concentrated is the health care market in which the entities operate? How (if at all) will concentration change as a result of the transaction?
- **Prices.** How (if at all) will the transaction affect the prices consumers (e.g., patients, members) or payers (e.g., insurers, employers, and governments) pay for health care services?
- **Spending.** How (if at all) will the transaction affect total health care expenditures for the entities and the state as a whole?
- **Financial condition.** How (if at all) will the transaction impact the financial condition of the entities? If there is an immediate risk of insolvency, is the transaction likely to significantly reduce this risk? In the case of an acquisition, will the transaction reduce the financial security of the acquired entity?

HCMO will consider results across all four outcomes in arriving at a finding on the overall cost impacts of the transaction. Appendix B details the approaches HCMO will use to assess likely impacts in the cost domain. These methods include concentration (Herfindahl-Hirschman Index) analysis, diversion analysis, Willingness-to-Pay (WTP), merger simulation, and analysis of potential efficiencies from integration.

Access

HCMO will assess current performance and the likely impact of the transaction on three broad access outcomes: availability of services, payer mix, and patient demographics. The below subsections describe the assessment questions and analytic methods HCMO expects to use for current performance and impact analyses, respectively.

Current Performance

- **Availability of services.** What is the volume of services (e.g., primary, specialty, behavioral health, oral health, emergency, urgent care, inpatient/outpatient, maternity, etc.) provided by the entities? How does this compare to overall utilization of these services in the geographic service area? What is the ratio of service utilization/provider counts to population?
- **Payer mix.** What is the payer mix of the entities? How does this compare to the overall population in the geographic service area and to other nearby provider organizations?
- **Patient demographics.** What is the composition of the patient/member population based on race/ethnicity, gender, language, disability status, income/social determinants of health, and medical/behavioral health complexity? How does this compare to the overall population in the geographic service area and to other health care entities?

A list of potential measures for each outcome is provided in Appendix A.

Impact Analysis

- **Availability of services.** What is likely impact of the transaction on the volume of services (e.g., primary, specialty, behavioral health, oral health, emergency, urgent care, inpatient/outpatient, maternity, etc.) provided by the entities?
- **Payer mix.** What is likely impact of the transaction on the payer mix of the entities?
- **Patient demographics.** What is the expected impact of the transaction on the demographics of the population served by the entities?

HCMO will consider impact analysis results across all four measures in arriving at a finding on the overall access impact of the transaction. To assess impacts on access measures, HCMO will consider factors such as the entities' current performance on access measures, any plans to consolidate service lines, or any plans to improve availability of services, shift payer mix, or enhance access for particular populations. HCMO will also consider any concerns about adverse impacts on access outcomes voiced by members of the public, specifically by community members within the geographic service area of the entities.

For comprehensive reviews, HCMO may request to review the entities' plans and proposals in the context of integration planning. Of particular interest would be the level of detail of these plans or proposals (for example, inclusion of specific locations for expansion, assessments of provider capacity, number of clinicians needed, resource commitments, and timelines). In addition, HCMO may rely on financial analysis of service line or facility-level profitability to assess the potential for access reductions, as profitability is likely to be a factor in any decision to discontinue services or shift the location of services. HMCO may convene a CRB to provide input on potential access impacts. Where possible, HCMO may also rely on retrospective quantitative analysis of previous transactions involving the relevant entities to assess impacts of those transactions on access.

Equity

HCMO will assess current performance and the likely impact of the transaction on four broad equity outcomes: equitable access, equitable quality, community engagement, and equity-enhancing services. The below subsections describe the assessment questions and analytic methods HCMO expects to use for current performance and impact analyses, respectively.

Current Performance

- **Equitable access.** How does patient or member utilization of the entity's services vary by race/ethnicity, gender, language, disability status, income, and other characteristics? How (if at all) does utilization among populations experiencing health inequities (e.g., low-income individuals, racial/ethnic groups, people with disabilities, LGBTQ+, people with limited English proficiency) differ from that of other patients or members? How does this compare to other similar health care entities?
- **Equitable quality**. How does the entity's performance on quality measures vary by race/ethnicity, gender, language, disability status, income, and other characteristics? How (if at all) does care quality for populations experiencing health inequities (e.g., low-income individuals, racial/ethnic groups, people with disabilities, LGBTQ+, people with limited English proficiency) differ from that of other patients or members? How does this compare to other similar health care entities?
- **Community engagement:** What is the extent of the entities' investment in the communities they serve? How much do they spend on community-level initiatives to address health inequities and social determinants of health? What is the ratio of this spending to operating profits? How do the entities involve the community in the decision-making process for such investments?
- **Equity-enhancing services.** Do the entities provide services that promote health equity, such as preventive services, coordination with social services, services provided by community/traditional health workers, culturally

appropriate services, chronic disease management services, and translation/interpretation services?

A list of potential measures for each outcome is provided in Appendix A. For assessing equitable quality and access measures, preference during preliminary review will be placed on claims-based measures whose results can be disaggregated by population demographics available within existing data sources, including race, ethnicity, age, language, gender, and disability status. Additional information may be obtained from existing health equity or community benefit reporting, community health assessments, etc. For comprehensive reviews, HCMO may use additional data sources such as workforce data and information on referrals to community-based organizations.

Impact Analysis

- **Equitable access.** How will the transaction affect the entities' provision of services for populations experiencing health inequities, overall and relative to other populations?
- **Equitable quality**. How will the transaction affect the entities' performance on quality measures for populations experiencing health inequities, overall and relative to other populations?
- **Community engagement:** What is the likely impact of the transaction on the level of investment in the entities' local communities, particularly as it pertains to initiatives to address health inequities and social determinants of health? How will the transaction affect the entities' ability to respond to community needs?
- **Equity-enhancing services.** What is the likely impact of the transaction on the entities' provision of services that promote health equity?

HCMO will consider impact analysis results across all four measures to arrive at a finding on the overall equity impact of the transaction. To assess these impacts, HCMO will consider factors such as the entities' track record in addressing health inequities (as measured by the analysis of current performance), integration plans post-transaction, and any health equity plans or assessments developed in connection with the transaction. Of particular interest would be the level of detail of such plans (for example, identification of priority populations and services, inclusion of specific locations for expansion, assessments of provider capacity and workforce representation, number of clinicians needed, resource commitments, and timelines). Any consolidation of service lines or facility closures resulting from the transaction would be concerning if the changes are likely to disproportionately affect populations experiencing health inequities. Additionally, HCMO will consider whether the transaction brings a shift in management from the local/facility level to a higher organizational level (e.g., system). This may affect the entities' ability to provide services that are responsive to community-level socioeconomic and demographic characteristics, as well as their ability to identify effective strategies for addressing health inequities.

HCMO will also consider any concerns about impacts on equity outcomes voiced by members of the public, specifically by community members within the geographic service area of the entities. For comprehensive reviews, HCMO may convene a CRB or conduct interviews with representatives of priority population groups or community-based organizations to obtain input on potential equity impacts. (Please refer to HCMO sub-regulatory guidance: Criteria for Community Review Boards.[5])

Quality

HCMO will assess current performance and the likely impact of the transaction on three broad quality outcomes: clinical processes, patient outcomes, and patient experience. The below subsections describe the assessment questions and analytic methods HCMO expects to use for current performance and impact analyses, respectively.

Current Performance

- **Clinical processes.** How do the entities perform on quality measures related to clinical processes? How does this compare to the statewide average or national benchmarks?
- **Patient outcomes.** How do the entities perform on quality measures related patient outcomes? How does this

[5] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/Draft-Community-Review-Board-Criteria-20220121.pdf.

compare to the statewide average or national benchmarks?

- **Patient experience.** How do the entities perform on quality measures related to patient experience? How does this compare to the statewide average or national benchmarks?

A list of potential measures for each outcome is provided in Appendix A. For preliminary reviews, HCMO will focus on measures that can be calculated from readily available administrative data (e.g., claims), publicly available reports, scorecards, or rankings, and measures already calculated at the entity-level for quality reporting purposes. For comprehensive reviews, if there are concerns about adverse quality impacts, HCMO may request additional data from the entities, such as Electronic Health Record (EHR) extracts or entity administered Consumer Assessment of Healthcare Providers and Systems (CAHPS) survey data.

HCMO will also consider the entities' participation and performance in national or statewide care delivery transformation efforts, as well as participation in quality-based risk contracts. For comprehensive reviews, HCMO may request and review additional documentation from the entities on quality improvement activities, such as:

- Quality improvement plans
- Implementation of quality tracking/improvement systems
- Governance for quality management
- Participation in population health management programs
- Electronic health record use and interoperability

Impact Analysis

- **Clinical processes.** What is the likely effect of the transaction on performance on quality measures related to clinical processes?
- **Patient outcomes.** How might the transaction impact performance on quality measures related patient outcomes?
- **Patient experience.** How might the transaction impact performance on quality measures related patient experience?

HCMO will consider impact analysis results across all four measures in arriving at a finding on the overall quality impact of the transaction. At the preliminary review stage, HCMO will assess how any potential anti-competitive effects of the transaction identified under the cost domain might affect the entities' incentives for quality improvement or quality-enhancing innovation. HCMO will also consider the entities' track record in delivering high quality health care services (as measured by the analysis of current performance) and any concerns about adverse impacts on quality outcomes voiced by members of the public, specifically by community members within the geographic service area of the entities.

For comprehensive reviews, HCMO may request to review the entities' plans and proposals for integration of clinical or administrative operations post-transaction. These would be relevant to assessing the degree of integration or coordination in the production of health care services that would result from the transaction. They would also be informative for understanding quality improvement initiatives planned as part of integration activities. Based on these plans and the entities' current performance on quality, HCMO would consider the impact of the transaction on quality improvement opportunities and the development of quality improvement initiatives through access to a shared pool of capital, patients and knowledge. Of particular interest would be the level of detail of these plans or proposals (for example, inclusion of specific service lines, assessments of quality improvement opportunities, required platforms and systems, resource commitments, and timelines). HCMO may interview representatives of the entities to obtain additional information on such plans and their proposed implementation. HMCO may also convene a CRB to provide input on potential impacts of the transaction on patient experience. In cases where an entity has engaged in a similar transaction previously, HCMO may perform statistical analyses to assess whether the previous transaction was associated with any adverse effects on quality.

Follow-up Reviews

HCMO is statutorily required to evaluate the impact of each transaction one, two, and five years after closing. Analyses performed during the preliminary or comprehensive review of the proposed transaction will be revisited to assess for any changes likely driven by the transaction. These follow-up reviews will focus on several key areas:

- **Conditions for approval.** HCMO will gather information and perform analyses to verify that all entities are meeting any conditions attached to transaction approval. Examples include confirming that facilities remain operational, rates of service access are being maintained, costs have not significantly increased, or that quality of care has not declined.
- **Commitments in the notice.** Transaction approval may be predicated on statements or commitments presented in the notice itself, particularly around access and cost. Follow-up reviews will confirm whether entities are upholding those commitments, for example maintaining a similar payer mix among patients served.
- **Areas of concern.** Preliminary or comprehensive review may identify issues that do not contradict conditions for transaction approval but do raise concerns for consumers, for example existing poor quality of care from a provider or limited access to services within a region. HCMO may determine that these issues are unlikely to be changed by the given transaction, or improvement in these areas might not be attached as a condition to approval. Follow-up analyses can provide transparency around the entities' independent efforts to make improvements to service delivery.
- **Post-transaction changes.** Follow-up reviews will assess what other changes have occurred within the entities post-transaction that may impact delivery of health care services in the future, for example organizational restructuring, changes to leadership or staffing, closing or downsizing of facilities or lines of service, or reduced resources to programs meeting special health care needs. Impacts of these changes may not be detectable in early follow-up reviews but may be identified as areas of concern to revisit in subsequent analyses.

HCMO may request additional information from entities to support follow-up review. This may include updates to supplemental items requested during preliminary or comprehensive review. Given the time lag in administrative data, HCMO may also request more current data collected by the entities to more accurately measure short-term impacts of the given transaction.

Identifying Comparator Entities

This section describes HCMO's approach to identifying comparator entities for purposes of assessing relative performance and market shares. This will be based on three main considerations: geographic service area, facility type (in the case of provider organizations), and type of service.

Geographic Service Area

To identify comparator entities, HCMO will first define the geographic area in which the majority of the entities' customers (patients, members) reside.

For provider organizations, HCMO will calculate the primary service area (PSA) as the set of contiguous of zip codes around the provider location from which the entity draws 75% of its patients.[6] Appendix C provides an example of this

[6] The 75% threshold is used by the U.S. Department of Justice and Federal Trade Commission to calculate PSAs for antitrust oversight of Medicare Accountable Care Organizations (ACOs). The federal agencies note that, while the PSA does not necessarily correspond to a "relevant market" for antitrust purposes, it is a useful screen for evaluating competitive effects of ACOs. (See Federal Trade Commission/Department of Justice, Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program, October 28, 2011, available at https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf.)

calculation for a general acute care hospital. HCMO may rely on commonly used, pre-existing service area definitions, if these are roughly consistent with the service area identified by the 75% method.

For insurance carriers and CCOs, HCMO will use plan service areas and CCO service areas, respectively.

Facility Type

HCMO will identify the type(s) of facilities at which the provider organization's services are offered (e.g., inpatient acute care hospital, specialty hospital, ambulatory care center, clinic.) In selecting comparator hospitals, HCMO may also consider other commonly accepted classifications, such as the level of trauma care provided, designation as a teaching hospital, safety-net hospital, or critical access hospital.

Type of Service

HCMO will consider the type(s) of service(s) offered by the health care entity. For inpatient facilities (e.g., hospitals), a service type is defined as Major Diagnostic Category (MDC). For physicians, a service type is the physician's primary specialty (primary care, cardiology, oncology, etc.) For outpatient facilities, service types would be defined as categories of services based on procedure (CPT/HCPCS) codes.

For payers, HCMO will consider factors such as the type of plan offered (e.g., POS, PPO, or HMO) and the market segments served (e.g., commercially insured, Medicare, Medicare Advantage, Oregon Health Plan, or individual/marketplace).

Collaboration with Other State Agencies and Programs

HCMO will coordinate and collaborate on an as-needed basis with other state agencies and programs that oversee health care entities in Oregon in reviewing material change transactions. Coordination may be required when there is overlap of agencies' oversight responsibilities. Additionally, communication or collaboration for the purpose sharing expertise and data will facilitate expedient, high-quality reviews, avoid duplication of work, and reduce the need for data requests from the entities. Where inter-agency sharing of information is needed, HCMO will share a minimum necessary information in accordance with regulations or contractual agreements governing privacy and confidentiality.

- **Department of Consumer and Business Services (DCBS).** HCMO will collaborate with DCBS on any transaction involving at least one domestic insurance carrier. HCMO and DCBS will each carry out their own review, and HCMO will provide a recommendation to DCBS, who will decide the outcome of the review.
- **Department of Justice (DOJ).** HCMO may rely on legal advice and analysis by DOJ as needed. Depending on the scope of work and internal capacity, DOJ may contract with an external law firm for legal counsel. (Please refer to HCMO's sub-regulatory guidance: Criteria for OHA Use of Outside Advisors for Material Transaction Review.[7])
- **OHA Office of Actuarial and Financial Analytics (OAFA).** For any transaction involving a CCO, HCMO will coordinate its review activities with OAFA to avoid duplication of effort. HCMO and OAFA will come to a mutually acceptable decision on the outcome of the review.
- **Other OHA Programs, including Cost Growth Target, Hospital Reporting, and All Payer All Claims (APAC) Programs.** HCMO will consult with the Cost Growth Target, Hospital Reporting, and APAC programs within OHA regarding data and quantitative methods, particularly relating to measures of cost and hospital performance. Program staff may provide analytic support on HCMO reviews and share data collected by the programs on an as-needed basis. HCMO may also consult with the Certificate of Need (CN) program if the transaction involves facility or service expansion projects potentially subject to CN rules.

[7] Guidance is available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/HCMO-Outside-Advisors.pdf.

Appendices

A. Measures

Table A1 displays a menu of measures HCMO may use to analyze current performance and assess impacts of the transaction in each domain. Not all of these will be applicable to each transaction, and exact definitions will depend on the specifics of the health care services in question. This list is not exhaustive; HCMO may incorporate other measures not included here. This list will be updated periodically as additional measures or new data sources are considered during the course of HCMO reviews.

To measure outcomes at the entity level, HCMO will use National Provider Identifier (NPI) information from the NPI form submitted with the notice, supplanted with additional NPI information available to the Oregon Health Authority (e.g., from provider enrollment databases).

Table A1: HCMO Outcome Measures Menu

Domain	Outcome	Measure
Cost	Market share	Share of inpatient general acute care discharges (by payer, specialty) Share of outpatient visits (by payer, specialty) Share of adult primary care visits (by payer) Share of specialty provider visits (by payer) Share of enrollment in large group/small group/individual market(s) Share of Net Patient Service Revenues (by payer)
	Price	Prices for commercial inpatient services, relative to other similar entities (or state average), by payer (based on paid/allowed amounts) Prices for commercial outpatient services, relative to other similar entities (or state average), by payer Prices for commercial services relative to Medicare Bonus and performance payments Out of pocket payments Premiums
	Spending	Total cost of care (PMPM) Total resource use (PMPM) Annual spending growth (overall and by major spending category) Health status adjusted total medical expense (HSA TME) for patients attributed to each entity's PCPs, by payer Percentage of spending in value-based-payment contracts (by LAN category)
	Financial condition	Payer mix (Medicaid, Medicare, commercial, individual/marketplace, charity care) Operating revenues and expenses (per discharge or other unit) Other income and expenses Operating margin Total margin Total net assets on hand Readily available cash/investments Current ratio Debt-to-capital ratio Average age of plant Medical loss ratio

Domain	Outcome	Measure
		Equity & consolidated investments Profitability by service line or facility
Quality	Clinical processes	Participation and performance in national/statewide care delivery transformation efforts Revisits for frequent Emergency Department (ED) users Participation in quality-based risk contracts Medical home (e.g., PCPCH tier) Integration of behavioral health/oral health care with physical health care (e.g., avoidable ED visits, avoidable hospitalization, follow-up after hospitalization)
	Patient outcomes	Patient safety (falls, healthcare-associated infections, medication safety, etc.) All-cause readmissions Avoidable complications Low value care Prevention/screening (e.g., immunization, cancer screening, well-care visits, contraception use) Chronic disease management Maternity (e.g., low-risk caesarian delivery, postpartum care)
	Patient experience	Overall rating of health care/provider/health plan (CAHPS) Getting care quickly (routine/urgent care) (CAHPS) Staff explained medicines/gave patient discharge information Customer care service Patient/ consumer complaints Language access to culturally responsive services
Access	Availability of services	Number of visits for/ number of providers offering - Primary care - Specialty care - BH care (including SUD treatment) - Dental care/ oral health - Emergency care - Urgent Care - Inpatient (acute/non-acute) - Outpatient (including ambulatory surgical centers) - Prenatal/maternity Provider to population ratios - Primary care - Pediatric - Geriatric - Nurses - Specialists - Counselors and therapists Provider network size, composition Provider direct patient care FTE Number of PCPs accepting new patients
	Payer mix	Payer mix based on gross patient service revenue (GPSR)

Domain	Outcome	Measure
	Patient demographics	Case mix index (CMI) Composition of patients/members served by: - Race/ethnicity - Sex/gender - Language - Income level - Disability status - Medical/behavioral health complexity
Equity	Equitable access	Service utilization stratified by race, ethnicity, age, language, gender, disability status, etc. Access disparities between populations experiencing health inequities (low income, racial/ethnic groups, LGBTQ+, people with disabilities, people in rural areas, HNA populations) and other populations. Workforce diversity/representation of community (by occupation): - Language - Race/Ethnicity
	Equitable quality	Quality domain measures stratified by race, ethnicity, age, language, gender, disability status, etc. Quality disparities between populations experiencing health inequities (low income, racial/ethnic groups, LGBTQ+, people with disabilities, people in rural areas, non-English speaking, HNA populations) and other populations. For example, - Avoidable hospitalization - Avoidable ED visits - Readmissions within 30 days
	Community engagement	Community Benefit Spending Percentage of profits allocated to community-level investments Established relationships or collaborations with community-based organizations
	Equity-enhancing services	Volume of services relative to population served: - Services related to the treatment of a chronic condition - Prevention services, including non-clinical services - Pregnancy -related services - Culturally appropriate services - Translation and interpretation services - Care navigation/coordination services - Services provided by Traditional Health Workers or Community Health Workers - Screening for social needs - Referrals to community-based organizations for social services

Approach to Selection of Quality and Equity Measures

HCMO will seek to apply consistent and standardized metrics to health plan, health system and provider organization performance to assess current performance and potential impacts in each domain. Hundreds of validated and standardized measures exist to quantify processes and outcomes regarding safety, quality, access, and patient experience across all applicable health care entities. Needing to balance thoroughness with expediency, HCMO will select key measures that can serve as broader indicators of the overall ability of an entity to equitably provide high quality care. Within the state of Oregon, several committees under the purview of the Oregon Health Policy Board have been tasked to consolidate and

prioritize a menu set of measures to drive quality improvement, systems transformation and health equity across sectors, and several programs have successfully or are currently utilizing these measures to drive process efficiencies and better health outcomes for Oregonians. HCMO will borrow from these measure sets and associated technical specifications whenever possible. During preliminary review, preference will be placed on metrics that can be constructed using readily available data sources (e.g., APAC, hospital discharge data) and measures already calculated at the entity-level for other reporting purposes (e.g., CCO metrics, hospital quality metrics, Medicare metrics, NCQA accreditation data, etc.).

B. Methods for Analyzing Cost Impacts

This appendix describes the approaches HCMO may use to assess the likely impact of a material change transaction in the cost domain. The specific facts of the proposed transaction, the availability of reliable data, and time constraints associated with preliminary and comprehensive review periods will affect the analytic methods for a given transaction.

Concentration (HHI) Analysis

Concentration is a measure of the degree of competition in a market; highly concentrated markets are generally characterized by a smaller number of firms and higher market shares for individual firms. (See Glossary for additional definitions.) When a transaction involves health care entities offering similar products or services (a "horizontal" transaction), the level of concentration in the market and the change in concentration resulting from the transaction is useful as an initial screen for potential anticompetitive effects.

Market concentration will be measured using the Herfindahl-Hirschman Index (HHI), a measure commonly used by federal and state antitrust enforcement agencies. HHI is calculated as follows:

$$HHI = (S_1^2 + S_2^2 + S_3^2 + \cdots S_n^2)$$

Where S_1 is market share (in percentage points) of firm 1 and n is the total number of competitors in the market. By summing the squared values of market shares, the HHI gives greater weight to firms with larger market shares.

Transactions occurring in concentrated markets and those involving a significant change in concentration are more likely to have adverse effects on competition and lead to price increases. For horizontal transactions under preliminary review, HCMO will use the HHI thresholds specified in the U.S. Department of Justice and Federal Trade Commission Horizontal Merger Guidelines[8] to identify transactions that may have anticompetitive effects (see Table B1 below). Transactions meeting the HHI thresholds for "high" or "moderate" levels of concern would indicate the need for a comprehensive review.

Table B1: HHI Thresholds

Post-transaction HHI	HHI Change	Level of Concern
> 2,500	> 200	High (if both). Presumed likely to enhance market power:
> 2,500	>= 100 and <= 200	Moderate (if both). Potentially raises significant competitive concerns and often warrants scrutiny.
>= 1,500 and <= 2,500	>= 100	Moderate (if both). Potentially raises significant competitive concerns and often warrants scrutiny.
< 1,500	< 100	Low (if either). Unlikely to have adverse competitive effects and ordinarily requires no further analysis.

There may be instances where a transaction does not lead to an increase in HHI but nevertheless has the potential to reduce competition. One such case is "cross-market" consolidations, for example, a hospital system acquiring a hospital outside its service area. If both parties negotiate with a common buyer (e.g., an insurer), and customers of the buyer (e.g., large employers) value the inclusion of both parties in their bundle, the consolidated entity may be able to negotiate higher

[8] U.S. Department of Justice and the Federal Trade Commission, Horizontal Merger Guidelines, August 19, 2020, available at https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

prices for hospital services.[9] In this example, HCMO may determine that a comprehensive review is needed so that further analyses (such as diversion analysis and Willingness-to-Pay, described below) can be conducted.

Diversion Analysis

HCMO may use diversion analysis to assess the likely price effects of a transaction under comprehensive review. The diversion ratio seeks to measure the impact on the probability that consumers will choose a given product or service if a competing product or service is excluded from their choice set (e.g., due to consolidation). It is commonly used by federal antitrust agencies to screen for anti-competitive effects of hospital mergers.[10] Using the example of a hospital merger, diversion analysis quantifies the extent to which patients consider the merging hospitals to be substitutes for one another. This, in turn, affects the bargaining power of the merged entity in reimbursement rate negotiations with insurers. When hospitals are close substitutes, the costs to an insurer of failing to reach agreement with the merged entity (via reduced value of its provider network) are higher than the costs of failing to reach agreement with either of the merging hospitals individually, resulting in higher reimbursement rates compared to pre-transaction rates.

The diversion ratio from hospital k to hospital l is:

$$d_{kl} = \frac{\left(\sum_i prob_{il\backslash k} - \sum_i prob_{il}\right)}{\sum_i prob_{ik}}$$

Where $prob_{il}$ is the fitted probability that patient i is treated at hospital l, $prob_{ik}$ is the fitted probability that patient i is treated at hospital k, and $prob_{il\backslash k}$ is the fitted probability that patient i is treated at hospital l under the hypothetical exclusion of hospital k. In this example, the diversion ratio is derived from estimating a regression model of patient hospital choice using hospital discharge data. This parameter can be used to calculate the value of diverted sales; if this value is small (e.g., 5% or less), the merger is unlikely to lead to significant price increases.[11]

Willingness-to-Pay (WTP) Analysis

Another possible approach for assessing price impacts from a merger or acquisition under comprehensive review is Willingness-to-Pay (WTP) analysis. WTP is a measure of provider market power based on a bargaining model of provider-insurer price negotiation. It assumes that when competing providers merge, they negotiate on an all-or-nothing basis (i.e., the insurer must contract with both providers in order to contract with either provider). When this happens, the insurer's cost of failing to reach agreement with the merged entity (in terms of welfare loss for the insurer's members) is higher than the sum of losses associated with failing to reach agreement with each provider individually. This increases the bargaining power of the merged entity and leads to higher reimbursement rates.

WTP is measured as the change in member welfare (consumer surplus) associated with the merged provider's inclusion in an insurer's network. The increase in market power associated with the merger is the net change in WTP associated with the combination of the two providers. WTP is obtained by estimating a regression model of patient provider choice.[12]

Merger Simulation

Merger simulation involves regression analysis to estimate the equilibrium price effect of a merger. Such approaches have been used in federal investigations of hospital mergers. For example, Farrell (2011) describes a simulation model used by the Federal Trade Commission that regresses case-mix adjusted prices on WTP per discharge and measures of cost. Like diversion and WTP analysis, merger simulation requires significant time and resources and could therefore only be conducted under a comprehensive review.

---

[9] See for example, Dafny et al (2019).

[10] See for example, Farrell et al (2011) and U.S. Department of Justice and the Federal Trade Commission, Horizontal Merger Guidelines, August 19, 2020, available at https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

[11] The Horizontal Merger Guidelines generally define "small" as 5% or less.

[12] See Vistnes & Town (2001) and Dranove & Sfekas (2009).

Analysis of Vertical Transactions

The diversion analysis and WTP methods were both developed for analysis of horizontal transactions and do not necessarily apply to vertical consolidation (for example, the acquisition of a physician group by a hospital). Federal antitrust agencies have not yet settled on guidelines for assessing market power and price effects of vertical transactions.[13]

For vertical transactions, HCMO will perform an HHI analysis for both upstream and downstream markets as part of preliminary review. Although HHI is not necessarily indicative of competitive concerns in the case of vertical consolidation, it remains relevant for assessing likely competitive effects. Anticompetitive effects from vertical mergers are less likely if neither of the entities has significant market power prior to consolidation. Furthermore, a vertical merger may result in a horizontal effect due to higher concentration in one of the affected markets. For example, a hospital's acquisition of multiple physician practices may reduce the number of competitors in the local physician services market.

For comprehensive reviews, HCMO will consider other options for assessing price effects from vertical transactions, such as measuring the likelihood of foreclosure and raising rivals' costs. Merger simulation may also be used. Foreclosure occurs when an upstream merged firm refuses to supply rivals of its downstream division with an input. In the example of acquisition of a physician group by a hospital, two types of foreclosure are possible: foreclosure of rival hospitals from access to physician services, and foreclosure of rival physician practices from hospital services. High diversion ratios and a high margin for downstream operations relative to upstream operations have been found to be associated with higher likelihood of foreclosure.[14] To assess the likelihood of foreclosure, HCMO may thus calculate the margin for hospital services relative to physician services, diversion ratios between the acquiring hospital and competing hospitals, and diversion ratios between the acquired physician group and other competing groups.

Raising rivals' costs is a less extreme form of foreclosure wherein the upstream division of the merged firm charges downstream rivals more for the input. HCMO may consider diversion ratios and relative margins as indicators of the likelihood of raising rivals' costs.

In the case of a hospital acquisition of a provider group, HCMO will also assess the ability of the hospital to obtain higher facility fees for physician services due to the transaction.

Potential Efficiencies from Integration

Any claim by the entities that the transaction would generate substantial cost savings (e.g., from economies of scale) would need to be substantiated by the entities and possibly reviewed by an outside advisor as part of a comprehensive review. HCMO may request to review the entities' plans and proposals for integration of clinical or administrative operations post-transaction. These would be relevant to assessing the degree of integration or coordination in the production of health care services that would result from the transaction and resulting opportunities for realizing any cost savings. Based on these plans and the entities' current performance on cost, HCMO would consider the impact of the transaction on opportunities for cost reduction and the likelihood that anticipated efficiencies would materialize. Of particular interest would be the level of detail of related plans or proposals (for example, inclusion of specific service lines, assessments of cost reduction opportunities, systems integration plans, resource commitments, and timelines). HCMO may interview representatives of the entities to obtain additional information on such plans.

In the case of vertical transactions, HCMO will also consider opportunities for vertical integration to reduce transaction costs (for example, associated with contracting), facilitate communication and coordination, and harmonize incentives of the

[13] In September 2021, the Federal Trade Commission and U.S. Department of Justice withdrew their guidelines for vertical mergers published in 2020. The agencies committed to continue working to review and update merger guidelines to reflect current economic theory and the dynamics of modern markets. (See https://www.ftc.gov/news-events/press-releases/2021/09/federal-trade-commission-withdraws-vertical-merger-guidelines.)

[14] See Lustig et al (2020).

transacting firms.[15] This may result in lower costs, improved quality, and increased investment and innovation.

More generally, HCMO will consider claims of cost savings from integration efficiencies in the context of the competitive environment facing the entities post-transaction. Anticipated cost savings, if they materialize, do not necessarily translate into lower negotiated rates with insurers or reduced costs for patients.

Financial Analysis

If the entities are requesting an emergency exemption, HCMO will perform an emergency review to determine the financial condition of the entity in question, the risk of insolvency, and the likelihood that the transaction would significantly reduce this risk. In the absence of insolvency risk, for transactions under comprehensive review, HCMO would assess the likelihood that the transaction would jeopardize the financial stability of one of the health care entities (in accordance with OAR 409-070-0060). This might occur, for example, if the acquiring entity holds a significant amount of debt or has a track record of relying heavily on debt financing to grow its operations.

Financial analyses would include a multi-year review of financial performance and credit rating based on standard metrics obtained from profit & loss and balance sheet statements. If an entity has been involved in previous mergers, acquisitions, or other combinations, HCMO may examine the impact of those transactions on the entity's financial condition. When analyzing a proposed transaction involving only carriers, HCMO will coordinate with DCBS to avoid duplication of analyses.

[15] See for example, Salop (2016). One often cited impact of vertical consolidation is the elimination of double marginalization (EDM) benefit. This occurs when a merger allows the downstream firm to acquire the upstream firm's input at a price=marginal cost, giving the downstream firm an incentive to reduce prices after the merger.

C. Example of Primary Service Area Calculation

Primary Service Areas (PSAs) will generally be calculated by service line, subject to data availability. For example, PSAs may be calculated for inpatient general acute care services, inpatient specialty acute care services, outpatient/ambulatory services, primary care services, and other service lines.

To calculate the PSA of a general acute care hospital:

1. For each zip code in Oregon, identify the number of general acute care discharges from the hospital of interest by patient zip code of residence for the most recent year(s) for which data is available.
2. Rank zip codes by number of discharges.
3. Starting with the facility's zip code, add contiguous zip codes to the map based on discharge volume rank. A zip code with a high volume of discharges that is not immediately contiguous with the facility zip code may be permanently excluded from the PSA, or only temporarily excluded until subsequent zip codes are added that fill in the geographical gap.
4. Continue to add zip codes until the total discharge count from zip codes contiguous with the facility constitutes 75% of the hospital's total discharges. The final zip code added to reach 75% of discharges may result in total PSA discharge volume exceeding the threshold.
5. If the resulting PSA completely encircles a zip code or set of zip codes not included in the PSA (due to low discharge volume), add encircled zip codes to the PSA to create a solid geographical area. This may also result in a PSA discharge volume over 75% but creates a more visually coherent geographic service area.

Glossary

Market – A collection of buyers and sellers that enter into agreements to purchase and sell a product or service. Markets are typically defined in terms of product/service and geographic reach (e.g., local, state, national, international, global).

Competition – A situation in a market in which firms or sellers independently strive to attract buyers for their products or services by varying prices, product characteristics, promotion strategies, and distribution channels.

Concentration – A measure of the degree of competition in the market; highly concentrated markets are generally characterized by a smaller number of firms and higher market shares for individual firms.

Market power – Also referred to as monopoly power, the power of a single firm or group of firms to set price profitably above the level that would prevail under competition. Increases in market concentration may confer market power.

Consolidation – The combination of two or business units or companies into a single, larger organization. Consolidation may occur through a merger, acquisition, joint venture, affiliation agreement, etc.

Horizontal consolidation – The combination of two or more business units or companies that formerly competed with one another. In health care, the combination of two hospitals or two insurers would be considered horizontal consolidation.

Vertical consolidation – The combination of two companies or business units in different lines of work or operating at different levels of the supply chain. In health care, the acquisition of an ambulatory care clinic by a hospital or the merger of a health plan with hospital system would be considered a vertical consolidation.

Health equity –As defined by OHA:

Oregon will have established a health system that creates health equity when all people can reach their full health potential and well-being and are not disadvantaged by their race, ethnicity, language, disability, age, gender, gender identity, sexual orientation, social class, intersections among these communities or identities, or other socially determined circumstances. Achieving health equity requires the ongoing collaboration of all regions and sectors of the state, including tribal governments to address:

- *The equitable distribution or redistribution of resources and power; and*
- *Recognizing, reconciling, and rectifying historical and contemporary injustices.*

References

Dafny, L., Ho, K. and R.S. Lee, "The price effects of cross-market mergers: theory and evidence from the hospital industry," *RAND Journal of Economics* 50, no.2 (2019), 286-325.

Dranove, D. and A. Sfekas, "The Revolution in Health Care Antitrust: New Methods and Provocative Implications," *The Milbank Quarterly* 87, no. 3 (2009), 607-632. doi: 10.1111/j.1468-0009.2009.00573.x

Farrell, J., Balan, D., Brand, K. and B. Wendling, "Economics at the FTC: Hospital Mergers, Authorized Generic Drugs, and Consumer Credit Markets," FTC Report, October 2011, available at https://www.ftc.gov/reports/economics-ftc-hospital-mergers-authorized-generic-drugs-consumer-credit-markets..

Gaynor, M. and R. Town, "Competition in Health Care Markets," in: M.V. Pauly, T.G. Macguire and P.P. Barros (eds.), *Handbook of Health Economics*, Volume 2, Elsevier 2012,499-637

Lustig, J., May, S., Noether, M. and B. Stearns, "Economic Tools for Analyzing Vertical Mergers in Healthcare," *Competition Policy International Antitrust Chronicle* (2020), https://media.crai.com/wp-content/uploads/2020/09/16164445/CPI-Lustig-May-Noether-Stearns.pdf (accessed January 13, 2020).

Massachusetts Health Policy Commission, Transaction List – Cost and Market Impact Reviews, https://www.mass.gov/lists/transaction-list-cost-and-market-impact-reviews (accessed January 13, 2022).
Massachusetts Health Policy Commission, Technical Bulleting for 958 CMR 7.00 Notices of Material Change and Cost and Market Impact Reviews, August 27, 2017, https://www.mass.gov/doc/final-958-cmr-700-technical-bulletin-0/download (accessed January 13, 2022).

Oregon Health Authority's review of health care entities' proposed material change transactions, proposed December 21, 2021 (to be codified at OAR 409-070-0000 through OAR 409-070-0085), https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/2021-12-21_409-070-NoticeFilingTrackedChanges.pdf.

Oregon Health Authority, Health Care Market Oversight Program sub-regulatory guidance: Criteria for OHA Use of Outside Advisors for Material Transaction Review, (January 2022), available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/Draft-Outside-Advisors-Criteria-20220121.pdf.

Oregon Health Authority, Health Care Market Oversight Program sub-regulatory guidance: Criteria for Community Review Boards, (January 2022), available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/Draft-Community-Review-Board-Criteria-20220121.pdf.

Oregon Health Authority, Health Care Market Oversight Program sub-regulatory guidance: Criteria for Comprehensive Review of Material Change Transactions, (January 2022), available at https://www.oregon.gov/oha/HPA/HP/HCMOPageDocs/DRAFT-Criteria-for-Comprehensive-Review_1.21.22.pdf.

Salop, S. and D. P. Culley, "Revising the U.S. Vertical Merger Guidelines: Policy Issues and an Interim Guide for Practitioners," *Journal of Antitrust Enforcement* 4, no. 1 (2016), 1-41.

Town, R. and G. Vistnes, "Hospital Competition in HMO Networks," *Journal of Health Economics* 20, no. 5 (2001), 733-753.
U.S. Department of Justice and the Federal Trade Commission, Horizontal Merger Guidelines, (2010), available at https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf

U.S. Department of Justice and the Federal Trade Commission, Horizontal Merger Guidelines, August 19, 2020, available at https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf.

U.S. Department of Justice and Federal Trade Commission, Statement of Antitrust Enforcement Policy Regarding Accountable Care Organizations Participating in the Medicare Shared Savings Program, October 28, 2011, available at https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf.

Version: August 2024

The Oregon State Legislature authorized APAC in 2009 to measure and improve the quality, quantity, cost and value of health care services. Oregon Revised Statutes and Administrative Rules provide guidelines for APAC data collection, use and release and the Oregon Health Authority (OHA) is responsible for APAC oversight. APAC contains protected health information and data that identifies people. OHA is responsible for ensuring compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the protection of people's health information, identity and privacy. OHA ensures that data requests comply with HIPPA, protect the privacy of members and their health information, are justified and that **OHA shares only the minimum necessary data.**

The purpose of the data elements workbook is for data requesters to specify APAC data options and data elements requested for their project described in their APAC3 application. OHA uses the data elements workbook and the APAC3 data request application to assess HIPPA compliance,risks and to determine if the projects meets the APAC data use and release guidelines.

Please return this completed worksheet along with your APAC data request application to apac.admin@odhsoha.oregon.gov

Please answer each of the following questions:

What is your study population? For example: people with an inpatient hospitalization, diabetes, pregnant substance use disorder, cancer etc	Our study population is the entire population of Oregonians who obtained health care between 2011 and 2022.
How is your study population defined? For example: by diagnosis, procedure and/or national drug codes, APAC grouper type, clinical categories (CCSR), BETOS, DRG, MDC etc.	As stated above, our study population is the entire population of Oregonians, hence it is not restricted by clinical characteristics such as diagnoses. However, we plan to examine if there are heterogeneous results for different patient groups, e.g. by their insurance types.
What are your specific independent variables, predictor variables?	Our research plans do not seek to test the hypotheses of relationships between specific independent and dependent variables. Rather, we intend to use the APAC data to analyze the state of competition in the Portland region for health care services, in accordance with OHA's Health Care Market Oversight (HCMO) Analytic Framework. For example, we plan to analyze patient choice, payor mix, service line offerings, patient draws, and competition among health care systems in the region for inpatient, outpatient and physician services. Please refer to our completed APAC Data Application for details.
What are your specific covariate variables?	Same as the above.
What are your specific dependent variables? Note that 'health outcome(s)' is not a specific dependent variable.	Same as the above.

Do you want claims and eligibility data for selected age groups only?	All ages	Exclude people 65 yrs and older	Specify age range:
	X		

Do you want to limit claims and eligibility data by sex/gender?	Include all	Only females	Only males
	X		

Please indicate the year(s) of data requested	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
	X	X	X	X	X	X	X	X	X	X	X	X

Do you want people who are not Oregon residents and their claims included? People with Medicaid coverage or Medicare Part A and Part B are Oregon residents regardless of address.	Yes	No
	X	

Do you want people with pharmacy coverage, but no medical coverage included?	Yes	No
		X

Do you want people with dental coverage, but no medical coverage included?	Yes	No
		X

Do you want orphan claims included? (claims, but no eligibility or coverage reported)	Yes	No
	X	

Do you want denied claims included? (No reason is provided for denied medical or pharmacy claims. Claims can be denied then paid)	Yes	No
	X	

What payer types do you want?	Commercial	Medicaid	Medicare (commercial Medicare Advantage and Part D only)	Medicare Part A and Part B (Available to OHA only)
	X	X	X	

One payer reported the claim status for all of their claims as fee-for-service for some years when most claims were encounter or managed care claims. Do you want the claim status changed to managed care?	Change to encounter	Do not change
	X	

Do you want APAC to correct payer reported errors for product codes, claim status, orphan status, COB status for member month and claims data?	Yes	No
	X	

What medical claim types do you want?	Inpatient hospital	Emergency department	Outpatient	Professional	Other
	X	X	X	X	X

Do you want to limit medical claims data to selected diagnoses, procedure or other codes?	No	Yes. Please list codes
	X	

Do you want substance use disorder claims (SUD)? SUD claims were not available for request prior to APAC release 14. SUD requests require detailed information about purpose, hypotheses and analyses, information about data access, security, data destruction and data linking to any other source and detailed justification for requested data elements. Date use and release of information are restricted. Requires additional Data Use Agreement	Yes	No
		X

Do you want APAC to calculate payer paid, member paid and total paid by claim and or claim line?	Yes-by claim ID	Yes-by claim line
	X	X

Do you want medical Coordination of Benefit (COB) claims?	No	Yes, when both the primary and secondary payer claims are linked	Yes,when the secondary payer claim does not link to a primary payer claim
		X	X

Do you want pharmacy claims?	Yes	No	Yes, but limited to these NDCcodes:
		X	

Do you want pharmacy claims for people with pharmacy coverage, but no medical coverage?	Yes	No
		X

Do you want APAC to calculate payer paid, member paid and total paid by claim for pharmacy claims?	No	Yes
	X	

Do you want dental claims?	Yes	No
		X

Do you want dental claims for people with dental coverage, but no medical coverage?	Yes	No
		X
Do you want APAC to calculate payer paid, member paid and total paid by claim line for dental claims?	Yes-by claim ID	Yes-by claim line
	N/A	N/A

Do you want monthly eligibility data (insured/covered by year, by month, by payer)?	Yes	No
	X	

Are you requesting identifiable data?	No	Zip code	County	Address	Name	Month of birth	Date of birth	CMS reported date of death (Available to OHA only)
		X	X					

Do you want provider data (rendering, prescribing, billing, pharmacy, hospital, ambulatory surgery center)?	Yes	No
	X	

Do you want APAC data linked to Oregon Center for Health Statitistics (CHS) Death Certificate data and/or Birth Certificate data? Please include a list of the birth and or death data variables that you plan to request from birth and/or death certificate data. You will need approval from both CHS and APAC. Submit request to APAC first. After APAC approval submit request to CHS and provide APAC approval notice. https://www.oregon.gov/oha/PH/BIRTHDEATHCERTIFICATES/VITALSTATISTICS/Pages/Data-Use-Requests.aspx	Yes	No
		X

Is your requested APAC data going to be linked by the APAC Team or data requester to any other data source?	No	Yes, linked by APAC	Yes, linked by data requester
	X		

Please **mark an X** in the Field Requested column to identify your requested data elements

Please delete the rows for data elements that you do not want for your project

Please **delete the Medical Claim tab** if you are not requesting any Medicaid Claims data elements

Refer to the APAC Data Dictionary for more detailed information about each data element

Field Requested	Data Element	Security Level	Description	Justification (Please provide reason needed and minimum necessary for project)
The data elements highlighted in blue are provided in every data request	uid	De-Identified	A unique identifier that links to the row as submitted in the MC Intake File Layout. Used for linking tables/views	
	release_id	De-Identified	A value associated with the data release	
	mc059_service_start_dt	De-Identified	Date services for patient started	
	dw_claim_id	De-Identified	A unique medical claim identifier	
	mc005_line_no	De-Identified	Line number for the claim that begins with 1 and is incremented by 1 for each additional service line of a claim	
	uniquepersonID	De-Identified	A unique identifier for a person across payers and time	
	dw_member_id	De-Identified	A payer & plan specific unique identifier for a person. A person can have multiple member IDs for a single payer because they can have multiple plans. DW_member_IDs are not unique identifiers for a person across payers and years	
	mc038_claim_status_cd	De-Identified	Claim status. P (Paid), D (Denied), C - (MCO/CCO encounter) E (other)	
	mc038a_cob_status	De-Identified	Coordination of benefit claim. Indicates secondary payer for a claim	
	orphan_fl	De-Identified	Identifies orphan claim with no corresponding eligibility for the date of service. 1 (Yes), 0 (No)	
	mc003_insurance_product_type_cd	De-Identified	A code that indicates an insurance coverage type. Data element required for linking claims to member months	
	Suppressed_Fl	De-Identified	1 (denied claim line), 0 (other than denied)	
	RemovedReversal_Fl	De-Identified	1 (claims not included before release 13 because the charge, paid amount, and allowed amounts are zero or zero when summed across claim lines and after the removal of denied claim lines, 0 (otherwise)	
X	mc060_service_end_dt	De-Identified	Date services for patient ended	To segment time-series analyses by date.
X	COB	De-Identified	Links primary and secondary payer claims based on uniquepersonID, date, charged amount, procedure code and provider and identifies the primary payer claim, secondary payer	To identify coordination of benefit claims.
X	Claim_LOB	De-Identified	Payer line of business: 1 (Medicare), 2 (Medicaid), 3 (commercial, 0 (no line of business reported)	To identify insurance type to segment commercial from non-commercial claims.
X	mc207_payment_type	De-Identified	Indicates the payment methodology: 01 (Capitation); 02 (Fee for Service); 07 (Other)	To identify capitated encounters, or other payment arrangements like pay for performance. If this field is not consistently populated, it can be excluded.

X	self_insured_fl	De-Identified	Self Insured flag	To identify self-insured commercial claims.
X	mc001_payer_type	De-Identified	Payer reported payer type codes:(C) Carrier, (D) Medicaid, (G) Other government agency, (P) Pharmacy benefits manager, (T) Third-party administrator, (U) Unlicensed entity	To identify insurance type to segment commercial from non-commercial claims.
X	mc018_admit_dt	De-Identified	Admission date	To segment time-series analyses by date.
X	mc203_admit_type_cd	De-Identified	Admission type:1 (Emergency), 2 (Urgent), 3 (Elective), 4 (Newborn), 5 (Trauma Center), 9 (missing)	To segment between emergent and elective care.
X	mc204_admission_source_cd	De-Identified	Admission source	To identify patients that are transferred to a hospital (and hence might not have a specific choice of facility).
X	mc205_admit_diagnosis_cd	De-Identified	Admitting diagnosis. ICD-10 diagnosis code for dates of service beginning 10/01/2015, ICD-9 diagnosis code for dates of service before 10/01/2015	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc070_discharge_dt	De-Identified	Discharge date-required for inpatient hospitalization	To segment time-series analyses by date.
X	mc023_discharge_status_cd	De-Identified	Status for member discharged from a hospital	To identify patient status at discharge (transferred, deceased, etc.) and possibly to determine patient need for post-acute care.
X	LOS	De-Identified	Length of stay of inpatient admission measured in days. Discharge Date - Admit Date. <1 is rounded to 1. Negative values set to NULL	To identify potentially higher-acuity inpatient discharges (i.e., higher LOS can be indicative of higher acuity for patients with the same MS-DRG).
X	mc036_bill_type_cd	De-Identified	Type of bill on uniform billing form (UB)	To segment by type of facility and type of care being sought (e.g., inpatient vs. outpatient).
X	mc037_place_of_service_cd	De-Identified	Industry standard place of service code	To segment by type of service site where professional services were rendered (e.g., inpatient setting vs. a physician clinic).
X	mc054_revenue_cd	De-Identified	Revenue code	To segment by type of service being sought or by department of service billing.
X	mc041_principal_diagnosis_cd	De-Identified	Principal Diagnosis code	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc042_other_diagnosis_2	De-Identified	Additional Diagnosis 2	To identify specific co-morbidities associated with a patient that might drive choice of provider.

X	mc043_other_diagnosis_3	De-Identified	Additional Diagnosis 3	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc044_other_diagnosis_4	De-Identified	Additional Diagnosis 4	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc045_other_diagnosis_5	De-Identified	Additional Diagnosis 5	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc046_other_diagnosis_6	De-Identified	Additional Diagnosis 6	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc047_other_diagnosis_7	De-Identified	Additional Diagnosis 7	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc048_other_diagnosis_8	De-Identified	Additional Diagnosis 8	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc049_other_diagnosis_9	De-Identified	Additional Diagnosis 9	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc050_other_diagnosis_10	De-Identified	Additional Diagnosis 10	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc051_other_diagnosis_11	De-Identified	Additional Diagnosis 11	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc052_other_diagnosis_12	De-Identified	Additional Diagnosis 12	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc053_other_diagnosis_13	De-Identified	Additional Diagnosis 13	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc201_icd_version_cd	De-Identified	Identifies ICD9 or ICD10 version	To help ensure we are using the appropriate ICD version.
X	mc055_procedure_cd	De-Identified	Current Procedural Terminology (CPT) code or Healthcare Common Procedure Coding System (HCPCS)	To identify specific procedures being sought by patients.

X	mc056_procedure_modifier_1_cd	De-Identified	CPT or HCPCS modifier	To identify the appropriate context of the specific procedure being sought by patients.
X	mc057_procedure_modifier_2_cd	De-Identified	CPT or HCPCS modifier	To identify the appropriate context of the specific procedure being sought by patients.
X	mc057a_procedure_modifier_3_cd	De-Identified	CPT or HCPCS modifier	To identify the appropriate context of the specific procedure being sought by patients.
X	mc057b_procedure_modifier_4_cd	De-Identified	CPT or HCPCS modifier	To identify the appropriate context of the specific procedure being sought by patients.
X	claim_type	De-Identified	Vendor generated claim ltype. Identifies claim lines as inpatient facility claim (1), outpatient facility claim (2) and professional claim (3) based on bill type, revenue code and place of service. Null means claim line type could not be determined.	To segment claims by facility type or professional services.
X	APACgrouper	De-Identified	Groups all lines of a claim in prioritized order as inpatient, emergency department, outpatient, professional, pharmacy and other based on type of bill, revenue and place of service codes	To help cross-reference to other fields in determining claim segmentation.
X	final_mdc	De-Identified	a code identifying the final Major Diagnostic Category (MDC)	To segment by type of service being sought in the inpatient setting.
X	final_drg	De-Identified	a code indentifying the final Diagnosis Related Group	To segment by type of service being sought in the inpatient setting.
X	CCSR grouper	De-Identified	AHRQ clinical classification software refined (500 categories)	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	CCS grouper	De-Identified	Clincal classification software (285 categories)	To identify specific co-morbidities associated with a patient that might drive choice of provider.
X	mc058_icd_primary_procedure_cd	De-Identified	The main inpatient procedure code	To identify specific procedures being sought by patients.
X	mc058a_icd_procedure_2	De-Identified	Inpatient procedure ICD-10 code 2	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.

X	mc058b_icd_procedure_3	De-Identified	Inpatient procedure ICD-10 code 3	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058c_icd_procedure_4	De-Identified	Inpatient procedure ICD-10 code 4	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058d_icd_procedure_5	De-Identified	Inpatient procedure ICD-10 code 5	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058e_icd_procedure_6	De-Identified	Inpatient procedure ICD-10 code 6	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058f_icd_procedure_7	De-Identified	Inpatient procedure ICD-10 code 7	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058g_icd_procedure_8	De-Identified	Inpatient procedure ICD-10 code 8	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058h_icd_procedure_9	De-Identified	Inpatient procedure ICD-10 code 9	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058j_icd_procedure_10	De-Identified	Inpatient procedure ICD-10 code 10	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.

X	mc058k_icd_procedure_11	De-Identified	Inpatient procedure ICD-10 code 11	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058l_icd_procedure_12	De-Identified	Inpatient procedure ICD-10 code 12	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc058m_icd_procedure_13	De-Identified	Inpatient procedure ICD-10 code 13	If available, this will be helpful to segment by type of service being sought. If not consistently populated, the principal procedure code field will be most helpful.
X	mc201_icd_version_cd	De-Identified	ICD version code 9 - ICD-9, 10 - ICD-10	To help ensure we are using the appropriate ICD version.
X	mc061_service_qty	De-Identified	count of units reported on claim line	To more accurately capture components of the final cost for services provided.
X	mc017_paid_dt	De-Identified	Payment date	To uniquely identify claim records.
X	mc062_charge_amt	De-Identified	Payer reported charges or billed amount for the service	Information on charges are helpful for analyses comparing prices to the extent we might have to run some validation exercises (e.g., examine observations where prices paid exceed charges to determine whether they are valid observations or ought to be excluded from the sample).
X	member paid amount claim line	De-Identified	Deduplicated member paid amount at claim line (sum of copayment, coinsurance and deductible or patient paid amt--whichever is larger)	To determine the net price faced by patients while choosing providers.
X	Payer paid amount claim line	De-Identified	Deduplicated payment made by payer	The paid amount is helpful in determining the net revenues accruing to each provider so the net savings can be estimated.
X	Total paid amount line	De-Identified	Sum of member paid amount and payer paid amount at claim line	Useful for validation of the patient portion and payer portion of the paid amount.

X	mc063_paid_amt	De-Identified	Payment made by payer	The paid amount is helpful in determining the net revenues accruing to each provider so the net savings can be estimated.
X	mc065_copay_amt	De-Identified	Expected Co-payment by the member	To determine the net price faced by patients while choosing providers.
X	mc066_coinsurance_amt	De-Identified	Expected Co-insurance by the member	To determine the net price faced by patients while choosing providers.
X	mc067_deductible_amt	De-Identified	Expected Deductible by the member	To determine the net price faced by patients while choosing providers.
X	mc067a_patient_paid_amt	De-Identified	Expected Patient paid amount. Combination of copayment,coinsurance and/or deductible	To determine the net price faced by patients while choosing providers.
X	mc202_provider_network_indicator	De-Identified	Indicator of service received in or out of network:1 (in network), 2 (National network), 3 (out-of-network)	To understand whether the payments associated with a claim that occur at a given provider are within the health plan network.
X	dw_rendering_provider_id	De-Identified	A unique identifier associated with a unique rendering provider across plans, payers and years.	To be used in conjunction with the Provider Composite table in order to identify the physician rendering each claim service line.
X	dw_billing_provider_id	De-Identified	A unique identifier associated with a unique billing provider across plans, payers andyears.Can be linked to dw_provider_ID in provider data	To be used in conjunction with the Provider Composite table in order to identify the physician billing each claim service line.
X	rendering_hospital_id	Limited	Hospital that rendered services	To identify the hospital rendering each claim service line.
X	hospital_name	De-Identified	Name of Oregon Hospital	To identify the hospital rendering each claim service line.
X	billing_hospital_id	Limited	Hospital billed for services	To identify the hospital billing each claim service line.
X	rendering_asc_id	Limited	Ambulatory surgery center that rendered services	To identify the ASC rendering each claim service line.
X	ASC_name	De-Identified	Name of Oregon Ambulatory Surgery Center	To identify the ASC rendering each claim service line.
X	billing_asc_id	De-Identified	Ambulatory surgery center billed or services	To identify the ASC billing each claim service line.
X	age	De-Identified	Age on date of service	To understand the demographic characteristics of patients served by different providers.

X	me013_member_gender_cd	De-Identified	member's gender F = Female, M = Male, U = Unknown	To understand the demographic characteristics of patients served by different providers.
X	urban_fl	De-Identified	Zip codes grouped into urban and rural identified by OHA	To segment by available geographic information.
X	member_zip_three	De-Identified	First three characters of member zip code from the date of service	The member's zip code of residence is needed for determining travel distance of the patient to various provider options. We are requesting this in addition to the 5-digit zip code, which is the standard geographic variable used in defining hospital service areas.
X	interim_fl	De-Identified	Flag identifying interim bills	To segment by claim type and final claim status.
X	interim_claim_id	De-Identified	Unique identifier set by DW_Claim_ID of the initial interim claim	To segment by claim type and final claim status.
X	MCAID_Claim_Type	Limited	Medicaid claim type: I=inpatient, M=professional, B=professional crossover, C=outpatient crossover, A=inpatient crossover, O=outpatient, L=long term care, Q = compound pharmacy, D=dental	To segment by claim type.
Data elements that are frequently denied				
X	payer_cd	Sensitive	Payer name abbreviation code	To identify unique payers and to segment commercial from non-commercial insurance products to appropriately focus the scope of the analyses.
X	mc062a_allowed_amt	Limited	Allowed amount	This field will be used to calculate the price charged by each provider for each service, where the price is estimated as the negotiated allowed amount paid per service, with adjustments for the intensity of services provided.

Please **mark an X** in the Field Requested column to identify your requested data elements

Please delete the rows for data elements that you do not want for your project

Please **delete the EligibilityMemberMonth tab** if you are not requesting any eligibility month data elements

Refer to the APAC Data Dictionary for more detailed information about each data element

Field Requested	Data Element	Security Level	Description	Justification (Please provide reason needed and minimum necessary for project)
The data elements highlighted in blue are provided in every data request	uid	De-Identified	A unique identifier that links to the row as submitted in the MM Intake File Layout. Used for linking tables/views	
	release_id	De-Identified	A value associated with the data release	
	year_Eligibility	De-Identified	Year of eligibility	
	month_Eligibility	De-Identified	Month of eligibility	
	dw_member_id	De-Identified	A unique identifier associated with a single plan and payer and assigned to all eligibility and claims records associated with a given individual for that plan/payer. An individual can have multiple member ids for a payer because they can have multiple plans.	
	uniquepersonID	De-Identified	A unique identifier for a person across payers and time	
	me003_insurance_product_type_cd	De-Identified	A code that indicates an insurance coverage type	
	me018_medical_coverage_flag	De-Identified	Medical Coverage Flag not required when ME001=E	
	me019_prescription_drug_coverage_flag	De-Identified	Prescription Drug coverage flag	
	me207_dental_coverage_flag	De-Identified	Flag indicates dental coverage for the month	
	member_state	De-Identified	People with Medicaid coverage and people with Medicare coverage reported by the Centers for Medicare & Medicaid Services are Oregon residents regardless of reported address	
X	Month_Start	De-Identified	Date of Eligibility set to the first of the month	To identify each patient's insurance plan and/or status by time period.
X	Me005a_plan_term_dt	De-Identified	Plan termination date	To identify each patient's insurance plan and/or status by time period.
X	LOB	De-Identified	Payer line of business: 1 (Medicare), 2 (Medicaid), 3 (commercial, 0 (no line of business reported)	To identify insurance type to segment population, for example to study payor mix.
X	MedicareType	De-Identified	Medicare Advantage (Part C and/or PartD) or MedicareFFS (Medicare Fee-for-service-Part A, B and/or D)	To identify insurance type to segment commercial from non-commercial claims.

X	DualMedicareMedicaid	De-Identified	Medicaid and Medicare coverage same month, year	To identify insurance type to segment commercial from non-commercial claims.
X	RXnomedicalMM	De-Identified	Pharmacy coverage and no medical coverage during same year, month	To identify insurance type.
X	DentalnomedicalMM	De-Identified	Dental coverage and no medical coverage during same year, month	To identify insurance type.
X	me009a_pebb_flag	De-Identified	Public Employees Benefit Board covered members Oregon includes out-of-state residents	To identify insurance type to segment population, for example to study payor mix.
X	me009b_oebb_flag	De-Identified	Oregon Educators Benefit Board covered members Oregon includes out-of-state residents	To identify insurance type to segment population, for example to study payor mix.
X	me201_medicare_coverage_flag	De-Identified	Type of Medicare coverage for Medicaid members only. A - Part A, B - Part B, AB - Parts A and B, C - Part C, D - Part D, CD - Part C and D, X - other, Z - none, not required when ME001=E	To identify insurance type to segment commercial from non-commercial claims.
X	me012_member_subscriber_rlp_cd	De-Identified	Relationship code	To understand the source of each patient's insurance coverage.
X	me013_member_gender_cd	De-Identified	Member Gender:M (male), F (female), and U (unknown)	To understand the demographic characteristics of patients served by different providers.
X	yob	De-Identified	Year of Birth from Member_DOB field from Member DAV. If no date of birth has been reported, NULL	To understand the demographic characteristics of patients served by different providers.
X	me009d_omip_flag	De-Identified	Flag indicates Oregon Medical Insurance Pool (OMIP) coverage for the month	To identify insurance type to segment commercial from non-commercial claims.
X	me202_market_segment_cd	De-Identified	Market Segment	To identify insurance type to segment population, for example to study payor mix.

X	me203_metal_tier	De-Identified	Health benefit plan metal tier for qualified health plans (QHPs) and catastrophic plans as defined in the ACA:0 (Not a QHP or catastrophic plan), 1 (catastrophic), 2 (bronze), 3 (silver), 4 (gold), 5 (platinum)	To understand the level of generosity/coverage of the health plan.
X	me205_high_deductible_health_flag	De-Identified	High Deductible Health Plan Flag	To understand the level of generosity/coverage of the health plan.
X	me206_primary_insurance_ind	De-Identified	Flag indicates primary insurance	To identify primary source of payment and coordination of benefits.
X	MCAID_cde_medicare_status	De-Identified	Medicare status reported for Medicaid recipients: MA (Part A only), MAB (Part A & B), MABD (Part A,B&D), MAD (Part A & D), MB (Part B only), MBD (Part B & D), MD (Part D only)	To identify insurance type to segment commercial from non-commercial claims.
X	MCAID_cde_enroll_recip_status	De-Identified	Medicaid enrollment status: managed care enrolled cap payment (1), managed care enrolled no cap payment (3), not managed care enrolled cap payment (5), fee for service (6) or null	To identify insurance type to segment commercial from non-commercial claims.
X	urban_fl	De-Identified	Zip codes grouped into urban and rural identified by OHA	To segment by available geographic information.
X	member_zip_three	De-Identified	First three characters of member zip code from the date of eligibility	The member's zip code of residence is needed for determining travel distance of the patient to various provider options. We are requesting this in addition to the 5-digit zip code, which is the standard geographic variable used in defining hospital service areas.
X	rarestre	De-Identified	The rarest race-ethnicity identified for a person across payers and years (only one identified per person): (P) Native Hawaiian or Pacific Islander, (B) Black or African American, (I) American Indian or Alaskan Native, (A) Asian, (H) Hispanic or Latino, (W) White, (O) other and (noRE) no race-ethncity reported	To understand the demographic characteristics of patients served by different providers.
X	re1_race_cd	De-Identified	All races reported by all payers for all years for a person: (P) Native Hawaiian or Pacific Islander, (B) Black or African American, (I) American Indian or Alaskan Native, (A) Asian, (W) White, (O) other, (U) unknown, (R) refused and null	To understand the demographic characteristics of patients served by different providers.

X	re2_ethncity_cd	De-Identified	All ethnicities reported by all payers for all years for a person: (H) Hispanic), (O) Not Hispanic, (U) unknown, (R) refused and null	To understand the demographic characteristics of patients served by different providers.
X	re3_primary_language_cd	De-Identified	All primary spoken languages reported by all payers for all years for a person	To understand the demographic characteristics of patients served by different providers.
Data elements that are frequently denied				
X	payer_cd	Sensitive	Payer name abbreviation code	To study differences in pricing by pairs of payer and provider.
X	me015_member_city_nm	Limited	Member City from the date of eligibility	This provides an additional dimension of geographic detail to understand the patients' choice of providers.
X	HSAcity	De-Identified	HSA City field from the Darmouth Atlas Zip Code Crosswalk	This provides an additional dimension of geographic detail to understand the patients' choice of providers.
X	me017_member_zip	Limited	Zip code-from the date of eligibility	We need the 5-digit zip code since it is the standard geographic variable used in defining hospital service areas. Also, the member's zip code of residence is needed for determining travel distance of the patient to various provider options.
X	county_fips	Sensitive	Five digit Federal Information Processing Standard (FIPS) county code associated with me017_member_zip	This provides an additional dimension of geographic detail to understand the patients' choice of providers.

Please delete the rows for data elements that you do not want for your project

Please **delete the Provider Composite tab** if you are not requesting any provider data elements

Refer to the APAC Data Dictionary for more detailed information about each data element

Field Requested	Data Element	Security Level	Description	Justification (Please provide reason needed and minimum necessary for project)
Provided in every data request	release_id	De-Identified	A value associated with the data release	
X	dw_provider_id	De-Identified	A unique identifier associated with a unique provider across plans and payers	To link the Provider Composite table information to either the rendering or billing provider of the claim service lines in the Medical Claims data.
X	provider_entity	De-Identified	Provider entitiy-1) Individual or 2) organization	To identify whether the provider is an individual or an organization.
X	national_provider_id	De-Identified	National Provider Identifier (NPI)	The NPI is a provider's internal identifier key with the NPPES linking them to a primary practice location and licensed taxonomy information.
X	provider_tax_id	De-Identified	Provider Tax identifier (attending, billing, pharmacy)	This field is useful in determining the type of provider.
X	license_1	De-Identified	Provider state license code number 1	Useful in determining the state in which the provider is licensed to provide healthcare services.
X	license_state_1	De-Identified	State where provider license number 1 was granted	Useful in determining the state in which the provider is licensed to provide healthcare services.
X	Provider_First_Nm	De-Identified	Provider first name; null if provider is an organization entity (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.

X	Provider_Middle_Nm	De-Identified	Provider middle name or organization name (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Last_Nm	De-Identified	Provider last name or organization name (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Suffix	De-Identified	Suffix of provider name	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Org_Nm	De-Identified	Name of provider's organization	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Prefix	De-Identified	Prefix of provider name	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Org_Nm_Other	De-Identified	Other name of organization	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Last_Nm_Other	De-Identified	Other last name of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_First_Nm_Other	De-Identified	Other first name of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Middle_Nm_Other	De-Identified	Other middle name of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Prefix_Other	De-Identified	Other prefix of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Provider_Suffix_Other	De-Identified	Other suffix of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	primary_street	De-Identified	Provider street address (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.
X	primary_city	De-Identified	Provider city (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.
X	primary_state	De-Identified	Provider state (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.

X	primary_zip	De-Identified	Provider location zip (attending, billing, pharmacy)	To identify the healthcare provider performing services in the Medical Claims data.
X	Credential_Text_1	De-Identified	Provider NPI credential 1	To identify the type of healthcare provider.
X	Credential_Text_2	De-Identified	Provider NPI credential 2	To identify the type of healthcare provider.
X	Credential_Text_3	De-Identified	Provider NPI credential 3	To identify the type of healthcare provider.
X	provider_gender	De-Identified	Gender of provider - U if unknown	To identify the healthcare provider performing services in the Medical Claims data.
X	Taxonomy_Cd_1	De-Identified	NUCC provider taxonomy for the billing provider; NPI if not reported	To identify the type and specialty of healthcare provider.
X	Taxonomy_Cd_2	De-Identified	NUCC provider taxonomy for the billing provider; NPI if not reported	To identify the type and specialty of healthcare provider.
X	Taxonomy_Cd_3	De-Identified	NUCC provider taxonomy for the billing provider; NPI if not reported	To identify the type and specialty of healthcare provider.
X	Taxonomy_Cd_4	De-Identified	NUCC provider taxonomy for the billing provider; NPI if not reported	To identify the type and specialty of healthcare provider.
X	Taxonomy_Cd_5	De-Identified	NUCC provider taxonomy for the billing provider; NPI if not reported	To identify the type and specialty of healthcare provider.
X	Taxonomy_grouping	De-Identified	Code that indicates provider specialty or taxonomy 1	To identify the type and specialty of healthcare provider.
X	Taxonomy_classification	De-Identified	Taxonomy classification	To identify the type and specialty of healthcare provider.
X	Taxonomy_specialization	De-Identified	Taxonomy specialization	To identify the type and specialty of healthcare provider.
X	Addr_Type	De-Identified	Address type of provider (B) Business, (L) Location, (S) Secondary Location, (I) Provider Index	To identify the healthcare provider performing services in the Medical Claims data.

X	Addr_Street_1	De-Identified	Address of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Addr_Street_2	De-Identified	Address 2 of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Addr_City	De-Identified	City of Provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Addr_State	De-Identified	State of provider	To identify the healthcare provider performing services in the Medical Claims data.
X	Addr_ZIP	De-Identified	ZIP Code of provider - may include non-US codes	To identify the healthcare provider performing services in the Medical Claims data.

MarshMcLennan

CONFIDENTIALITY STATEMENT AND AGREEMENT

The information contained herein is the confidential and proprietary information ("Confidential Information") of Marsh McLennan Companies, Inc. and its businesses ("MMC"). ***By continuing to open and read this document, you agree that you have read and understand the below terms and that you are entering into this agreement on behalf of your company, and you represent that you have the authority to bind your company to these terms:***

1. Your company may use the MMC Confidential Information for the sole purpose of evaluating MMC's data security controls (the "Purpose.") Your company will hold all MMC Confidential Information in confidence, using at least the same degree of care it employs to avoid unauthorized disclosure of its own information of a similar nature, and it will not disseminate, transfer, or otherwise disclose any MMC Confidential Information or make it available to any third party except to its affiliates and service providers who have a need to know for the Purpose. Your company shall be responsible for its affiliates and service providers' use of the MMC Confidential Information.

2. In the event of any unauthorized disclosure or loss of any MMC Confidential Information, your company will promptly (a) notify MMC at IncidentReporting@mmc.com and give MMC all known details; and (b) take such actions as may be necessary or reasonably requested by MMC to address and minimize the disclosure or loss and any damage resulting there from;

3. As between MMC and your company, MMC is the sole and exclusive owner of MMC Confidential Information contained herein, and, upon termination of your company's review of MMC's Confidential Information, or at any other time requested by MMC, your company shall destroy the MMC Confidential Information in its or its affiliates and service providers' possession; provided, however, that your company may retain copies of MMC Confidential Information as required by applicable law; and

4. This agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all written or oral prior agreements, understandings, and negotiations with respect to such matters. This agreement shall be governed by the laws of the State of New York, without regard to its choice of law principles. This agreement shall be binding on, and apply to, the parties herein and their respective successors and assigns. If any provision of this agreement is declared void or unenforceable, such provision shall be deemed to be severed from this agreement, which otherwise shall remain in full force and effect.

If you do not agree to the above terms, please close this document and delete any and all copies from your systems.

MarshMcLennan

Marsh McLennan

INFORMATION AND CYBER SECURITY PROGRAM

MAY 2024

This *Information and Cyber Security Program* guide follows the structure of guidelines for information security programs promulgated by organizations such as the International Organization for Standardization (ISO), and the National Institute of Standards & Technology (NIST), the most common security standards that many companies use as frameworks for their information and cyber security programs.

Contents

Disclaimer

Unless specifically stated otherwise, the policies, procedures, standards, and guidelines described herein apply to Marsh McLennan Companies, Inc., and its businesses as a whole - Marsh, Guy Carpenter, Mercer, and Oliver Wyman Group (collectively ”MMC”, “Marsh McLennan” or "our company"). Please note that the contract(s) between our clients and our business unit(s) contain the scope of services provided and the related legal, data privacy, and information security terms governing the relationship and associated liabilities. The contents of this document are for informational purposes only, and our company makes no warranty and disclaims any terms or statements contained herein that seek to impose legal or operational requirements on our company for the delivery of any services to the extent not otherwise addressed in any existing contract between us.

The information provided herein is subject to change without notice and is deemed our proprietary and Confidential Information. Please also note that any Yes/No responses must be interpreted in the context of the supplied comments and qualifications, and given the diversity and complexity of the services, will not be absolute or applicable in all instances. The explanation and/or any supporting documentation we provide to you may comprise our company's full response and control regardless of the Yes/No response.

1 - Business Overview

Our company is committed to cybersecurity and data protection, establishing internal controls that will comply with business and regulatory requirements, and protecting our information assets, including the confidential and personal information that clients entrust to us. These administrative, technical, and physical security measures, which include related planning, development, and implementation of documented policies, procedures, standards, and guidelines, are reviewed periodically, and updated where applicable to help maintain the confidentiality, integrity, availability, and security of company and client information.

This Information and Cybersecurity program document (the “Program” is structured using the control category order used within the Standardized Information Gathering (SIG) questionnaire from the Santa Fe Group (e.g., section main headers align to the SIG’s main control categories). While this program document will not cover all your questions, it intends to provide information related to the care and handling of information and information technology (IT) assets used within and by our company. The policies, procedures, standards, and guidelines described herein will assist you in assessing our enterprise-wide compliance, privacy, and information and cyber security practices. In some cases, it also addresses some related areas such as privacy and compliance, where appropriate.

Services provided to you may include your access to certain application systems or technology solutions developed and hosted by our business units within company data centers and/or private cloud tenants, however, our company does not provide commercial cloud services, commercial IT support services, commercial co-location/hosting services, or commercial software development services to clients. See also Section 16 – Cloud Services.

The services you may receive do not include client-exclusive or dedicated servers, data center rack space, network infrastructure, application infrastructure, or related IT management services (i.e., services and related applications or technologies that may be included are provided on a "shared" or “multi-tenant” basis).

Our company's network and data center infrastructure are managed by our company's dedicated technology infrastructure organization (“MMC Tech”). Applications hosted within our own or co-located data centers are maintained by our company’s business units' dedicated solutions delivery or application technology teams that are also part of MMC Tech, which may be supplemented by third-party development services and support providers.

Application systems developed and hosted in support of client services may be internal only or may be Internet-facing and accessible by our clients. Internet-facing systems employ a “defense in depth” approach including network segregation and multiple servers, both physical and virtual, running on either Microsoft Windows, RedHat Linux, Oracle Linux, or Oracle Solaris among other variants of Unix/Linux operating systems.

We utilize a variety of commercially recognized and globally supported software, information technology, and security products and platforms to support our security and technology operations, including but not limited to (and subject to change without notice) products from Cisco, Juniper, Microsoft, Crowdstrike, Palo Alto, ProofPoint, Qualys, Zscaler, and more.

Various business unit services involve the collection, processing, and storage of confidential and/or personal data or personal information provided by clients to our company. Data and information exchanged with our company may be processed and stored within internal electronic file repositories and/or within various structured application databases or systems, depending on the services from one or more of our business units. *For more information about the specific types of data or data elements, and application systems or technology used within the scope of services you may be receiving from one or more of our business units, please contact your business unit consultant or client relationship manager(s).*

1.1 Policies, Procedures, and/or other assurance materials

Our company's internal policies, procedures, standards, technical and other documentation are considered proprietary and confidential and are not distributed outside of our company or made available for copy by external parties. However, below is a brief outline of various company compliance and information technology security policies, procedures, and standards (see also Section 12– Business Ethics and Corporate Governance).

- The Greater Good – our code of conduct – covers various aspects of working at MMC and for our clients, including maintaining confidentiality of client data and information and an employee's obligations therein. A copy of The Greater Good (our Code of Conduct) is publicly available on the Marsh McLennan website at http://integrity.mmc.com.
- Compliance and Ethics Policies, Procedures, Guidelines and Standards
  - Handling Information Appropriately Policy, including:
    - Using Company Information and Technology
    - Protecting Personal Information
    - Retaining Records and Records Retention Schedules
  - Information Classification Standard and Unified Information Handling Guidelines
  - Global De-Identification Standard
  - Global Public-Facing Website and Application Standard
  - Cyber Incident Response Standard
- Annual Privacy and Security Training and awareness programs
- Human Resources practices and procedures related to background screening, new hire onboarding, and employee training.
- Business Resiliency Management Policy
- Safety and Physical Security Policies, Procedures and Standards
  - Architectural considerations
  - Emergency planning
  - Office physical security including but not limited to electronic access control systems, CCTV, and visitor access.
  - Protection of Company assets
  - Workplace and personal safety
- Global Information Security Policies, procedures, and standards applicable to our company's IT infrastructure:
  - IT Policies
    - *Identify*
      - Asset Management
      - Business Environment
      - Governance
      - Risk Assessment
      - Risk Management Strategy
      - Supply Chain Risk Management
    - *Protect*
      - Identity Management and Access Control
      - Awareness and Training
      - Data Security
      - Information Protection Processes and Procedures
      - Maintenance

        - Protective Technology

    - *Detect*
        - Anomalies and Events
        - Security Continuous Monitoring
        - Detection Processes

    - *Respond*
        - Response Planning
        - Communications
        - Analysis
        - Mitigation
        - Improvements

    - *Recover*
        - Recovery Planning
        - Improvements
        - Communications

- IT Standards
    - Access Control
    - General Logging and Security Information Event Monitoring (SIEM)
    - Cybersecurity Risk Assessment
    - Secure Access Standard
    - Kubernetes Network Policies Standards
    - Third-Party Connectivity
    - Bluetooth Security
    - Secure Application Hosting
    - Encryption Management and Security Ciphers
    - Wireless LAN Security Standard
    - Securing VoIP Technology
    - IoT Devices
    - Company Systems Usage Warning Banner
    - Desk and Screen Standard
    - File Transfer and Connectivity Standard
    - Email Auto Forwarding Standard

Who approves the Company's policies?

These policies are approved by senior management, which may include the Company's Compliance Leaders, Global Chief Privacy Officer, Chief Information Security Officer, Legal Department, and other senior executive leaders. Company policies and procedures also allow the Company to take disciplinary action for violation of the policies, up to and including termination of employment or contract for services.

How often are your policies reviewed and updated?

The Company's policies are subject to periodic review by Legal & Compliance, Information Security, and/or other pertinent executive management teams and are updated as needed based on applicable changes to privacy laws and regulations.

Can I obtain a copy of the Company's privacy and data protection policy (or policies)?

The Company's privacy notices are linked at the bottom of our websites, as applicable. In addition, The Greater Good, Corporate Governance documents, and Government Relations Conduct & Policies

can be viewed at www.marshmclennan.com under the ‘About’ tab. Other policies or summaries thereof may be available through your service representative.

2 - Enterprise Risk Management

Is a documented risk governance plan approved by management that defines the Enterprise Risk Management program requirements?

Various teams coordinate our company’s risk management, compliance, and information security programs.

These independent teams develop, implement, and maintain our Compliance policy programs and training, business resiliency/continuity and disaster recovery, and information security programs. These teams also support our business units by providing advice on and enforcing the implementation of risk assessment and management activities, information security frameworks, solutions, and procedures, and liaise with business, internal audit, and IT staff to identify, assess, and mitigate risks including that of third-party providers, and monitoring and detecting security incidents in our technology environment.

Such reviews or assessments are carried out periodically (monthly, quarterly, annual, or on-demand or ad-hoc basis) depending on the type of assessment and reported to applicable internal management and internal stakeholders.

Our company does not distribute, share, or discuss the reports or results of the reviews and assessments described above with clients or other external parties.

Is there a documented third-party risk management program in place for the selection, oversight, and risk assessment of fourth parties (e.g., subcontractors, suppliers, service providers, dependent service providers, sub-processors)?

Our company has procedures in place to assess the information and cyber security practices of third-party service providers (e.g., subcontractors, suppliers, or vendors), as well as other related areas such as privacy and compliance, using questionnaires, meetings, and inspections as deemed necessary by our company and subject to applicable legal and regulatory requirements. Access to data or company systems by such third parties is permitted only after the completion of a risk assessment. Periodic reassessments of a third party’s security measures are performed using a risk-based approach.

Review of third-party contracts and service agreements can include review by our Legal & Compliance, information security, IT internal audit, and other teams as appropriate. Upon such review, contracts will include relevant terms and conditions commensurate with the types of services provided by the third party (including contract and temporary personnel).

Does the Enterprise Risk Management Program include measures for defining, monitoring, and reporting risk metrics?

The condition of information security is actively monitored and reported to senior management and the board of directors regularly.

Do you permit clients to perform audits or inspections of your policies, procedures, and/or facilities?

Subject to reasonable limitations, and contractual terms and conditions, including but not limited to confidentiality and non-disclosure terms, restrictions on physical and/or logical access within our offices and data centers, and to documentation, reports, and other material, clients and prospective clients may perform risk assessments of our information and cybersecurity policies and procedures applicable to the services being received.

Does the organization perform independent reviews of its approach to information security management?

Reviews of our company's approach to information security management are conducted by our internal IT auditors as part of their annual audit plan which is derived from their annual risk assessment. Information Security is also assessed by our company's external auditors as part of Sarbanes-Oxley S404 reviews. MMC will also periodically engage with a third-party accessor to measure the MMC security program maturity against industry benchmarks.

Have operations been audited for compliance with privacy laws/regulations (e.g., GLBA, HIPAA)?

Yes, compliance and internal audit reviews are performed on a periodic, risk-based approach, to assess compliance with regulatory requirements such as CCPA, GLBA, GDPR, HIPAA, the NYDFS Cybersecurity Regulation, and Sarbanes-Oxley. Audit reports include findings and management remediation plans that are intended to address any gaps that are identified. Results are reported to senior management and periodic updates from Internal Audit are provided to our Audit Committee.

Regular assessments of our internal financial reporting controls are conducted according to the framework for public companies set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework and the PCAOB criteria for external auditors of financial statements and related information.

Are operational controls independently audited periodically by internal or external auditors?

Marsh McLennan's information technology infrastructure organization ("MMC Tech") retains the services of an external audit firm to perform a SSAE 18 SOC 2 Security Type II audit and report the results on an annual basis. The report represents technical, administrative, and security controls designed and implemented by MMC Tech, and MMC Global Information Security (GIS) to secure infrastructure services that MMC delivers to our businesses and functions from strategic data centers servicing the Americas, EMEA, and Asia Pacific regions. Current and prospective clients of a Marsh McLennan business unit can contact their business consultant or account relationship manager to request the *MMC Trust Package*, which includes the MMC Tech SOC 2 report and other company Information Security Policy documents and materials. Subject to appropriate confidentiality/non-disclosure terms and confirmation that business services delivered to the client rely on MMC Infrastructure delivered from a data center in scope, the Trust Package will be released directly to the client or prospective client following verification of confidentiality terms.

In addition to the MMC Tech SOC 2 report for infrastructure services, security audits, and reviews are performed by MMC's Internal Audit function and some MMC business units may retain an external auditor for a SSAE18 SOC x, ISAE3402, AAF 01/06 or equivalent. *Please contact your Marsh, Guy Carpenter, Mercer or Oliver Wyman business consultant or account relationship manager to discuss whether the specific services you receive from one of our business units are covered by an attestation or certification from an external party.*

Does the organization have an insider risk management policy or program?

Our company has a dedicated Insider Risk Management program and team that identifies, investigates, and raises awareness of potential damage to the firm by malicious (intentional or unintentional) insiders. This program is built in collaboration with Legal, Employee Relations, and Human Resources.

See also Section 2 - Requests for Policies, Procedures and/or other assurance materials for a list of related policies and procedures that support insider risk management.

Does the organization maintain cyber security insurance?

Our company maintains Cyber insurance. Our cyber insurance includes first-party coverage, such as coverage for breach management expenses, as well as third-party liability coverage.

* *Due to the ever-changing cyber insurance market, our company cannot guarantee this type of coverage within multi-year agreements executed between you and our business units.*

3- Information Security

3.1 Organization of Security

Does the organization, vendor, or service provider have a dedicated information security division/group?

Our company has a dedicated MMC Chief Information Security Officer (CISO) who is responsible for our company's cybersecurity program and IT infrastructure operations and manages the Global Information Security (GIS) and IT operations teams. The CISO reports to our company's Global Chief Information Officer (CIO) and works closely with Legal & Compliance, Privacy Risk Management teams, and business unit CIOs and CISOs.

GIS is comprised of information security professionals who are responsible for a variety of areas including:

- business unit CISOs (Marsh, Guy Carpenter, Mercer, Oliver Wyman, and IT Shared Services)*;
- security engineering and architecture;
- IT and cyber risk management;
- application security;
- cyber security incident response and investigations;
- cyber security operations;
- security governance including information security policy management, training and awareness, and metrics reporting; and
- supply chain (vendor) IT/cyber security risk management.

**Our business unit CISOs report to MMC CISO and are responsible for assuring the MMC information security program is successful within their respective business unit.*

Are new processing facilities reviewed and approved by the security organization to confirm that all relevant security policies and requirements are met?

Defined technology onboarding processes are used to manage the introduction of new information-processing systems and facilities. These processes employ standard work steps to verify that all aspects of management authorization, system requirements, and communication are completed before new systems are introduced. All systems changes are covered by a documented change-control procedure.

3.2 Information Security Policies

Are comprehensive and documented information security programs and policies in place?

Our company has and maintains documented internal policies and procedures that support the organization's information confidentiality, integrity, availability, and security objectives, and covers management and security of the internal systems used by us as well as operations and systems supporting services provided to clients. In some cases, individual business units may implement additional or more stringent policies and procedures that supplement our company policies, including to address specific regulatory or business requirements applicable to those services.

These policies and procedures are based on common cybersecurity frameworks and industry standards including but not limited to ISO/IEC 27001 and the NIST Cybersecurity Framework (NIST CSF). They outline responsibilities and requirements for the acceptable use of company computing systems, access controls and password use, handling, processing, and safeguarding of confidential information, including personal information and sensitive data, and compliance with applicable laws and regulations.

Our company's policies and procedures outline the roles and responsibilities of our colleagues and allow us to take disciplinary action for violation of the policies, up to and including termination of

employment or contract for services. Our company also recognizes the importance of protecting and managing personal information. As such, there are policies, programs, and procedures in place to protect company and client personal information from loss or misuse, and to comply with applicable data privacy laws.

For more information, please also refer to the Documentation *section above.*

Are security policies approved by senior management?

Information Security and Compliance policies are approved by senior management, which may include Legal & Compliance leaders, corporate and business unit Chief Information Security Officer(s), and our technology policy council.

How often are the policies reviewed and updated?

Our company's *IT Information Security Policy* is reviewed, and updated as needed, on an annual basis by Global Information Security (GIS). Other security standards and Information Technology (IT) operating procedures are reviewed regularly and updated on an as needed basis by GIS, Legal & Compliance, MMC Tech, and/or other pertinent management teams. In addition, internal IT audits consider the relevant policies within a given assessment which may provide recommendations for additional policy review and/or updates as a result.

How are policy exceptions handled?

Exceptions are expected to be temporary with a defined period of deviation from a policy, standard, or process. Exceptions are expected to be recorded in our risk register and managed by our IT and Cyber Risk Management function. Most risks require explicit approval from the relevant Technology Product Manager (if applicable), impacted business owner, and Business Chief Information Security Officer (BCISO). Higher severity risks and/or permanent exceptions require additional approvals which may include the CIO, COO, CEO, CISO, CPO, and other senior executives.

Are security policies communicated to all relevant parties including employees, contractors, and other third parties?

Awareness of our company's information security policies and practices is provided through multiple communication channels which include annual mandatory cybersecurity and privacy training, corporate materials such as our employee handbooks, as well as through periodic information security and compliance awareness campaigns through channels such as emails, newsletters, intranet postings, and through more proactive measures such as employee phishing awareness campaigns.

Third parties that have access to company data or systems are notified of our information security and data protection requirements through terms and conditions outlined in the contracts executed with these third parties, as may apply to the services received from the third party (including contractors and temporary personnel) and taking into account the sensitivity of the data they will collect, process and store. Review of third-party contracts and service agreements typically includes members of our Legal & Compliance, information security, IT internal audit, and other teams as appropriate.

3.3 Network Security

Is your network separated from the Internet by a firewall?

Our company has adopted a "defense in depth" approach to segregate areas of our network to protect client and company information from intruders on the Internet.

Our company's firewall architecture consists of multiple pairs of redundant FIPS-certified firewalls and various DMZs that isolate and segregate networks, including stateful inspection, logging, monitoring, and stealth rules. These rules are created within the change control framework and are reviewed by the appropriate management and security personnel before implementation, and they are tested by IT Internal Audit during various information security reviews.

We also utilize Software Defined Wide Area Networks (SDWAN), to securely connect remote offices using Direct Internet Access (DIA) access circuits for transport, and a cloud-based security suite (e.g., Zscaler), which is used to secure local browsing and enable secure application access.

Are all firewall rules reviewed and updated periodically to identify and remove any networks, subnetworks, hosts, protocols, or ports no longer in use?

While our company does not conduct scheduled periodic reviews of all firewall rules, a decommissioning process is in place with a detailed review undertaken by our company's global Cyber Security Operations Center (CSOC), following the requirements of the change management process. Our company removes any networks, sub-networks, hosts, protocols, or ports no longer in use as part of a detailed decommissioning process managed under the global change management process.

Do you have a service or mitigation plan to continue to make the service available to customers during a denial of service (DDOS) attack?

Our company has deployed a DDoS protection solution to all company locations with web hosting. The solution utilizes a multi-layered, hybrid approach that includes on-premises protection for application-level attacks, and a cloud scrubbing service to protect our network from volumetric attacks.

Are separate tiers employed for web servers, application servers, and database servers?

Separate physical or logical tiers are employed to segregate web and application servers from database servers. Similarly, in our cloud-hosted environments, logical tiers are employed to segregate web and application servers from database servers through the use of security groups.

Do you use Web Application Firewalls (WAF)?

Our company WAF is deployed for all applications for which it is supported. *Please contact your account or client relationship manager for information regarding whether the services that your organization receives from one or more of our business units include web-facing applications.*

Is a solution present to prevent unauthorized devices from physically connecting to the internal network?

We are in the process of deploying a solution that will prevent unauthorized devices from connecting to the wired network. We have a solution to prevent unauthorized users from connecting to the internal wireless network that requires 802.1x authentication.

Describe the processes, if any, used to detect and prevent network and host intrusions.

Intrusion detection and prevention systems ("IDS/IPS") monitor all Internet connections. Management of such systems includes automated alerting, blocking, and notification to security and incident response managers and support personnel, which is integrated with our incident management system. IDS/IPS logs are sent to an internal security information event management (SIEM) system and are monitored continuously by a managed security provider per documented procedures and service level agreements ("SLAs"). Attempted intrusions are escalated, investigated, and resolved according to local and global incident management and escalation procedures.

3.4 Training and Awareness

Does the organization maintain a privacy or security awareness training program that is implemented annually?

Information security, privacy, and confidentiality training is provided during employment onboarding processes and annually thereafter for all employees. Additional role-based security training is implemented using a risk-based approach or, where required by local regulatory schemes. Our company also conducts ongoing phishing simulation campaigns and trains employees appropriately based on the results. Training records are maintained within an electronic learning module as part of our people management platform.

Additionally, information security newsletters are issued regularly to remind MMC colleagues to practice good cyber hygiene and keep them appraised of potential threats. The Training and Awareness program itself is also reviewed and updated annually based on the ever-changing cyber landscape. Finally, our company makes available a wide range of training, videos, and awareness materials on our company intranet site for all colleagues to access as needed.

Are security roles and responsibilities defined in accordance with the organization's information security policy?

Employee security roles and responsibilities are defined in our company's Compliance and Information Security policies.

Are employees instructed to protect equipment and information when working offsite?

Our company's policies and guidelines provide employees with information and instructions for safeguarding equipment and information as well as personal safety when working offsite and cover requirements for reporting a theft or loss of equipment or information.

3.5 Asset Classification and Inventory Management

Does the organization classify information assets according to a classification scheme or policy that addresses appropriate layers of protection according to the sensitivity and criticality of the information?

Our company has adopted an *Information Classification Standard* that classifies data as Public, Internal, Confidential, or Restricted and imposes increasing restrictions and handling controls at each level.

Does the organization have a documented policy or guideline for labeling information according to its value, sensitivity, legal requirements, and criticality to the organization?

Our company has information labeling and handling guidelines, and some client contracts impose specific labeling requirements. At a minimum, client information is deemed confidential under our *Information Classification Standard* and must be handled in accordance with the confidentiality provisions outlined in *The Greater Good* (our Code of Conduct), the *Information Classification Standard, and the Handling Information Appropriately Policy*, and other company compliance policies and procedures, which include guidance for labeling of information, as well as confidentiality and data management obligations for the information. Certain client information, such as sensitive personal information (SPI), is classified as restricted information and is thus subject to more heightened handling controls.

Does the organization have rules or policies detailing the acceptable use of its information assets?

Requirements for the appropriate and approved use of our company's information systems and assets are outlined in our *Handling Information Appropriately Policy,* and other company policies, procedures, and guidelines identified in other portions of this document.

Are information systems and technology assets inventoried to ensure that all information necessary to maintain business operations and services is documented and available?

Hardware and software assets are inventoried to facilitate asset tracking, configuration management, business resiliency, and other programs. IT asset tracking systems are integrated with our configuration management database (CMDB) which provides the ability for automated hardware and software asset discovery, and maintaining detailed inventories, IT asset configuration information, and status. MMC and its business units also maintain application and website inventories, and more detailed records of processing in certain jurisdictions.

Do technology assets have assigned owners who are responsible for classifying the asset according to the information it contains and defining and periodically reviewing classifications, access restrictions, and other applicable controls?

All technology and application system assets are assigned owners who are responsible for the safeguarding and protection of the physical asset provided to them (e.g., company laptops, desktops, or approved mobile devices), or who may be responsible for reviewing and approving changes or access requests to our company's technology assets or application systems.

3.6 Access Management and Authentication

Are unique and identifiable login IDs required for authentication to applications, operating systems, databases, and network devices?

Access to our company's network and application resources requires the use of a unique ID and password. User IDs may not identify user roles or access levels, nor contain information other than username or email address.

Is there an established process for the return of software, hardware, company documents, and equipment when employment or contract for services has been terminated?

Employment onboarding and termination procedures include steps for the return of all company-owned assets and equipment.

Is there an access control program that has been approved by management, and communicated to constituents and an owner to maintain and review the program?

Yes. User accounts (i.e., user IDs) and other access privileges for our employees are created and revoked only after appropriate requests are made in conjunction with HR onboarding and termination processes which includes automated user ID creation and revocation where technically possible. Procedures allow for prompt modification or revocation of user access in the event of job role or employment change, including emergency revocation when circumstances require, such as in the case of involuntary terminations; accounts that have been inactive for at least 90 days are disabled, and accounts that have been inactive for 180 consecutive days are removed.

Is access to all information and applications controlled so that only those with a business need to know have access to complete their job assignments?

Access to information is granted on a least-privilege and need-to-know basis. Within applications, a hierarchy of controls limits access to data and system functionality according to user roles, levels of authority, and/or job function.

Does management conduct periodic reviews of users' access rights?

While our company does not conduct reviews of all active user IDs and associated access privileges on a scheduled basis, reviews of employee network access accounts against "leaver" reports from HR are conducted at least monthly, and System Administrator accounts and Privileged User accounts are reviewed quarterly.

Is elevated or system administrator access limited and controlled by secure logon procedures?

Access to accounts with elevated privileges is restricted to a limited number of authorized support personnel who require such access to perform their job functions. Server administrators have an administrative account that is separate from their standard user account. System Administrator accounts are reviewed quarterly. Additionally, MMC has implemented a training program that requires all MMC Tech staff, regardless of role, to complete Privileged Access Account training.

Does all system administrator access require multi-factor authentication (MFA)?

Our company has deployed a privileged information management system to enforce multi-factor authentication (MFA) for privileged system administrator and database administrator access. MFA is also deployed to any systems where required by law or regulation.

How is data isolated to prevent other customers from accessing another customer's data?

Depending on the type of system, data is logically separated using file system directory structures, individual database schemas, realms, or unique client keys or IDs.

Does the organization utilize clean-desk practices?

Employees and third parties are instructed to secure all hard-copy materials that contain sensitive or personal information in locked cabinets or drawers when not in use. Paper documents that are no longer needed are shredded according to our company's retention policies. Waste paper with client information is disposed of via locked containers and then shredded regularly.

Does the organization utilize screensavers for unattended systems?

Password-protected screen locks, which are configured to initiate after 15 minutes of inactivity, are mandatory on all company systems.

How does the organization manage idle system sessions?

Session activity timers are not used for employee access in all systems. However, password-protected screen locks, which are configured to initiate after 15 minutes of inactivity, are mandatory on all company systems and access to systems and data (including when working remotely or connected over VPN) is controlled via user privileges assigned to the user's network access account.

3.7 Desktops, laptops, tablets, smartphones

Does the organization permit remote access for employees, contractors, subcontractors, and/or other third-party vendors?

Employee remote access to our company's network is permitted and provided through a virtual private network (VPN), using multi-factor authentication (MFA).

Third-party access or interfaces must meet our company's standards and approvals and must be secured through a dedicated VPN or other secured private channel or protocols. Access to third parties is granted subject to risk assessment and appropriate contract terms and conditions.

Has the organization identified the risks of introducing support for corporate applications on personal mobile devices?

Yes. BYOD is only available in countries that have been approved by our company's Legal & Compliance teams where the environment allows the use of personally owned devices. There is a supervisor approval for BYOD to make sure that the role the colleague has within the firm enables the use of BYOD and employees need to accept an end-user agreement establishing rules for such devices. BYOD access is typically limited to select applications such as email and Zoom and offers limited functionality in other cases.

Various inputs have included assessments from our company's Global Information Security, Legal & Compliance, and HR teams including technical risk assessments of third-party security products or services chosen by our company, legal reviews of employee consent agreements, and HR reviews of employee rights.

Does the organization provide mobile device security training for all users utilizing BYOD?

The consent agreements required to be signed by approved company employees form the basis of awareness for utilizing BYOD.

Our company's BYOD policy has been defined to include:

- Defined process for employee requests including criteria for employees who can be approved for using such devices (e.g., employee is in an appropriate role and must handle sensitive data),
- Device type(s) permitted under the program (e.g., Apple OS and approved Android devices),
- Required employee consent agreements,
- Nature of services that will be permitted (e.g., Outlook, Teams and Zoom)
- Acceptable use requirements

Does your organization utilize Mobile Device Management (MDM) or Mobile Application Management (MAM) solutions?

Yes. Our company uses various tools or solutions to manage BYOD and corporate mobile endpoints. For example:

- All MAC endpoints are configured with an MDM solution from JAMF that provides the ability to fully manage the device.
- For Windows mobile endpoints (e.g., laptop computers) an MDM solution, similar to SCCM, is currently available to our support staff for use on an as-needed basis, such as when the SCCM agent on a Windows endpoint is not responding.

Our MDM solution is cloud-based and hosted within the US. The management tools are cloud-based, and the infrastructure that provides access to email and data is on our premises and distributed into our company's strategic global data centers.

If MDM or MAM is utilized, does it detect any mobile devices (i.e., iPhone) that have been rooted (i.e., "jailbreaking", "broken")? (Note: "jailbreaking" or "rooting" allows users to gain access to the operating system of a device to permit the installation of unauthorized software functions and applications and/or to be tied to a particular wireless carrier.)

Yes. The MDM solution can detect if the device is jailbroken or compromised. If detected, the device is quarantined and removed from the system.

If MDM is utilized, is it used to manage/install anti-malware protection against malicious applications, viruses, spyware, infected digital cards, and malware-based attacks?

Our company deploys Ivanti Mobile Threat Defense (MTD) to Mobile Devices registered in our Ivanti MobileIron UEM. MTD identifies network attacks, risky and malicious profiles, and applications; allowing the UEM to take action against these detections.

What type of device and connection security protections are used?

Mobile devices are required to be configured with passwords that meet our company's standards in order to access data from our housed data on the device.

A digital certificate is used to secure the connection (2048-bit encryption). Access to corporate data is provided through secured apps, with multifactor authentication required.

Devices are encrypted to protect against loss or theft. A centralized management console is used to provide remote wiping and password management.

3.8 Encryption

What types of cryptographic techniques are used to protect sensitive information when transmitted over untrusted networks, or when stored?

The methods for exchanging data or information with our business units may include secure email, secure file transfer solutions (sFTP), or other secured company websites or portals (e.g., SharePoint portals). The decision to use encryption and the tool utilized depends on the sensitivity of the data that is exchanged with clients or other third parties (e.g., personally identifiable information, personal health information, or other SPI). The associated transmission methods our company uses and supports include Transport Layer Security (TLS v1.2 and v1.3) encryption, sFTP, and other encryption solutions such as WinZip and PGP (AES 256).

Removable device encryption is deployed to company laptops and desktop computers, and company laptops and desktop computers are required to have whole-disk encryption (AES 256) installed and enabled.

Backups stored on disk-based appliances employ AES-256 encryption, while Backups stored on tape use varying encryption standards based on hardware versions and method of encryption (hardware or software), with a preference to 256-bit encryption when possible (128-bit encryption minimum).

As to production data, our company's business units develop and maintain a variety of application systems related to the services provided to clients, some of which involves the collection and processing of personal information, including sensitive personal information, for certain services. Our company seeks to comply with all applicable security and compliance requirements and industry standard practices and has evaluated whether to encrypt data at rest on internal servers managed by our company and stored in our company's data centers, our chosen colocation centers and/or business office server rooms.

While data is not encrypted at rest within all internal electronic file repositories such as local area network shared drives, or all application databases, other internal file repositories, databases, or application systems may rely on encryption like whole-disk encryption. All applications subject to cybersecurity regulations that require encryption of personal information or other sensitive data have file/folder, database, or field-level encryption (AES 256). Additionally, our company has proactively applied encryption to systems deemed high-risk (e.g., Internet-facing application systems that process or store personal information).

In addition to encryption (where used), our company utilizes a layered approach to security ("defense in depth"), including but not limited to physical security, logical access and password management controls, multi-factor authentication, server and network device event log management and monitoring, and network security (e.g., firewalls, IDS/IPS, and DLP) controls. *For more information regarding any specific application solutions that may be in the scope of services you receive from one or more of our business units, please contact your account or relationship manager.*

How are encryption keys managed?

Encryption keys are managed in accordance with industry standards and our company's Encryption Management Policy and standards, which include but is not limited to roles and responsibilities, and requirements for the administration of key management systems and processes, key generation, and key storage, security, and compromise.

3.9 Cloud Services

Are Cloud Services Provided?

While our company may provide and maintain technology or application solutions in connection with client-facing services, our company is ***not*** a commercial cloud services provider (i.e., we do not provide Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) to our clients).

Will data be located in a private cloud? If not, what type of cloud is our data hosted on (e.g., public, community, hybrid, private)?

Our company's technology department currently leverages public and private cloud technology as an extension of our existing virtual server infrastructure. This deployment follows all existing operational policies and controls for management of technology infrastructure. The use of third-party or supplier cloud solutions by our business units to support their client services requires a cloud framework review of the business initiative and a risk assessment of the proposed service supplier solution, and the use of such supplier solutions must be consistent with existing client agreements.

Our private cloud is contained within our company's strategic data centers and company-managed environments. Our company also leverages AWS and Microsoft Azure public cloud platforms and services in addition to these private cloud environments (e.g., M365 for e-mail). Our AWS and Azure public cloud platforms are architected, implemented, and secured in accordance with existing company policies and standards.

Our company's clients are not involved in the configuration or day-to-day system management or maintenance of our company's internet-facing systems hosted within cloud environments, our data centers, or facilities, or those maintained by any third-party suppliers or service providers used by our business units. As such, virtual images are not provided by our company to our clients, such as commercial cloud service providers or suppliers may provide to their cloud service customers.

Does data hosted in the private cloud reside only in the US?

Within our company's private cloud, data will be housed within our company's strategic data centers located in the US (Ashburn, VA, Dallas, TX), UK (Bedford, UK and Dublin, Ireland), and Australia (Sydney and Melbourne). The implementation of private cloud technology does not impact or change the geography in which data or business application systems are housed. Data hosted in the public cloud is hosted in the appropriate country as required by statutory requirements.

Are virtual machines used and if yes, are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?

Administration of virtual machines is managed by Role-Based Administration Control (RBAC), based on the responsibility of each team that has access to the Virtual Infrastructure through Active Directory-managed security groups. Executed tasks can be audited if required. RBAC extends into the Public Cloud environments as well following the same standards.

Are attacks that target the virtual infrastructure prevented with technical controls?

Firewalls are used and public cloud hypervisor security standards are implemented within our virtual server infrastructure, in addition to routine security patching to protect against targeted attacks.

3.10 System Monitoring and Audit Logging

Are computer systems monitored to identify potential security breaches (file access, unsuccessful login attempts)?

Our company's servers and network are monitored continuously for system performance, and availability and to detect intrusion attempts. System activity is logged, and the logs are used to investigate any potential incidents reported.

System and security event logs are enabled which include but may not be limited to routers, firewalls and IDS/IPS devices, user directory, authentication systems, and application and database servers to capture events that may include the date, time, success, or failure of login attempts, user ID, workstation name, IP address, and account creation or modification activities. Such logs are sent to a centralized security incident and event log management system (SIEM). Access to the SIEM is restricted to a limited number of IT support and incident response personnel to protect the logs from loss and unauthorized modification.

How often are logs reviewed?

Our company has defined playbooks that note what security logs constitute a security incident and require investigation. These defined incidents, and the associated logs, are raised automatically and are reviewed in line with our agreed-upon service level objectives.

How long are logs retained?

System and security event logs will be maintained for up to three years depending on the nature of the system, log type, laws, and regulatory requirements.

3.11 Penetration Tests

Are penetration tests performed at least annually, by independent trained, and experienced personnel, using manual and automated procedures?

Our company, in our sole discretion, performs penetration tests and threat hunts of our external network infrastructure on an annual and ad hoc basis using dedicated internal staff specially trained and experienced in industry standard penetration test scopes and methods, or suppliers chosen by our company to perform such tests. Applications developed and hosted by our businesses may also be subject to annual or other periodic penetration tests. Clients (or their chosen third parties) are not permitted to conduct any such vulnerability scans, penetration tests, or other code or port scans against our company's network or application systems.

Our company does not discuss nor share the results of its network penetration tests or vulnerability scans of its internal systems. *For additional information or executive reports regarding any application code testing or application penetration testing conducted against any Internet-facing applications hosted by our businesses that may be in the scope of services to you, please contact your account or relationship manager(s)*.

3.12 Change Management

Is there a documented change management process? If yes, please describe the process.

Our company maintains a Global Change Management Policy and a documented change management process using a commercially recognized and globally supported commercial software tool. The process is based around Information Technology Infrastructure Library (ITIL) standards. Changes must be logged, reviewed, approved, and monitored according to our change management process and system. Testing is conducted on development systems, and changes cannot be approved for production installation without proper documentation, details, and test results.

Do you organize regular reviews of appropriate changes that are open to the IT/business community?

Our company's change advisory board meets regularly to review submitted change requests and how they might affect the IT/business environment.

3.13 Information Backup

How often is information backed up?

The standard for regular data backups is to use a daily incremental, weekly and/or monthly schedule that meets business backup requirements. Back-ups are performed using standard management software to disk, cloud storage (i.e., for some business unit applications that may be hosted in an external cloud such as AWS, Microsoft Azure), and/or tape back-up systems.

Are backups stored in offsite locations?

Backup tapes are stored offsite. For disk-based backups, replicas are held at alternate company sites, or where applications are hosted in the cloud, related data back-ups are stored within the applicable third-party cloud provider back-up environments (e.g., AWS, Microsoft Azure).

How is backup or other physical media protected while in transit or when outside the organization's boundaries?

Backup tapes are securely transported and stored offsite in secure facilities. Handling of backup tapes includes but is not limited to, stringent tracking steps and the use of secured containers to transport tapes between our company and its contracted offsite facilities. Offsite storage facility personnel do not have direct access to the data stored on the tapes; only authorized internal operations and business continuity personnel have access to the backup tapes.

Are backup tapes recalled from the offsite location to test/check for effectiveness when trying to restore a system or piece of data?

Backup jobs are monitored, and backup restores are tested as part of routine data restorations. Various tapes are validated through our company's business continuity and disaster recovery testing. Disaster Recovery itself is tested yearly and during other audits and reviews.

Are backups encrypted?

Backups stored on disk-based appliances employ AES-256 encryption, while backups stored on tape use varying encryption standards based on hardware versions and method of encryption (hardware or software), with a preference to 256-bit encryption when possible (128-bit encryption minimum).

What is the retention period for backup tapes?

Backup tapes and disk-based backups are retained for disaster recovery and operational restores only, with limited exceptions. Back-up tape media is overwritten after the retention period is satisfied. Back-up tapes or media may not be returned or destroyed based on individual client requests as these tapes or media contain data of multiple clients.

3.14 Password Management

Does the organization maintain a password policy that includes a defined length, are not displayed in clear text on screens or reports, history is maintained to prevent reuse of old passwords, composition rules are used to enforce strong passwords (e.g., alphanumeric, and other characteristics)?

Passwords for our company's employees:

- must be of a defined minimum length (8 characters for standard users; 14+ characters for System Administrators);
- are required to be changed at least every 90 days;
- are required to contain a reasonable level of complexity (e.g., case sensitive, alpha-numeric, and/or special characters);
- are not displayed on screens or reports;
- Password history (8 prior passwords) is maintained to prevent the reuse of recent passwords;
- intruder policies lock accounts after no more than 6 failed attempts;
- where possible or supported, systems are configured to prevent passwords from being changed by the user more than once in 24 hours without System Administrator support.

Where system policies are not available to enforce such rules, users are provided with guidance about password composition.

Are all vendor-supplied default passwords changed?

Yes.

Are passwords encrypted in storage? If yes, what is the encryption method or cipher strength?

Passwords are hashed in storage using AES-256 and/or SHA-256 encryption.

3.15 Incident Management and Response

Does the organization have mechanisms for users to report security incidents, including the loss or theft of information?

Employees and third parties are instructed to report data and security incidents, including the loss or theft of equipment or information, to our company's IT service desk or utilize other dedicated reporting channels (such as a dedicated email for vendors to report incidents). Defined incident response processes to ensure proper incident escalation, investigation, and resolution.

Is there a defined security incident response process that is documented and followed?

Our company has an Incident Response Standard for cyber-information security and data incidents. The standard includes various protocols for handling specific types of incidents such as cyber-only, data-only, and hybrid data and cyber incidents. Our company assigns responsibility for incident

response to dedicated and trained teams, and where needed these teams involve a cross-functional mix of members. The assignment of incidents is based on an initial risk assessment of the incident and the potential impact on data subjects. There are clear escalation procedures in place to ensure the appropriate allocation of incidents.

Is there a dedicated Cyber Incident Response Team (CIRT)?

A dedicated cyber security incident response team is in place. This team follows the *Cyber Incident Response Standard* and including incidents that impact client data and personal information or incidents that otherwise implicate cyber laws and regulations. The cyber security incident response team is responsible for defining relevant IT security incident response actions, providing direction to responder teams, conducting forensics investigations, and working with other internal functional areas (e.g., HR, Legal & Compliance, Privacy, IT, Internal Audit) as needed and as may be required to support external notification obligations.

Is the incident response process tested regularly?

Our company regularly (at least annually) performs tests of our incident response plan. Such tests consist of tabletop exercises based on real-life scenarios selected to reflect the relevant risks faced by the organization. The tabletop exercises require senior management from the various business segments and corporate teams to work through the scenarios using our company's incident response protocols to demonstrate the effectiveness in handling the scenarios and identifying opportunities for improvement.

How are clients notified of security incidents or data breaches?

Our company's incident response standard addresses the timing and responsibilities of all relevant parties in the case of a data incident, including complying with legal and regulatory requirements.

Are post-incident reviews undertaken to identify weaknesses and learn from any mistakes?

The cyber incident response process requires the Incident Response Team to conduct an After-Actions activity after all incidents if deemed necessary. If applicable, corrective action plans are developed to prevent the recurrence of similar incidents and/or allow our company to remediate similar types of incidents more effectively.

Has your organization experienced a data or privacy breach in the past 3-5 years?

Although we are unable to share details of incidents with those not directly impacted, we can share at a high level our company has had some data incidents in the past 3-5 years. The nature of incidents our company has experienced is largely clerical in nature (e.g., mailing error or erroneous transmission of data by email). We did suffer one incident in 2021 that was beyond the types described above, however, it was largely limited to internal files with data of our current and former employees. It also impacted a very small number of client files and all such clients and their employees were notified in accordance with regulatory and contractual obligations. As this breach is subject to ongoing litigation in NY (which tends to trigger more recent media coverage) we cannot discuss it further. We can further advise that during the relevant timeframe our company has not suffered any large-scale breach involving client data, or any type of breach that has materially affected our security or operations, as such, we remain confident in the overall quality of our information and cybersecurity program.

3.16 Media Handling and Data Disposal

Does the organization have a secure disposal procedure to ensure information is removed from systems before re-use or disposal?

Our company maintains hardware asset management policies and procedures that require secure disposal of IT assets using industry-standard methods (e.g. electronic media, such as system hard drives, are sanitized before disposal using a multi-pass, random character overwriting procedure. Other electronic media and portable devices may be physically destroyed through shredding, pulverizing, or secure wiping before disposal). As our company's systems contain data and information of multiple clients, and systems disposal is not performed on an individual client basis, our company does not provide Certificates of Destruction to clients.

Is there a process for the secure disposal of paper?

Our company maintains a records retention policy and other protocols that require paper documents containing client information that is no longer needed to be disposed of via locked containers which are shredded regularly by a third party.

What is the retention period of data on both electronic and non-electronic media?

Data is retained in accordance with our document retention schedules. Retention periods are based on business needs and/or legal requirements. Personal information will be retained for no longer than is necessary for the purpose(s) for which the information was collected and any other permissible, related purpose or than is necessary to comply with our legal requirements.

Is removable media (e.g., CD/DVD, USB devices) used or are workstations configured to allow usage? If yes, what controls are in place to secure media and prevent data loss (e.g., encryption, USB port disabled by default, authorization process for usage)?

Our company laptop and desktop computers are configured with whole-disk encryption software using strong 256-bit AES encryption. Additionally, our laptop and desktop computers are configured with security tools to prevent data from being copied to removable storage devices (e.g., USB memory sticks). Exceptions to this position are tracked and monitored.

Does the organization have a Data Loss Prevention (DLP) system in place to detect and prevent sensitive data or PI from being copied or transmitted to unauthorized recipients or devices?

Our company has deployed a Data Loss Prevention (DLP) solution. This program includes monitoring, detecting, and auto-encrypting (for emails) or blocking (for websites) of files or messages with sensitive personal information, based on Compliance-directed policies. In addition, a portion of the alerts are, on a risk-based approach, selected for review and internal disciplinary handling where appropriate.

While our company reserves the right to modify the coverage and scope of the rules applied in DLP, in general, the rules are designed to prevent the loss of unencrypted sensitive personal information, including some types of health or medical information, financial information such as credit card numbers and national identifiers such as Social Security Numbers.

What procedures are in place for sanitizing electronic media for reuse?

Before systems are reused, they are re-imaged with our company's standard operating images.

3.17 Physical Security

What types of physical security controls are used at your facilities?

Our company has established specific policies and guidelines relating to our physical security program for its facilities which include electronic and procedural access control, alarm, and environmental monitoring, closed circuit television (CCTV) placement and recording, and architectural design analysis to ensure proper controls are present. Additional controls as warranted may include on-site security staff and x-ray screening of mail and packages.

Are buildings that house critical IT facilities physically protected from the perimeter?

Perimeter protection for our facilities is addressed as part of the overall physical security program to the degree reasonable and practical based on the physical location, the criticality of the operations, and the likelihood of any given disruptive event. Controls adopted may include security perimeter fencing, a gated vehicle/ pedestrian control, security officer patrols, and crash or other physical barriers designed to protect the exterior of the facility from vehicular attack.

Is physical access to buildings that house critical IT facilities restricted to authorized individuals?

Our company's physical security policies require our locations to institute access control procedures for employees, visitors, and contractors, including restricting access to sensitive areas (e.g., IT-related

facilities such as data centers or server rooms) to only those personnel whose job duties require access to such areas. The list of authorized personnel having access is reviewed quarterly.

Does the organization conduct risk assessments of its facilities?

Threat and vulnerability risk assessments are conducted of our company's data centers every two years. Rental screening questionnaires for our company's business offices are also completed at the time of acquisition of new or during lease renewal and include questions relating to local specific risks, security, and building life safety.

Does the organization periodically review access to restricted areas?

Owners of restricted areas are responsible for managing day-to-day access authorizations, however, authorization for access to restricted areas is reviewed quarterly, at a minimum.

Are secured areas physically segregated from other areas of the general environment?

Yes.

Is access to secure areas logged with the date and time of entry?

Our company's physical security policies indicate that secured sensitive and critical areas have electronic controls that allow for logging and review of access histories in addition to controlling authorized access. Access is revoked as job roles change or employment is terminated. This function is also reviewed during related data center and server room audits.

Do surveillance cameras monitor all building entrances and IT facilities?

Common areas, such as entrances, of commercial buildings where our company has tenanted space may be under camera surveillance (e.g., CCTV), as part of the building security program. Camera surveillance of our business offices is part of the overall physical security program when permitted or made available by the facility management (we have limited control over the use of CCTVs in buildings where we are a tenant and have no operational or security control over entrances). Camera surveillance of our data centers is also in place and is monitored 24x7.

Are CCTV recordings retained for 30 days or more?

Our company's physical security policy requires CCTV recordings to be retained for a minimum of 30 days. However, recordings may be retained for longer or shorter periods as may be required to meet specific regulatory requirements or as implemented by third parties who operate these systems outside of our control. Where correlated with an incident, recordings or the relevant portions thereof are retained until no longer required.

Describe the security or safeguards in place for loading areas.

In the vast majority of locations our company is a tenant, therefore we rely on building management to maintain the security of loading areas. Depending on the location and type of loading area available, safeguards may include camera surveillance, electronic and/or procedural control of access, and a security staff or dock master presence.

Are visitors required to sign in and be escorted when on the premises?

Our company's physical security policies require that offices must have procedures in place to authorize and control visitor access to the workplace. Procedures may include the use of a designated reception area, visitor sign-in, and identification, meet and greet by the host, and escort during the visit. Depending on the facility, sign-in may also be required at the building's security desk and may require a government-issued ID. Visitors must be escorted by authorized staff. Visitor logs are retained for at least two years and are reviewed on an as-needed basis when correlating events.

3.18 Data Center Locations

Our company operates data center facilities throughout the world with data centers housed in each of three key regions – North America (Dallas, TX, Ashburn VA, in the USA), EMEA (Bedford UK and Dublin, Ireland), and APAC (Melbourne & Sydney in Australia).

These facilities are a mix of company-operated (Dallas) and co-location in vendor-operated facilities. (Dublin, Ireland, Melbourne, and Sydney (AUS), and Ashburn).

In the co-location facilities:

- Company-owned systems are housed in secure areas to which no other companies have physical or logical access.
- Dedicated communication links providing Internet and WAN services for Company systems are provided by our chosen telecommunications carriers.
- Systems are remotely maintained and managed by company-authorized IT support staff in accordance with our company's policies, procedures, and standards as described in this document.

Files containing client information may also be stored within internal electronic file repositories housed in secure server rooms in the business offices from which the services are provided.

For information regarding the specific physical or geographical company locations where your data may be accessed, processed, or stored, please contact your account or client relationship manager(s).

3.19 Problem Management

Does the organization maintain a documented problem-management program?

A dedicated problem management team and process are in place to assist our company's Infrastructure and business IT teams in performing problem analysis and troubleshooting to determine the root cause of one or more incidents. The problem management process is based around ITIL standards and includes the development and production of corrective action plans and post-mortem reports. Depending on scope and scale, corrective actions are prioritized as changes (following the change management process), service improvement programs, or formal IT projects.

3.20 Patch Management and Protection against Viruses & Malicious Code

Are systems patched regularly?

Systems are patched regularly (e.g., weekly, monthly, or on an emergency basis as may be deemed necessary and appropriate under the circumstances). MMC has implemented a risk-based approach for prioritizing the patching of vulnerabilities to ensure consistent and effective vulnerability management. The risk-based approach focuses on the most critical vulnerabilities for prioritizing patches.

Known vulnerabilities requiring patches or hot fixes are tracked, assessed for risk, tested, and deployed in accordance with our company's vulnerability identification and assessment, and change management processes.

MMC focuses on timely patching and considers it critical in maintaining a strong security posture. In circumstances where we cannot apply a patch in the recommended window because it conflicts with critical business operations, an assessment is performed, identification of compensating controls is determined, and plans are created and documented to address the risk. These plans are monitored and reported on until the patch can be implemented.

Are policies, procedures, and technical controls in place to protect against malicious code such as viruses, worms, and spyware?

Next-generation threat protection (to include Endpoint Detection and Response) – using globally recognized supported, and centrally managed products – is in place for network gateways, e-mail systems, Linux OS, Microsoft Windows servers, and workstations, and MAC OS workstations. Virus filtering policies are deployed on e-mail servers that scan all incoming and outgoing messages and their attachments for viruses and other types of malicious content. Where available and permitted by

law, URL filtering prevents access to inappropriate sites including those known to spread malicious code (which includes free file-sharing sites and personal email sites). Additionally, using a threat prevention tool implemented within our email and web-browsing infrastructure, we analyze both web and email traffic to prevent and protect our company from sophisticated cybersecurity attacks. Each web attachment and URL sent to our company is reviewed in real-time, along with browsing activity, which enables us to quarantine any identified malicious content. Once such items are identified by the tool, they are blocked or referred to the Incident Response team for further analysis. Threat prevention software solutions are deployed and updated using automated deployment and installation systems. Users cannot change or disable the threat protection solutions or related updates.

Are personal firewalls used?

Our company's laptop and desktop computers are protected with a robust Endpoint Detection and Response (EDR) product suite that includes a host-based firewall and advanced threat protection technology.

Is File Integrity Monitoring used to detect unauthorized changes?

Our company does not employ File Integrity Monitoring (FIM) technology specifically; however, numerous other layers of defense capabilities are maintained including Indicators of Compromise (IOC) detection capability on Windows hosts (servers and workstations).

What safeguards are used to protect electronic messaging?

Anti-malware systems, sandboxing, reputation, DMARC, DKIM, and other controls are deployed within the email messaging environment to scan all incoming and outgoing messages and their attachments for viruses, and malware, reject messages with certain attachment types, and validate the integrity of transmitted messages. Encryption of e-mail messages or attached files is also employed where necessary to protect personal or sensitive information during transmission as described in our DLP response. Additionally, using a threat prevention tool we are able to analyze both web and email traffic in order to prevent and protect our company from sophisticated cybersecurity attacks using advanced detection and sandboxing technologies. Each email attachment and URL sent to our company is reviewed in real-time, along with browsing activity, which enables us to delete any identified malicious content. Once such items are identified by the tool, they are either blocked or referred to the Incident Response team for further analysis.

3.21 Vulnerability Management

How are cyber vulnerabilities monitored and managed?

A vulnerability identification, assessment, and management program is in place that includes server hardening, scanning, alerting, and security and operating system patch management. Security vulnerabilities and emerging threats are tracked by information security personnel, assessed by technical experts, and remediated according to risk priority. Critical vulnerabilities are required to be remediated within 30 days or less.

How does the organization keep current with the latest threats and other vulnerabilities?

Our company's Cyber Threat Intelligence Team continuously monitors open-source and closed-source intelligence feeds, services, and groups, such as FS-ISAC, for emerging threats and vulnerabilities. Relevant threats and vulnerabilities are ingested into an AI-based cyber threat intelligence tool that provides enhanced information for analysis, and intelligence is distributed to relevant stakeholders and systems.

Is there a Vulnerability Management Policy or Program that has been approved by management, communicated to the appropriate constituent, and an owner assigned to maintain and review the policy?

A vulnerability identification, assessment, and management program is in place that includes server hardening, scanning, alerting, and security and operating system patch management. Security

vulnerabilities and emerging threats are tracked by information security personnel, assessed by technical experts, and remediated according to risk priority. Critical vulnerabilities are required to be remediated within 30 days or less.

Systems are patched regularly (e.g., weekly, monthly, or on an emergency basis as may be deemed necessary and appropriate under the circumstances). Known vulnerabilities requiring patches or hot fixes are tracked, assessed for risk, tested, and deployed in accordance with our company's vulnerability identification and assessment, and change management processes.

Are network vulnerability scans performed against internal networks and systems, and against internet-facing networks and systems?

Vulnerability threat assessment scanning of our internal and external facing systems is performed weekly. Web application code testing may also be performed on an as needed or scheduled basis upon request from the internal business application owners. These scans provide a granular view of system configuration (e.g., operating systems, open ports, running services) and are designed to detect known security vulnerabilities as well as backdoors and other malicious applications; and in the case of web applications, by simulating attacks (e.g. cross-site scripting, HTTP response splitting, etc.). The scans are performed by a dedicated security team using our company-chosen industry-standard solutions and/or other third-party services.

3.22 Wireless Systems and Protection

Are wireless networks authorized and used within the company?

Wireless Local Area Networks (WLAN) are controlled according to our company's wireless network standard which includes the use of safeguards such as strong encryption (e.g., EAP-TLS). All WLAN access, including guest access, requires unique authentication (e.g., 802.1x). Access and intrusion detection attempts are logged and monitored. Our company's WLAN infrastructure is also segmented from the internal network via dedicated WLAN controllers and access policies defined based on device and user roles.

Do you perform periodic scans for rogue wireless access points?

Our company's WLAN controllers include built-in intrusion detection (IDS) functions and are configured to perform continuous scanning for rogue access points. The logs are secured and accessible only to authorized IT support personnel, and these logs are used as needed to investigate and correlate WLAN issues and incidents in accordance with our company's IT incident management and response procedures.

3.23 System Acceptance Criteria

Do defined system planning, and acceptance procedures exist to minimize the risk of system failures?

To minimize the risk of system failure, our company's system implementation lifecycle requires a dedicated team within MMC Tech to assist with service on-boarding, capacity planning, and testing, and to provide guidance on equipment specifications and lead times. Project and Business-as-usual (BAU) infrastructure forecasts are collected quarterly from business unit IT departments to predict additional infrastructure capacity needed within key data centers across all regions. These forecasts are fed into quarterly pre-purchases of shared infrastructure components to ensure sufficient resources for new and existing business applications are available when required, with limited reserves for unforeseen requests.

Are information systems tested before being introduced into production use?

Before being released into production, new systems and changes to existing systems are tested with results retained, to verify systems work as intended.

Is a review process in place for standard security configurations to ensure that operating systems, applications, and desktops are configured according to approved standards and industry best practices?

Operating systems, applications, and network devices (e.g., computing workstations, servers, firewalls, routers, switches) are configured in accordance with internal and external industry standards and practices and are hardened in a variety of ways including, but not limited to, disabling/removing vendor-provided default access configurations, codes or passwords, disabling default ports and services, routine security patching, protection against malware, and access controls. Our company's operational and security processes include steps to proactively and automatically determine patch level status, and anti-virus and threat protection status.

Is a defined Software and/or Systems Development Lifecycle (SDLC) maintained and followed?

Our company's business units maintain dedicated technology or solutions delivery teams (MMC Tech) that are responsible for application development and maintenance. Application development staff follow standardized software development lifecycles using agile, waterfall, or project management-based approaches which include documenting business and security requirements and using third-party tools and services to perform dynamic and static testing of application code (which includes OWASP testing of web applications) as may be deemed necessary depending on the nature and purpose of the software or application system being developed.

Are development, test, and operational systems appropriately separated?

Development, test, and production systems are appropriately separated, such as through the use of physically separate hardware and network segments.

Are duties segregated to reduce opportunities for unauthorized access or unintentional misuse of information assets?

Duties are segregated such that changes, additions, or modifications to our company's information technology assets and facilities are reviewed and authorized by appropriate management personnel, most of whom are organizationally separate from the user/requestor and those responsible for the implementation. Personnel responsible for user access administration do not have system/transaction processing responsibilities.

3.24 Artificial Intelligence (A.I.)

Are we using Artificial Intelligence in conjunction with any client data or services we provide?

Our Company uses a variety of internally developed and externally sourced AI tools and solutions for various aspects of client services and products including text extraction automation, document summarization, chatbots, and other customer-service interactions. Many of our uses involve an internal generative AI tool called LenAI that leverages a private endpoint model offered through Microsoft and functions similarly to ChatGPT. It was developed with extensive review by our privacy, security, and technology teams. We are not training LenAI, and LenAI does not retain any outputs it generates. LenAI and Marsh McLennan do not contribute any data to train the OpenAI model, and we limit the use of public generative AI models from our network.

Our uses of AI are subject to internal reviews with specific consideration towards the safety of our customer data and meeting our legal obligations. We use a variety of channels to guide our colleagues on the risks associated with AI, as well as our expectations regarding the input of confidential information to any AI tool not managed by the Company.

4 - Human Resources Security

4.1 Personnel

Does the organization conduct background checks or pre-employment screening?

Background checks are conducted on all new hires, interns, and contingent workers, as permitted under applicable law. Depending on the location of the role, and applicable law, screening may include, but may not be limited to, verifying prior employment, and verify education. confirming stated qualifications, reviewing criminal histories, checking other civil records, checking federal exclusion lists (i.e., OFAC), and conducting credit checks. Background checks are done at the time of hire and upon client request. Fingerprinting is only done if the state requires it to complete the background check and upon client request. Our company does not perform drug screenings, unless requested by a client or for cause, according to our Drug-Free Workplace policy.

Does the organization require all employees, temporary workers, agency staff, contractors, and other third parties to sign confidentiality and/or non-disclosure agreements?

In certain jurisdictions according to the applicable law, employees are required to sign Confidentiality and/or Non-Disclosure Agreements, and in all jurisdictions, employees are required to agree to comply with company policies including, but not limited to, *The Greater Good* (our Code of Conduct), and the *Handling Information Appropriately Policy*. Contracts with vendors, subcontractors, or other service providers are required to be reviewed by our Company's legal department and include confidentiality, security, and privacy terms and conditions commensurate with the types of services provided by the third party.

Do employment contracts include security responsibilities of employees and managers?

Employees in the U.S. do not typically enter into employment contracts with our company but do so outside the U.S. Employment with our company requires all staff to comply with the policies contained in *Working Here - A Colleague Guide to Policies*, *The Greater Good* (our Code of Conduct) which includes maintaining the confidentiality of information, and other company Compliance policies as appropriate to the individual's position or that may be implemented from time to time.

Does the organization have a disciplinary process for employees who have violated its policies?

Our company's policies allow for disciplinary action for violation of company policies, which can include termination of employment or contract for services.

Are employees required to sign the information security policy upon hire and at least annually thereafter?

At time of onboarding, employees are required to acknowledge that they have read and will agree to comply with *The Greater Good* (our Code of Conduct). In addition, at onboarding and annually thereafter, employees are required to complete our *Privacy and Security Awareness and Training* and certify that they understand the privacy and security policy requirements and will comply.

5 – Business Continuity & Disaster Recovery

Does the organization have a managed process for maintaining business continuity and disaster recovery?

Our company has dedicated business resiliency management ("BRM") and disaster recovery ("DR") teams that coordinate our capability to recover systems and provide support using internal and/or external resources. Solutions are designed to meet requirements defined by impact analyses for system, facility, colleague, and/or critical third-party disruptions outages. Where appropriate, human or computer workload is distributed among multiple locations to reduce or eliminate downtime due to local outages.

While our company does not maintain third-party certifications for our BCP/DR management programs, ISO 22301 is used as a guide to design and maintain our BRM program framework.

For additional information regarding our crisis preparedness and business resiliency management program, please contact your account or relationship manager to request a copy of our Statement of Recoverability.

How often do you test/exercise your Business Continuity plans and what methods are employed?

Business Continuity Plans (BCP) are tested/exercised on a regular and representative basis. Using a risk-based approach, we do not test/exercise all plans on the same schedule. A range of test/exercise methods are employed, as appropriate. Representative examples include:

- Remote access (e.g., work from home, work from a different office)
- Commercial work area recovery exercises
- System fail-over testing, including external vendors where appropriate
- Evacuation drills, notification system tests, and periodic generator tests

What is the expected recovery time objective for critical business functions?

BCP recovery time objectives vary based on requirements defined through the Business Impact and Application Risk Analyses.

How are application disaster recovery (DR) exercises conducted?

Disaster recovery tests are coordinated by our company's dedicated global DR group ("DR Services" at the request of internal business IT teams/application owners. Test objectives are defined and agreed to by the business lead, business IT support lead, and DR Service leads.

Recovery procedures are reviewed and updated in the test planning process. Recovery and validation are performed by DR Services, business unit IT, and other business unit participants. Results against each objective are reported to business and technology stakeholders, and any remediation tasks identified by the test are documented and assigned for follow-up.

How frequently do you perform application disaster recovery tests?

Our company has an active DR testing program. Multiple DR tests across the globe are conducted each year, ranging from single-application tests to multiple applications recovered during a single test. Our company's business units define the scope and frequency with which specific applications must be recovery tested which is based on application criticality.

What types of application disaster recovery tests do you perform?

Application disaster recovery tests include the following types:

Component - Individual hardware or software components or groups of related components that are part of protective systems or critical to the operation of the organization are tested.

Full - All systems and components that support the plan are tested. This can include all upstream and downstream dependencies**.**

What is the organization's disaster recovery approach?

Our company's Disaster Recovery service works by replicating the application state between two data centers or public cloud regions; if the primary data center becomes unavailable, then the backup site can take over and a new copy of the application will be recovered using the most recently replicated data.

Data centers are configured with redundant power feeds, telecommunications circuits, backup generator power, and uninterrupted power supply (UPS) systems. Server rooms are configured with UPS systems and depending on the facility's size there may be on-site backup power, such as a generator. Such systems are tested periodically (e.g., quarterly, semi-annually) depending on the system and location.

Each of our critical business and corporate functions maintains Business Resiliency/Disaster Recovery plans with specific provisions for employee mobilization, alternate workspaces, recovery of network and telecommunications systems, restoration of data, and communication with clients and critical third parties. These plans are created based on a Business Impact Analysis that identifies business recovery requirements and priorities.

The Business Resiliency/Disaster Recovery plans address the loss of:

- Office facilities and personnel.
- Network services, data, operating systems, or application software.
- Mission-critical functions and processes.
- Key third-party providers.

Critical company operations and functions are required to maintain copies of their current Business Resiliency plans on the Business Resiliency Management System (BRMS – Fusion)and, as they deem necessary, in hardcopy. Disaster Recovery plans are kept and maintained by the business unit IT organizations; copies are also maintained by our company's MMC Tech team, centrally. Critical applications are designed for high availability, using clustering or load balancing technology.

Disaster recovery strategies are implemented based on business-defined requirements, including near real-time data replication and delivering recovery in the optimum of time. Furthermore, Software-as-a-Service (SaaS) Disaster Recovery or Disaster Recovery as a Service (DRaaS) is also used to provide recovery to the Cloud. The DRaaS solution replicates workloads from our on-premises infrastructure to the AWS or Azure Cloud in various regions across the globe. All replicated data in transit to and at rest in the Cloud is encrypted. In addition, where production systems are hosted in the Cloud, DRaaS services are also available to provide cross-region replication.

Audits of the Disaster Recovery Services are carried out by internal company teams or third-party external auditors periodically (on demand or ad-hoc basis), depending on the type of assessment.

How are application RPOs and RTOs set?

The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for an application is determined by the business. Business unit IT teams complete application impact analyses (ARAs) for the applications they support, which define the required RTO and RPO for each application based on criticality. They are reviewed and approved by the application support manager, application business owner, and DR Services.

How does the organization improve and introduce innovative techniques for disaster recovery?

The Disaster Recovery Center of Excellence (COE) was established to analyze and establish new methodologies that ensure the recoverability of critical business applications at any time and in ways not previously achievable. The DR COE's objective is to establish world-class standards for advanced architecture design and innovative technology that facilitates enhanced testing and recovery processes, real-time DR status reporting, innovative data center technologies, and DR process automation tools that set us apart from most other companies.

Our Company's Disaster Recovery Services team works with each of the businesses, as well as our Business Resiliency Management (BRM) group, application development teams, MMC Tech

Engineering, and MMC Tech project managers to develop and manage recovery strategies for the technology systems that support our critical business functions. *For additional information, a copy of our* Statement of Recoverability *can be provided upon request. Please contact your account or relationship manager.*

5.1 Equipment Protection

How does your organization protect against natural or man-made hazards such as fire, flood, earthquake, and water damage?

Our company's data centers and server rooms are protected against environmental hazards using fire response protection, moisture detection, and cooling systems, as well as backup and uninterruptable power supply (UPS) systems. For critical data centers, these systems include alarms that are connected to building alarm systems and city services (for instance, fire response units). Other protections include fire extinguishers throughout each facility and routine emergency evacuation exercises.

Does the infrastructure provide built-in redundancy for critical services such as utilities, telecommunications, and electrical service interruptions?

Our company's data centers are configured with redundant power feeds, telecommunications circuits, backup generator power, and uninterrupted power supply (UPS) systems. Server rooms are configured with UPS systems and depending on the facility's size or criticality there may be on-site backup power, such as a generator.

Are equipment protection systems (e.g., generators, UPS systems) tested periodically?

Equipment protection systems are maintained and tested periodically (e.g., quarterly, semi-annually) depending on the system and location.

Describe the protection for power, telecommunications, and other network cabling.

Cable management and conduit systems are utilized as appropriate to allow for proper configurations and to minimize interference problems.

Is there a procedure to ensure that equipment or media may not be taken off-site without prior authorization?

Except for assets that are expected to be routinely taken off-site (e.g., company-provided laptops, or smartphones), server and network equipment may not be moved into or out of our server rooms and data centers without approved change orders in accordance with our change management process.

6 – Business Governance and Compliance

6.1 Legislative, Regulatory, and Contractual Governance

Are there policies and procedures to ensure compliance with applicable legislative, regulatory, and contractual requirements? If yes, is there a documented process to identify and assess regulatory changes that could significantly affect the delivery of products and services?

Yes. Our company's Legal & Compliance team works to monitor and review relevant regulatory developments within their regions and subject-matter areas. They continuously evaluate regulatory developments in real time, track them, and identify their potential impacts on our operations. This proactive approach allows us to stay ahead of changes and understand how they may affect our business. Once the impacts are identified, our Legal & Compliance team works closely with relevant stakeholders across regions and disciplines to implement applicable changes. As an example, we regularly monitor cybersecurity regulations across various jurisdictions. Our team analyzes these regulations and assesses their impact on our cybersecurity practices. When changes are warranted, we promptly update our processes and controls to align with the new requirements. Overall, our robust approach to assessing legislative and regulatory changes allows us to stay in step with the ever-evolving legal landscape and maintain a strong compliance posture across our organization.

Is there an internal audit, risk management, or compliance department, similar management oversight function with responsibility for tracking the resolution of outstanding regulatory or compliance issues?

Our company has appointed and maintains an independent internal audit function that includes an IT Audit team staffed to audit our IT security and operating procedures, using a risk-based approach. Internal Audit helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes regarding:

1. Reliability and integrity of financial and operational information.
2. Effectiveness and efficiency of operations and programs.
3. Safeguarding of assets.

Internal Audit accomplishes its objective through the development and implementation of an annual risk-based audit plan that considers a variety of inputs. This includes risk or control concerns identified by management and responds to the varying dynamics of the business. Internal Audit's annual audit plan is based on a multi-faceted risk assessment and is adjusted to reflect changes, as needed, throughout the year. Internal Audit reports the results to the Marsh McLennan Board of Directors and its audit committee.

Some examples conducted by internal audit include encryption, business application logging, vulnerability management, and NYDFS cybersecurity regulation. Io internal audit.

6.2 Corporate Governance

Is there an Environmental, Social, and Corporate Governance (ESG) program?

We continue to evolve the approach to ESG, overseen by the Marsh McLennan Board. In 2021 we integrated aspects of the Sustainability Accounting Standards Board (SASB), Global Reporting Initiative (GRI), and Taskforce for Climate Related Financial Disclosure (TCFD) within our ESG governance framework. We moved to annual reporting of our ESG having previously reported bi-annually through our Corporate Citizenship Report. A copy of our ESG Report can be found at https://www.mmc.com/about/esg.html.

The Greater Good (our Code of Conduct) requires adherence to the laws and regulations that apply to work that is being undertaken; it requires that staff undertake the requisite training to ensure they understand their responsibilities; to act honestly in all business dealings; to "Speak Up" if staff have a concern about any work-related behavior that may be a violation of the law or The Greater Good; and to raise concerns where necessary. We operate a Confidential Ethics & Compliance Line for use by staff or third parties. The Greater Good emphasizes the requirement to compete ethically including complying with laws related to competition. It covers the need to comply with laws governing international trade, trade sanctions, anti-terrorist financing, export controls, anti-human trafficking, and anti-boycott laws; and includes compliance with anti-money laundering laws.

Is there a compliance program or set of policies and procedures to address bribery, corruption, prohibition of providing monetary offers, incentives, or improper actions that create an unfair advantage in business practices?

Our Code of Conduct, The Greater Good, takes an uncompromising position against bribery.

We have global compliance policies which provide anti-corruption guidance to all our businesses, including:

- Giving and receiving – Gifts.
- Entertainment and Contributions.
- Working With Third Parties, Governments, and Vendors; and
- Understanding Trade Sanctions and Anti-Money Laundering.

The policies are available in multiple languages and posted on our internal websites.

Additionally, our Compliance area:

- Employs heightened due diligence procedures for higher-risk engagements of third parties (e.g., development of business case and assessment questionnaires submitted to and reviewed by our company’s Global Financial Crime team).
- Provide regular training to all employees and new hires globally, including anti-corruption training.
- Regularly monitors and audits the effectiveness of controls in place to mitigate corruption.
- Maintains a global hotline called the MMC Ethics & Compliance Line that any employee or other person may call to anonymously report (where allowable by law) issue of misconduct; and
- Conducts investigations into allegations of misconduct, via the hotline or otherwise, and provides regular oral reports to the Audit Committee of the Board of Directors.

Is there a compliance program or set of policies and procedures that address Anti-trust or Anti-Competitive Business Practices?

We are committed to competing vigorously and fairly for business by providing superior products and services -- not by engaging in improper or anti-competitive practices. We comply with all laws related to competition, antitrust, and obtaining competitive information legally in the countries in which we do business.

Is there a documented policy or set of procedures for Ethical Sourcing?

Procedures are in place to assess the privacy and information and cyber security practices of third-party service providers (e.g., subcontractors, suppliers, or vendors) using questionnaires, meetings, and inspections as deemed necessary by our company and subject to applicable legal and regulatory requirements. Access to data or company systems by such third parties is permitted only after the completion of a risk assessment. Periodic re-assessments of a third party’s security measures are performed using a risk-based approach. Review of third-party contracts and service agreements can include review by our Legal & Compliance, information security, IT internal audit, and other teams as appropriate. Upon such review, contracts will include security and privacy terms and conditions commensurate with the types of services provided by the third party (including contract and temporary personnel).

When making buying decisions staff are asked to consider Ethics and to ensure the consideration is consistent with the spirit of The Greater Good (our Code of Conduct) and other company policies. Employees should never follow a request to do something unethical or unlawful. Where employees are uncertain about aspects of an engagement, they are requested to consult their manager, Legal and Compliance, or to use the MMC Ethics & Compliance Line. Employees are asked to avoid using suppliers that have engaged in unlawful or unethical conduct.

Is there a records retention policy and retention schedule covering paper and electronic records, including email in support of applicable regulations, standards, and contractual requirements?

Our company believes that proper records management is important and takes its responsibilities concerning the handling of our records and data pertaining to our clients seriously. Our Records Retention Policy establishes uniform standards that our colleagues, globally, must follow to properly preserve, retain, and manage paper and electronic records that we create and receive in the ordinary course of business, to comply with our legal, regulatory, business, and contractual requirements. Our Policy also references Records Retention Schedules for our business lines which describe how long to retain company records.

Are there documented policies and procedures that address the prevention of modern slavery and human trafficking?

Our company does not tolerate any form of modern slavery within its operations or the operations of its suppliers. The Greater Good (our Code of Conduct) as well as other policies are in place to minimize the risk of modern slavery or human trafficking and to encourage the reporting of any related concerns (including through our Confidential Ethics and Compliance Line). Our company includes a requirement for compliance with modern slavery legislation in its standards terms and conditions. Suppliers are expected to maintain controls to ensure the risks associated with modern slavery, child and other forced labor are being managed. In some markets, we are required to issue a Modern Slavery Statement and to publish this externally. Our Modern Slavery Policy has been rolled out to staff and is incorporated in the induction training for new hires. There is additional training for staff involved in supply chain activity where the potential for encountering modern slavery is considered higher.

Is there a compliance program and procedures that address health and safety risks?

Our company strives to maintain a safe and healthy work environment for its colleagues, contractors, and visitors and is committed to do all that is reasonably feasible in accordance with industry standards for professional services firms operating in an office environment and in compliance with legislative and regulatory requirements. We strive to eliminate foreseeable hazards that may result in property damage, accidents, personal injury, or illness.

Has the organization complied with the requirements of the NYDFS cybersecurity regulation and/or any other cybersecurity laws?

Our company has robust policies, procedures, and controls, as outlined in this document, for the protection of information, including personal and other nonpublic information. Our company is also subject to various laws and regulations that mandate specific requirements for information security programs.

For example, various entities within our company are “Covered Entities” under the *New York Department of Financial Service’s (NYDFS)* Cybersecurity Regulation, and all have affirmatively certified compliance to the NYDFS Commissioner each year since the Regulation went into effect. This includes conducting an annual risk assessment of covered information systems and deploying risk-based processes and controls to protect nonpublic information and information systems, including multi-factor authentication and other access controls, encryption, systems and network monitoring, business continuity and disaster recovery plans, asset and device management, and a global incident response procedure. MMC also has established processes for overseeing third-party service providers in compliance with the NYDFS regulation.

When we act as a third-party service provider to clients who are themselves Covered Entities under the NYDFS regulation, we can help support the Covered Entities’ compliance needs by utilizing risk-

based access controls for systems housing nonpublic information and encryption of nonpublic information in transit and at rest, and by promptly reporting incidents affecting covered entities' information. See also Section 5 - Information Asset Handling and Encryption for more information.

Our businesses are also subject to various additional global laws and regulations that impose particular requirements on information security programs, including for insurance licensees. Our company's legal, IT, Information Security, Operations, and other teams work together to effectuate compliance with these laws through policies, procedures, and controls, and to impose required cybersecurity and information handling duties on our service providers.

6.3 Mergers & Acquisitions

Our company may acquire other entities in any given year. Most acquisitions include a due diligence period, during which we examine the cybersecurity and privacy capabilities and controls of the target organization. Upon closure, priority is given to assessing and remediating security controls and integrating the acquired entity's personnel and business services, and then to migrating legacy application systems and vendors into our company's data centers, IT infrastructure, and vendor management programs. As such, the various policies and procedures described herein may not *fully* apply to an acquired entity until such entity's systems have been *fully* integrated into our technology infrastructure and all legacy application systems identified for migration have been moved to our data centers or private cloud tenants. Depending on the size and nature of the acquired entity, as well as contractual and regulatory considerations, such integration and migration projects can span one to two years from the close of sale with priority given to higher-risk information and systems, including those covered by applicable regulations.

7 – Data Privacy Program

7.1 General Information

Has the organization developed and maintained a defined privacy program for the protection of personal information collected, accessed, transmitted, processed, disclosed, or retained on behalf of its clients?

Our company recognizes the importance of protecting and managing personal information. As such, the company maintains a comprehensive privacy and data protection program that includes (i) documented internal privacy and protection policies and procedures, (*refer to policies and procedures above for more information*), and (ii) discrete services and tools designed to protect the confidentiality and security of the information the Company processes, transfers, and stores.

Does the privacy program describe the structure of dedicated privacy resources and the coordination of responsibilities of various organizational roles responsible for different aspects of privacy?

Our company has a designated Global Chief Privacy Officer who oversees the Privacy Center of Excellence (COE) and reports to the Deputy General Counsel and Corporate Secretary, with dotted-line reporting to the Chief Information Officer. The Privacy COE oversees dedicated privacy teams covering key regions as well as a centralized Privacy Operations team and the COE members work closely with dozens of data protection coordinators and other members of the legal and compliance teams across the globe who are responsible for privacy matters in their respective jurisdictions. Our company also has a designated European Data Protection Officer.

The Privacy COE is responsible for administering our company's privacy program and overseeing the proper handling and use of personal information across our organization. The COE coordinates closely with Information Technology Information Security, Vendor Risk Management, Procurement, Marketing, HR, and Operations groups in this effort and is overseen by a Global Privacy Coordination Committee comprised of senior global executives from Legal/Compliance, Technology and Operations.

Does the organization have policies and procedures for conducting periodic privacy risk assessments?

Our *Handling Information Appropriately Policy* mandates that new or materially expanded personal data processing initiatives, technologies, and third-party engagements need to complete various risk assessment processes, including a privacy risk assessment (PRA). PRAs involve a review of technical, administrative, and physical safeguards for personal information, confirmation of lawful data use, sharing and ability to support data subject rights, and recommendations for additional protective measures to ensure adherence to company policies, client contractual requirements, and legal regimes pertaining to the processing of personal information. Various regulated entities across our company also complete annual and as-needed risk assessments that feed into a company-wide risk assessment, which informs our ongoing efforts to tailor privacy and security policies and procedures to emerging threats and regulatory requirements. Periodic reassessment of vendors based on risk is overseen by our Vendor Risk Management group.

Have you adopted a specific privacy-by-design procedure?

Yes. Our company requires its businesses and functions to conduct a Privacy Risk Assessment (PRA) before launching or materially altering software applications, information systems, and related initiatives, affecting the collection, use, retention, or disclosure of personal information.

Our PRA process has been enhanced to include GDPR (and relevant data protection laws) Data Protection Impact Assessment (DPIA) requirements and to ensure the risk assessment are adequately embedded across the organization to support Privacy by Design and Privacy by Default.

Does the Company share client information with third-party service providers?

The Company may share client information with third parties in the course of conducting day-to-day business activities in support of the services we extend to clients. Please review the applicable website privacy notices for a list of the categories of third parties to whom we disclose client information. Company policies and procedures require that we have written agreements in place with third parties, and such contracts contain industry-standard privacy and security requirements that are consistent with our internal, legal, and contractual obligations.

Does the organization utilize clean-desk practices?

Yes. We have protocols in place that instruct employees and vendors who process Company data on our behalf to lock their computer screens when stepping away from their desks and to secure all hard-copy materials that contain sensitive or personal information in locked cabinets or drawers when not in use. Our protocols require that paper documents that are no longer needed be securely shredded according to Company retention policies. Generally, wastepaper with client information is disposed of in locked containers, which are collected and shredded regularly.

What controls have been implemented to protect data and the privacy of personal information?

The Company maintains policies and procedures that are based on industry standards and outline responsibilities and requirements for handling, processing, and safeguarding personal and confidential information. The Company also deploys technical, physical, and administrative tools and other safeguards to advance the privacy and protection of Company and client information.

The Privacy and Information Security teams are responsible for communicating and educating colleagues about the policies, programs, and procedures that are in place to protect Company and client personal information from loss or unauthorized use or disclosure.

7.2 Data Handling

Are controls in place to limit the collection of personal information based on the contract between the client and the service provider?

Yes. Our privacy and data protection standards are predicated upon “minimum necessary” requirements; hence, colleagues should only collect and retain data that is required to provide services for the Company and/or clients, and as required by law or as permitted by contract. As a matter of course, we ask that clients do not provide us with more information than is required for us to provide the relevant services to them.

Are there control mechanisms in place to de-identify, mask, or pseudonymize personal data to prevent loss, theft, misuse, or unauthorized access?

Yes. The Company routinely uses such protocols and tools, where appropriate, to safeguard personal and sensitive information. In addition, the Company has an internal De-Identification standard governing the use of such tools and practices.

Regarding employees with access to the client's data, do they sign a confidentiality clause for the processing of personal information?

Employees are subject to employment contracts that include strict confidentiality obligations as well as adherence to The Greater Good, our Code of Conduct, and internal policies or are separately required to accept these obligations. The Code sets forth the non-negotiable standards of business ethics and integrity that apply to every employee.

7.3 Regulatory and Legal Requirements

Global Requirements

Does the Company monitor changes in regulatory requirements in jurisdictions it operates in, and adjust its privacy and information security programs to ensure compliance with the new regulatory requirements?

Yes. The Company's Privacy COE and local Legal & Compliance colleagues closely monitor jurisdictional changes in regional, country and/or state/provincial laws and regulations. Where required, a business impact assessment of a new/amended law or regulation is conducted, and a related regulatory change project is initiated to ensure the Company remains compliant with applicable laws and regulations.

Are periodic internal and/or external audits performed to assess compliance with applicable data protection legislation?

Compliance regularly monitors the effectiveness of our Policies and Procedures by visiting business units and conducting interviews and completing file reviews. This supplements routine audits by our Internal Audit group, which audits generally include compliance-related reviews. Both groups include reviews of privacy-related topics to ensure compliance with applicable laws and regulations.

How do you handle requests from Public Authorities?

Our company routinely receives data requests from local governments and law enforcement agencies. Our general practice is to have such requests handled by our Company General Counsel in consultation with the appropriate subject matter experts. If such a request involves EU or UK personal information, it is handled in accordance with the relevant laws and regulations.

After a thorough search, we have not found any data requests from state security agencies in third countries in relation to EU/UK personal data or seeking data from a jurisdiction other than the one where the data resides.

If such a request were to involve EU or UK personal information, then to the extent that our EU and UK BCRs apply, we are under an obligation to notify the competent Supervisory Authority and suspend responding to such request until the appropriate business privacy leads (supervised by the DPO) have assessed it. This obligation to notify applies unless we are legally prohibited from doing so, having used our best efforts to obtain a waiver of the prohibition to communicate as much information as we can and as soon as possible to a competent Supervisory Authority. We are also required to demonstrate to the competent Supervisory Authority that we have followed appropriate steps to deal with any requests in accordance with our EU and UK BCRs. Where we rely on the standard contractual clauses, we will comply with our obligations (depending on our characterization as controller or processor) to respond to, or cooperate reasonably in supporting, any obligation to comply with or to notify data subjects of such access request, subject to the terms of the commercial agreement in place.

Are all the necessary registrations & contractual agreements in place to allow the processing of data, including the movement of data across jurisdictional borders and/or amongst your affiliates?

Yes. Where required, Company databases are registered in accordance with local country law. With respect to the transfer of personal data between countries, the Company leverages its Binding Corporate Rules program for intracompany EU and UK data transfers and otherwise executes appropriate data transfer agreements, which may include standard contractual clauses, where required.

Does your service involve handling/processing cardholder data and, if so, are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?

The Company does not provide credit card payment processing services. However, in some jurisdictions, we have engaged third-party payment processors to process our clients' premium payments via credit cards. Such third-party payment processors are compliant with the Payment Card Industry Data Security Standard (PCI DSS). In such cases, the company also utilizes protocols such as pause and resume in call recording software to ensure the safety of the PCI data.

Has your Company implemented procedures to permit data subjects, in accordance with applicable laws or policies, to access and correct, amend, or modify their PI, including procedures to authenticate such individuals?

Yes. We have implemented procedures to handle and respond to data subject requests as required under applicable laws and regulations.

European Requirements

Are you certified under the U.S./EU data transfer framework? If not, what lawful data transfer mechanisms does the Company use for European Economic Area (EEA) personal data?

No. The Company is not certified under the Data Protection Framework (DPF) between the U.S. and the EU. However, the Company maintains a European Union (EU) approved Binding Corporate Rules (BCR) and a UK BCR program that allow multinational companies like ours to lawfully transfer personal data from the EEA and the UK to affiliates located outside of the EEA, or the UK, including the U.S. For other transfers of EEA or UK personal data to locations outside the EEA or the UK, the Company relies upon other legal transfer mechanisms (e.g. an adequacy designation of the recipient country or standard contractual clauses) for the cross-border transfers of personal data.

Do you maintain a record of processing activities as required under the EU and UK GDPR and the Swiss FADP?

We maintain a Register of Processing Activities. MMC's internal policies, procedures, standards, technical and other documentation are proprietary and not distributed outside the Company to help us protect the data entrusted to us by our clients, business partners, and employees. The data we process on behalf of the client will be detailed in the relevant contracts.

Please contact your business unit consultant or client relationship manager if you have any questions about the data we hold or process on your behalf.

US Requirements

What steps you have taken to become HIPAA compliant?

The Company does not act as a HIPAA covered entity in respect to its services to clients. To the extent that our businesses receive personal health information from covered entity clients, we comply with our obligations as a business associate. We maintain a HIPAA compliance program that includes standards and procedures designed to help us comply with our obligations under HIPAA, including technical, physical, and administrative safeguards required by HIPAA.

Are you compliant with the California Consumer Privacy Rights Act (CPRA) and other emerging state laws?

Yes. Prior to the CPRA's January 1, 2023, effective date, the Company's Privacy COE initiated a significant regulatory change project to enable compliance with the new California privacy law. This plan included a detailed analysis of our business processes, operations, IT systems/applications, and third-party relationships. Where warranted, new and/or amendments to existing business processes and controls (such as the delivery of privacy notices and enablement of individual data rights) were implemented to ensure compliance with the CPRA.

The Company’s Privacy COE has also assessed and addressed any additional or different requirements associated with the new state laws to allow us to comply with those obligations. This work will continue as new laws and regulations are introduced in the U.S.

END OF DOCUMENT

Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
+1 212 345 5000

VIA EMAIL

Oregon Health Authority's All Payer All Claims (APAC)
Data Review Committee (DRC) members

December 5, 2024

Re: APAC data request from Oregon Health and Science University (OHSU)

The Oregon Health Authority (OHA) is the state agency charged with operating the Health Care Market Oversight (HCMO) program under Oregon Revised Statutes (ORS) 415.500 through 415.900 and Oregon Administrative Rules (OAR) 409-070-0000 through 409-070-0085.

On October 4, 2024, OHA accepted a completed notice of material change transaction from the Oregon Health & Science University (OHSU), describing plans to purchase Legacy Health. OHA is currently conducting a comprehensive review of this proposed transaction.

On November 20, 2024, OHSU submitted an application (https://www.oregon.gov/oha/HPA/ANALYTICS/APAC%20Page%20Docs/6440-APAC-NERA-Material-Change-Transaction.pdf) requesting data from the All Payer All Claims (APAC) program. OHSU's data request states:

> *"The Parties anticipate that OHA may request that the Parties respond to and conduct APAC based analyses in connection with the HCMO review. The Parties have retained NERA Economic Consulting (NERA) to perform any APAC based analyses demanded of them by OHA during the HCMO process. For that reason, NERA is submitting this application on behalf of OHSU and Legacy to ensure the Parties have timely access to the APAC data necessary to respond as may be required by OHA."*

HCMO has not requested that OHSU perform any APAC based analyses or respond to any questions for which it would need APAC data, nor does the HCMO program anticipate making any such requests or demands during the remainder of the comprehensive review.

The HCMO program analyzes APAC data on its own to inform its review of proposed transactions and does not require that transacting parties obtain identical APAC data to participate in such analysis. Thus far, the HCMO program has conducted a number of preliminary and comprehensive reviews of proposed material change transactions. The HCMO program has not asked any entity for an analysis that would require data from the APAC program.

More information about the Health Care Market Oversight program can be found on the program website: https://www.oregon.gov/HCMO. If you have questions or need further information, please contact the Health Care Market Oversight team at hcmo.info@oha.oregon.gov.

Sincerely,

Sarah Bartelmann, MPH
Cost Programs Manager
Oregon Health Authority

New or Amended APAC Data Request Review (custom or OHA Business Associate)

Staff Reviewer: Karen Hampton

DRTS Number: 6440 APAC_NERA_Material_Change_Transaction

Date review completed: 12/4/2024

	Yes	No	N/A	Need more information
Is this a new APAC request?	X			
New APAC Request (skip to next section if amendment request):				
1.1 Project staff contact information provided	X			
1.2 Project technical staff information provided	X			
2.1 Project summary provided with adequate detail to identify a specific unambiguous project				Anticipated that OHA may request parties to conduct APAC based analyses in connection with the HCMO review.
2.2 Research questions provided with adequate detail		X		Intention to respond to OHA questions
2.3 Described planned products and reports derived from requested data	X			
2.4 Project begin and end date provided	X			
2.5 Acknowledgement that APAC data cannot be reused beyond the DUA	X			
2.5 Acknowledgement that data cannot be shared beyond the DUA	X			
3.1ab Data request purpose box checked & description	X			
3.2 Checked box for level of data identifiers	X			
3.3 IRB application, approval memo, end date			X	
4.1 Completed data elements workbook	X			Almost every item requested
4.2 Adequately described how the data elements requested are the minimum necessary				Justification provided for each; since questions unknown, difficult to determine minimum necessary
5.1 Plan provided to prevent re-identification	X			Aggregated; mask small cell sizes
5.2ab Plan to link APAC data to other data source			X	
5.2c Requests OHA to link APAC to other data			X	
5.2d Detailed data linking plan provided			X	
5.3 Provided adequate description of data management, security and data destruction plan	X			
Passes Minimum Necessary Review		X		Waiting confirmation from HCMO on analyses expected from applicants
Recommend management approval		X		
Amendment request for previously approved APAC request (not needed for staff change only):				
Any new data elements requested				

	Yes	No	N/A	Need more information
Any new years of data requested				
Any new project purpose or research questions				
Description of new project purpose				
Completed data elements workbook				
IRB application and approval memo				
Passes Minimum Necessary Review				
Recommend management approval				