UW Medicine
SUPPLY CHAIN

MSA 1420-5430

MASTER SERVICES AGREEMENT
FOR
PROJECT RESOURCES AND STAFF AUGMENTATION FOR INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

BETWEEN
UNIVERSITY OF WASHINGTON AND ON BEHALF OF UW MEDICINE
AND
V GROUP INC

This Master Services Agreement (MSA) for Project Resources and Staff Augmentation for Information Technology (IT) Professional Services is entered into by and between the University of Washington, for and on behalf of itself and UW Medicine ("Client"), as further defined in the Terms and Conditions and **V Group Inc.** ("Contractor").

V GROUP INC
379 Princeton-Hightstown Road, Building 3, Suite 2A,
East Windsor, NJ 08520

Brijesh Ravi
609-371-5400 # 312
brijeshr@vgroupinc.com

Washington State UBI No. 602 555 229
Federal ID No. 52-2175892

The University of Washington is an institution of higher education and an agency of the State of Washington. UW Medicine ("UWM") is an integrated clinical, research and learning health system comprised of multiple entities that are managed together as a health system. UW Medicine consists of the following components: Harborview Medical Center and its associated clinics ("HMC") as managed by UW pursuant to a Hospital Services Contract between the UW and King County; Public Hospital District No. 1 dba Valley Medical Center and its associated clinics ("VMC"); Fred Hutchinson Cancer Center, a separate entity that serves as the Cancer Center of UW Medicine; the University of Washington Medical Center, operating at two separate campuses, Montlake and Northwest, and its associated clinics ("UWMC"); UW Physicians Network dba UW Medicine Primary Care ("UWMPC"); The Association of University Physicians dba UW Physicians ("UWP"), the University of Washington School of Medicine ("UW SoM"), and Airlift Northwest ("ALNW") (each a "UW Medicine Component Unit" and collectively "UW Medicine Component Units").

UW Medicine's Information Technology Services (ITS) department is a shared services organization that supports all of UW Medicine. ITS is responsible for the ongoing support and maintenance of the infrastructure and applications which support all these institutions, along with the implementation of new services and applications that are used to support and further the UW Medicine mission.

Whereas Contractor submitted a response to UW Medicine's RFQQ 1420.

Whereas "Services" means the temporary staffing services of providing Client with one or more temporary employees ("contingent staff") to provide work under Client's management and supervision at a facility or in an environment controlled by Client.

Whereas UWM Information Technology Services ("ITS") Human Resources (HR) is the central point of contact at UWM for hiring clients seeking use of outside temporary staffing services.

Whereas UW Procurement Services is the central point of contact for UW Campus Departments.

In consideration of the mutual promises contained herein, the parties agree that this MSA will be performed in accordance with the following terms and conditions:

A. PURPOSE OF MASTER SERVICES AGREEMENT

The purpose of this Master Services Agreement (MSA) is for Contractor to provide Project Resources and Staff Augmentation for IT Professional Services in four (4) categories: Communications, Education, Project Management and Business Analysis, and Technical (Applications and Technology) on an as needed basis to Client.

B. STATEMENT OF WORK

The Contractor will provide services, and otherwise do all things necessary for or incidental to the performance of work, as set forth in section 4.2 of RFQQ # 1420 dated May 2, 2024, and listed below.

All services shall be performed pursuant to the terms of this MSA and shall be documented in a Statement of Work template (see Exhibit E), SOW established between the Client and the Contractor. This template is subject to change by Client.

I. Services

When consulting services are needed, Client will release a work request to Contractors that have been awarded contract(s) in a particular category. The Statement of Work (SOW) Exhibit E will be sent to the Contractor and will specify the scope of work, the deliverables, the timeline, and any other requirements. A SOW will be awarded to the Contractor from the pre-qualified pool that submitted the best response. A SOW must be executed prior to commencing any work.

1. Primary areas of responsibility include, but are not limited to:
    a. Analyzes customer business and technical requirements and issues and recommend solutions.
    b. Provides manager-level resources to be accountable for all communication, reporting, review, and issues resolution associated with this engagement.
    c. Designs, builds, tests and implements enhancements to meet functional requirements.
    d. Provides production support and ongoing system troubleshooting, maintenance, monitoring, and training; and
    e. Manages process and documentation to support customer needs.

II. End of SOW/MSA

Client does not provide equipment to Contractors except for rare occasions.

1. If Client has issued a laptop or any other equipment, Client will pay the cost of shipment to the Contractor but upon termination of any SOW or MSA, the loaned equipment shall be shipped back at the Contractor's expense within ten (10) business days from date of termination; and
2. If Client does not receive the loaned equipment back within ten (10) business days, Client reserves the right to bill the Contractor for the purchase value of the equipment.

III. Roles and Categories

Exhibit I lists all the categories, along with the corresponding roles, qualifications and experience required for each role.

1. The Contractor shall provide staffing that meets the requirements of each role when requested by Client.

IV. Client reserves the right to add new job categories or roles to the scope of this MSA at any time during the contract period.

V. Immunization

Applies to personnel who will be working onsite at any UW Medicine locations.
Comply with immunization and tuberculosis testing standards. Healthcare Organizations are required to assure compliance with national standards regarding immunizations, verification of immune status, and tuberculosis testing among all healthcare workers. These standards have been established by the Centers of Disease Control and Prevention (CDC). These are required for the protection of UW Medicine's vulnerable patient population.

1. Provides documentation of the following immunizations for personnel assigned to work onsite at UW Medicine.
    a. No active tuberculosis infection.
    b. Immunity to Hepatitis B.
    c. Immunity to Measles (Rubella).
    d. Immunity to Mumps.
    e. Immunity to Rubella (German Measles).
    f. Immunity to Varicella (Chicken Pox); and
    g. Annual Flu Vaccination

VI. Site Security

1. Acknowledge and agree to the requirements in Exhibit F for background checks and medical screening if applicable.
2. Shall be responsible to comply with any updated requirements as they become available.
3. Shall be responsible to remain current with annual vendor management system fees.
4. Shall complete on-line credentialing registration for Contractor's representative(s) conducting business at, visiting, or working remotely in service of the UWM locations prior to visiting any of the UWM facilities. Contractor's representative(s) are required to do the following:
    a. Pre-schedule all visits.
    b. Signs in on the day of the scheduled appointment at one of the vendor management system kiosks located at each UWM location; and
    c. Wears the temporary badge produced by the vendor management system at all times on UWM property. This badge shall be valid for one day only, the day of the scheduled appointment.
        i. Checks out at a vendor management kiosk prior to departing the UWM ITS location; and
        ii. Shall follow any additional security procedures required by specific departments, including but not limited to, Surgical Services, Pharmacy and Radiology

VII. Offshore Storage and Access

Offshore storage of and access to UW Medicine Data must comply with all relevant UW Medicine Compliance Patient Information Privacy policies and UW Medicine Information Security Standards. Because of the heightened privacy and security risks associated with offshore storage and access, the procedures described below must be followed to identify such risks, implement privacy and security controls to reduce risks to an acceptable level, and escalate proposed offshore arrangements to leadership for approval when appropriate.

1. Offshore storage of and access to UW Medicine Data may be considered in the following circumstances:
    a. UW Medicine contracts with a US-based third party that has offshore satellite offices, and employees.
    b. UW Medicine contracts with an offshore third party with limited presence in the USA.

c. An IRB-approved research project that involves offshore collaborators and data sharing which complies with UW Medicine policies, the executed Data Use Agreement, the research protocol, UW Office of Research standards and any other obligations associated with conducting the research (e.g., study sponsor requirements).

2. Offshore storage of and access to UW Medicine Data will not be considered in the following circumstances:
   a. UW Medicine may not provide direct access to an application containing UW Medicine Data (e.g., Epic) with an offshore third party.
   b. UW Medicine has a contract with a US-based vendor and the vendor seeks to subcontract work involving UW Medicine Data to an offshore subcontractor that has no physical presence in the United States.
   c. Offshore storage or access arrangements involving countries deemed safety risks by the UW Medicine Information Security Program.
   d. Offshore storage or access arrangements that would violate an existing contractual obligation or other restriction (e.g., Epic, Boeing ACN).
   e. When the offshore storage or access arrangement includes clinical data received as part of the Clinical Data Exchange Memorandum of Understanding between Fred Hutchinson Cancer Center and the University of Washington unless written approval is obtained from the Joint Clinical Data Oversight Committee or the data sharing occurs pursuant to a mutually agreed upon written offshore data policy.

VIII. Conversion Rate
Client does not engage in Contract-To-Hire agreements. If a Contractor wishes to become a Client's employee, they will be required to apply for positions and be selected through UW's open recruitment process. Client does not agree to pay conversion fees if a Contractor becomes a UW employee through the open recruitment process, regardless of the new employee's start date, position in which they are hired, and in which department they are hired.

IX. Acknowledgment
1. Acknowledges that all consultants shall abide by all the Client's rules and regulations.

Exhibit A contains the general terms and conditions ("UW Medicine General Terms and Conditions") governing this MSA.

Quality Assessment and Performance Improvement: In accordance with The Joint Commission (TJC) Leadership (LD.)04.03.09, Contractor agrees to work in collaboration with UW Medicine in the review and development of relevant quality assurance plans as opportunities for performance improvement are identified. This may include participation in quality assurance activities including event reviews, studies, plans of corrective action for deficiencies identified by either signatory to this MSA or third-party regulatory agencies. Contractor agrees to provide periodic reporting on the outcome of process changes and corrective actions to UWM Business Manager/ Department Manager named in the **MSA MANAGEMENT** Section below.

C. TERM OF MSA

1. The initial Term of this MSA shall be for three (3) years with fixed and firm pricing, commencing on March 1, 2025, and expiring on February 28, 2028.
2. At the Client's sole discretion, the MSA term may be extended by three (3) additional two-year 2-year) extension options, based on the Contractor's satisfactory performance in meeting the requirements of this MSA, not to exceed a total MSA term of nine (9) years. This shall be affected by Client giving written notice of the intent to extend the MSA to Contractor at least thirty (30) days prior to the then current expiration date of the initial term or the then current extension term of this MSA.
3. The term of any Staffing Level and Cost as included in Exhibit H shall not exceed the term of this MSA, including any mutually agreed upon extension.

4. At the Client's sole discretion, the MSA term may be extended on a month-to-month basis for up to an additional three (3) months after the final expiration date with the current Exhibit H pricing, terms, and conditions.

D. COMPENSATION AND PAYMENT

1. Client shall pay for the rates per role in Exhibit H (Contractor's Staffing Level & Cost); and
2. Rates shall not be increased during the initial term of the MSA.

E. INVOICE REQUIREMENTS FOR SERVICES

Client requires all incoming invoices to meet our standard billing requirements to ensure accurate, efficient, and timely processing of vendor invoices. A purchase order is required for the acquisition of all services. All incoming invoices must reference a valid purchase order. Our standard payment terms are Net30 after a correctly completed invoice is received in Accounts Payable. A separate invoice is required for each purchase order and must be received within 30 days of receipt of goods or services. As a general rule, Client does not pay from statements.

Invoice Requirements

- Valid Client purchase order
  - Bill to must reflect Client entity from which the purchase order was issued
  - Only Client purchase orders can be billed
- Remittance Detail
  - Vendor/payee name, remittance address, and payment terms
    - W9 or supplier registration form complete, consistent with payee/vendor name
    - Tax id and name accurately matches with information on file with IRS
  - Invoice number, invoice date, sub-total, tax (if applicable), grand total
- Purchase line detail – must mirror PO
  - Description of item, purchase order line #, item catalog #, quantity, unit of measure, price per unit, tax, extended line amount
  - Description of service, MSA number, equipment serial number (if applicable), service date(s)

Incorrectly completed invoices will be returned to vendor with a request to issue a new invoice with a current date and required information.

Paper invoices should be addressed correctly and mailed/emailed to the Accounts Payable department for the Client's entity listed on the purchase order.

UW Medicine bill-to:	
PO BOX 50014 Seattle, WA 98145	Invoices: uwashington@ghxinvoicing.com Inquiries: UWM-AP@uw.edu

UW bill-to:	

UW Medicine
SUPPLY CHAIN

University of Washington 4328 Brooklyn Ave NE Box 354967 Seattle, WA 98195-4967	Invoices: uwashington@ghxinvoicing.com Inquiries: PCSHelp@uw.edu

The Client is committed to pursuing GHX Electronic Data Interchange (EDI) invoicing with all our trading partners. For more information on utilizing this invoicing option, please contact Accounts Payable.

F. MSA MANAGEMENT

1. Contacts for University of Washington and UW Medicine and the Contract Manager for the Contractor are listed below and shall be the contact persons for all communications regarding the performance of this MSA. The Contract Manager for the Contractor shall competently and efficiently supervise and coordinate the implementation and completion of all MSA requirements specified within this MSA.
2. Contractor shall immediately notify UWM Supply Chain MSA Contact listed below in writing of any change of its designated Contract Manager assigned to this MSA and to UW Medicine Supply Chain at scmhelp@uw.edu;
3. Any notice, demand, or any other communication required or permitted to be given under this MSA or applicable law, shall be effective only if it is in writing and signed by the applicable party, properly addressed, and either delivered in person, or by a recognized courier service, or deposited with the US Postal Service as first class mail, postage prepaid certified mail, return receipt requested, to the UW Medicine Supply Chain, 7543 63rd Ave. NE, Bldg. 5B, Seattle, WA 98115 or sent by electronic mail to scmhelp@uw.edu.

DEPARTMENT MANAGER / BUSINESS MANAGER FOR UWM SUPPLY CHAIN	MSA MANAGER for CONTRACTOR is:
Lisa Walton 7543 63rd Ave NE Bldg. 5B Box 359795 Seattle, WA 98115 Phone: 206.597.9559 E-mail: lw225@uw.edu	Brijesh Ravi 379 Princeton-Hightstown Road, Bldg 3, Suite 2A, East Windsor, NJ 08520 Phone: 609-371-5400 #312 E-mail:**brijeshr@vgroupinc.com**
DEPARTMENT MANAGER / BUSINESS MANAGER FOR UWM ITS HR	**DEPARTMENT MANAGER / BUSINESS MANAGER FOR UW PROCUREMENT SERVICES**
Vivian Leu 325 9th Ave Seattle, WA 98104 Phone: 206.668.9469 E-mail: viviankl@uw.edu	Dawn Lake 4328 Brooklyn Ave NE Box 354967 Seattle, WA 98195-4967 Phone: 206.543.0814 E-mail: dawnlake@uw.edu

G. UW MEDICINE SITE SECURITY

1. Contractor shall register in the UW Medicine vendor management system (See Exhibit F) and comply with all applicable UW Medicine policies and/or procedures defined during the registration process, including but not limited to, credentialing, immunizations, confidentiality, and integrity.
2. Contractor shall be responsible to comply with any updated requirements as they become available.
3. Contractor shall be responsible to remain current with annual vendor management system fees.
4. Contractor representative(s) conducting business or visiting any of the UWM's facilities must complete on-line credentialing registration prior to visiting any of the Hospital(s). Contractor representatives are required to do the following:
   i. Pre-schedule all visits.

ii. Sign in on the day of the scheduled appointment at one of the vendor management system kiosks located at each UWM location.

iii. Wear the temporary badge produced by the vendor management system at all times on Hospital(s) property. This badge shall be valid for one day only, the day of the scheduled appointment.

iv. Check out at a vendor management kiosk prior to departing the UWM location.

5. Contractor and/or Contractor Representative(s) must follow any additional security procedures required by specific departments, including but not limited to, Surgical Services, Pharmacy and Radiology.
6. Contractor and/or Contractor Representatives' failure to follow any vendor management policies will result in disciplinary action up to and including permanent exclusion from all UW Medicine Component Unit facilities listed on page 1; and
7. UW Medicine agrees that in the event of a Security Event (a " Security Event" shall mean any act or omission that compromises the security, confidentiality, availability or integrity of Contractor or it's personnel's Personally Identifiable Data (as defined under applicable law) ("Contractor Data")) by UW Medicine's vender credentialing provider that relate to the protection of the security, confidentiality, availability or integrity of Contractor Data, UW Medicine will notify Contractor within 48 hours of UW Medicine being made aware of such a Security Event, and indemnify Contractor for any losses, costs, expenses, liabilities, penalties or fines resulting from such Security Event.

H. ORDER OF PRECEDENCE

Each of the Exhibits listed below is by this reference hereby incorporated into this MSA. In the event of an inconsistency in this MSA, the inconsistency shall be resolved by giving precedence in the following order:

- Applicable Federal and State of Washington statutes and regulations
- Special terms and conditions as contained in this basic MSA instrument
- Exhibit A – UW Medicine General Terms and Conditions
- Exhibit B – UW Business Associate Agreement
- Exhibit C – UW Data Processing Agreement (DPA)
- Exhibit D – UW IT Security Terms and Cyber Liability Rider
- Exhibit E – Statement of Work Template
- Exhibit F – Vendor Credentialing/Green Security Information
- Exhibit G – Workday Requirements
- Exhibit H – Contractor's Staffing Level and Cost
- Exhibit I - List of Categories and Roles
- UW Medicine's Request for Qualifications and Quotations #1420 dated May 2, 2024, and terms and conditions therein, its Amendments and incorporated herein by reference
- Contractor's proposal on or about June 28, 2024, incorporated herein by reference
- Any other provision, term or material incorporated herein by reference or otherwise Incorporated.

I. ENTIRE AGREEMENT

This MSA including referenced exhibits represents all the terms and conditions agreed upon by Client and Contractor. No other understandings or representations, oral or otherwise, regarding the subject matter of this MSA shall be deemed to exist or to bind the parties.

J. CONFORMANCE

If any provision of this MSA violates any statute, regulation, or rule of law, it is considered modified to conform to that statute, regulation, or rule of law.

K. APPROVAL

UW Medicine
SUPPLY CHAIN

This MSA shall be subject to the written approval of Client's authorized representative(s) and shall not be binding until so approved and signed below. The MSA may be altered, amended, or waived only by a written amendment executed by all parties.

UW Medicine
SUPPLY CHAIN

AUTHORITY TO BIND

This MSA is executed by persons signing below who warrant they have the authority to execute this MSA.

UNIVERSITY OF WASHINGTON AND ON BEHALF OF UW MEDICINE

DocuSigned by:
Lynn Magill
(signature)
1E8BC48E52D9459...

Lynn Magill
(printed name)

Assistant Director
(title)

2/21/2025
(date)

V GROUP INC

DocuSigned by:
Brijesh Ravi
(signature)
3DD62DA04FC3B489...

Brijesh Ravi
(printed name)

Manager - Consulting Service
(title)

2/25/2025
(date)

UW Medicine
SUPPLY CHAIN

EXHIBIT A

GENERAL TERMS AND CONDITIONS

Revised February 2024

1. DEFINITIONS – As used throughout this Master Services Agreement (MSA), the following terms shall have the meaning set forth below:

   a. "Master Services Agreement" means purchase order and/or the entire written agreement between Client and Contractor, including any exhibits, attachments, and other materials incorporated by reference.

   b. "Contractor" means that firm, provider, organization, individual or other entity providing goods and/or performing service(s) under this MSA.

   c. "Debarment" means an action taken by a federal official to exclude a person or business entity from participating in a transaction involving certain federal funds.

   d. "Ownership" includes the right to copyright, patent, and register, and the ability to transfer, these rights.

   e. "Client" shall mean the University of Washington, for and on behalf of itself and UW Medicine. For the purposes of this MSA, UW Medicine consists of the following components: Harborview Medical Center and its associated clinics ("HMC") as managed by UW pursuant to a Hospital Services Contract between the UW and King County; Public Hospital District No. 1 dba Valley Medical Center and its associated clinics ("VMC"); Fred Hutchinson Cancer Center, a separate entity that serves as the Cancer Center of UW Medicine; the University of Washington Medical Center, operating at two separate campuses, Montlake and Northwest, and its associated clinics ("UWMC"); UW Physicians Network dba UW Medicine Primary Care ("UWMPC"); The Association of University Physicians dba UW Physicians ("UWP"), the University of Washington School of Medicine ("UW SoM"), and Airlift Northwest ("ALNW") (each a "UW Medicine Component Unit" and collectively "UW Medicine Component Units").

   f. "RCW" means the Revised Code of Washington. All reference in this MSA to RCW chapters or sections shall include any successor or replacement statute.

   g. "Regulation" means any federal, state, local, UW or UW Medicine regulation, law, rule, or ordinance.

   h. "Subcontract" means any separate agreement or contract between Contractor and an individual or entity ("Subcontractor") to perform all or portion of the duties and obligations that Contractor is obligated to perform pursuant to this MSA.

   i. "Subcontractor" means one not in the employment of Contractor, and/or entity that owns or controls, is owned or controlled by, or is under common ownership or control of Contractor, who is performing all or part of those services under this MSA under a separate contract with Contractor and/or any person or entity appointed by or on behalf of Contractor to carry out any portion of the Work. The terms "Subcontractor" and "Subcontractors" means Subcontractor(s) in any tier. Control for the context of this paragraph shall mean the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting security, by contract or otherwise.

   j. "UW" means the University of Washington, any division, section, office, unit, or other entity of the University of Washington, or any of the officers or other officials lawfully representing the University of Washington.

   k. "Work" refers to all services, work, and activities involved in providing the materials, work product deliverables, or other obligations that are the subject of the MSA.

2. ACCESSIBILITY - Contractor represents that it is committed to promoting and improving accessibility of all its products as specified in the University of Washington IT Accessibility Guidelines (https://uw.edu/accessibility/guidelines), and will remain committed throughout the term of this MSA. If the Services are not in conformance with all applicable federal and state disability laws, policies, and regulations as of the Effective Date, Contractor shall use reasonable efforts to update the Services so as to be in conformance therewith. In the event any issues arise regarding Contractor's compliance with applicable federal or state disability laws, policies and regulations, University may send communications to Contractor as specified who will assign a person with accessibility expertise to reply to University within two (2) business days.
3. ADVANCE PAYMENTS PROHIBITED - No payments in advance of or in anticipation of services to be provided under this MSA shall be made by the UW except as authorized by law.
4. AMENDMENTS
    a. This MSA may be amended by mutual agreement of the parties. No material alterations in any of the terms, conditions, delivery, price, quality, quantity, or specifications shall be effective unless the alteration is expressly acknowledged and accepted in writing Client.
    b. Automatic extensions and renewals are not authorized unless stated in writing and included in MSA issued by Client.
5. ANTITRUST ASSIGNMENTS – Contractor hereby assigns to Client any and all claims for price fixing or overcharges relating to services and/or materials purchased under this MSA, except as to overcharges that result from antitrust violations commencing after the price is established under this MSA and are not passed on to Client under an escalation clause.
6. ASSIGNMENT – The Work to be provided under this MSA, and any claim arising thereunder, is not assignable or delegable by Contractor without prior written consent of Client. Provision of monies due under this MSA shall only be assigned with the prior permission of Client.
7. ATTORNEYS' FEES – In the event of litigation or other action brought to enforce the MSA terms, each party shall bear its own attorney's fees and costs.
8. BREACH, DEFAULT, TERMINATION
    a. Breach: A breach of a term or condition of this MSA shall mean any one or more of the following events:
        i. Contractor fails to perform the services by the date required or by a later date as may be agreed to in a written amendment to this MSA signed by Client.
        ii. Contractor breaches any warranty or fails to perform or comply with any term or agreement in this MSA.
        iii. Contractor makes any general assignment for the benefit of creditors.
        iv. In the UW's sole opinion, Contractor becomes insolvent or in an unsound financial condition so as to endanger performance hereunder.
        v. Contractor becomes the subject of any proceeding under any law relating to bankruptcy, insolvency or reorganization, or relief from creditors and/or debtors.
        vi. Any receiver, trustee, or similar official is appointed for Contractor or any of Contractor's property.
        vii. Contractor is determined to be in violation of any regulations and that such determination, in the Client's sole opinion, renders Contractor unable to perform any aspect of this MSA.
    b. Default: Contractor may be declared in default for a material breach of any term or condition.
    c. Termination for Convenience: Client may terminate this MSA or SOW, in whole or in part, at any time and for any reason by giving thirty (30) calendar days written notice to Contractor.

Termination charges shall not apply unless they are mutually agreed by both parties. Where termination charges are applicable, both parties agree to negotiate in good faith and to limit the extent of negotiations to valid documented expenses incurred by Contractor prior to date of termination. Should the parties not agree to a satisfactory settlement, the matter shall be handled in accordance with Section 18 ("Dispute Resolution").

d. Termination for Breach and/or Default: Except in the case of delay or failure resulting from circumstances beyond the control and without the fault or negligence of Contractor or Contractor's suppliers or subcontractors, Client shall be entitled, by written or oral notice, to cancel and/or terminate this MSA in its entirety or in part for breach and/or for default of any of the terms herein and to have all other rights against Contractor by reason of Contractor's breach as provided by law.

e. Termination Due to Change in Funding: If the funds Client) relied upon to establish this MSA are withdrawn, reduced, or limited, or if additional or modified conditions are placed on funding by the entity funding Client, Client may immediately terminate this MSA by providing written notice to Contractor. The termination shall be effective on the date specified in the termination notice.

f. Termination by Mutual Agreement: Client or Contractor may terminate this MSA in whole or in part, at any time, by mutual agreement.

9. COMPLIANCE WITH APPLICABLE LAW – At all times during the term of this MSA, Contractor shall comply with all applicable federal, state, and local laws and regulations, including but not limited to, nondiscrimination laws and regulations. To the extent Contractor will provide performance to Client, Contractor agrees to comply with all Client's Compliance policies and the UW Medical Center Corporate Compliance Plan. For additional information: http://depts.washington.edu/comply/policies/ or contact comply@uw.edu. Any violation of this section would be considered a material breach of this MSA. Contractor agrees to indemnify and hold Client harmless from any and all damages or claims caused by Contractor's failure to comply with the law.

10. COMPLIANCE WITH CIVIL RIGHTS LAW – Contractor and Subcontractor shall abide by the requirements of 41 CFR§§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability.

11. COMPLIANCE WITH NONDISCRIMINATION REQUIREMENT – During the term of this MSA, Contractor shall not discriminate on the bases enumerated at RCW 49.60.530(3). In addition, Contractor shall give written notice of this nondiscrimination requirements to any labor organization with which Contractor has a collective bargaining or other agreement. In the event Contractor enters into any subcontract, Contractor shall include this clause therein.

12. CONFIDENTIALITY – Contractor may use information gained by reason of this MSA only for the purpose of this MSA. Contractor shall not disclose, transfer, or sell any such information to any party, except as provided by law. Contractor shall maintain the confidentiality of all confidential information gained by reason of this MSA and shall return or certify the destruction of such information if requested in writing by Client.

    Nothing in this MSA shall prohibit Client from sharing confidential information with other Client affiliate and alliance partners.

13. CONFLICT OF INTEREST – Notwithstanding any determination by the Executive Ethics Board or other tribunal, Client may, in their sole discretion, by written notice to Contractor terminate this MSA if it is found after due notice and examination by Client that there is a violation of the Ethics in Public Service Act, Chapter 42.52 RCW, or any similar statute involving Contractor in the procurement of

this MSA, or provision of goods or services under this MSA. If this MSA is terminated as provided herein, Client shall be entitled to pursue the same remedies against Contractor as they could pursue in the event of a breach of this MSA by Contractor. The rights and remedies of Client provided for in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law.

14. COPYRIGHT AND INTELLECTUAL PROPERTY PROVISIONS – Unless otherwise provided, all Materials produced under this MSA shall be considered "works for hire" as defined by the U.S. Copyright Act and shall be owned by Client. "Materials" means all information in any format that includes, but is not limited to, data, reports, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, and sound reproductions Hospitals shall be considered the author of such Materials. If the Materials are not considered "works for hire" under the U.S. Copyright laws, Contractor hereby irrevocably assigns all right, title, and interest in Materials, including all intellectual property rights, to Client effective from the moment of creation of such Materials.

    For Materials that are delivered under this MSA, but that incorporate pre-existing materials not produced under this MSA, Contractor grants to Client a nonexclusive, royalty-free, irrevocable license (with rights to sublicense others) in such Materials to translate, reproduce, distribute, prepare derivative works, publicly perform, and publicly display. Contractor warrants and represents that Contractor has all rights and permissions, including intellectual property rights, moral rights, and rights of publicity, necessary to grant such a license to Client. Client shall receive prompt written notice or claim of copyright infringement received by Contractor with respect to any Materials delivered under this MSA. Client shall have the right to modify or remove any restrictive markings placed upon the Materials by Contractor.

15. COVENANT AGAINST CONTINGENT FEES – Contractor warrants that no person or selling agent has been employed or retained to solicit or secure this MSA upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee, except. g bona fide employees or bona fide established agents, as defined in the Federal Acquisition Regulations ("FAR") Subpart 3.4, maintained by Contractor for the purpose of securing business. Hospitals shall have the right, in the event of breach of this. clause by Contractor, to annul this MSA without liability or, in their discretion, to deduct from this MSA price or consideration or to recover by other means the full amount of such commission, percentage, brokerage, or contingent fee.

16. DATA PROCESSING AGREEMENT ("DPA") – If, during the course of the performance, administration, or maintenance of this MSA, or any extension or renewal thereof, Contractor acquires, uses, or otherwise obtains access to "University Personal Data ("UPD")," Contractor must implement appropriate administrative, technical, and physical security measures to protect that UPD. Contractor, at the sole discretion of Client, shall be required to execute a DPA that shall be attached to this MSA as an exhibit, attachment, or written amendment.

17. DELIVERY –Intentionally Omitted,

18. DELIVERY RESTRICTIONS – Contractor shall comply with all Client parking instructions, oral and written, and park in designated parking areas.

19. DISPUTE RESOLUTION – If a dispute arises out of or relates to this MSA, or the breach thereof, and if the dispute cannot be settled through negotiation, the parties agree first to try in good faith to settle the dispute by mediation administered by the American Arbitration Association under its Commercial Mediation Procedures before resorting to litigation or some other dispute resolutions procedure.

20. FEDERAL EXCLUSION AND DEBARMENT – Contractor, by accepting the terms of this MSA, certifies that Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions. Contractor shall include the above-mentioned requirement in any and all subcontracts into which it enters. In the event that Contractor becomes debarred, suspended or ineligible from

participating in transactions, Contractor shall notify Client and UW Medicine Supply Chain in writing within three (3) working days of an event. To the extent that Contractor will provide performance to Client, Contractor hereby represents and warrants that Contractor is not currently, and at no time has been sanctioned, debarred, suspended, or excluded by any federally funded healthcare program, including without limitation, Medicare, and Medicaid. Contractor hereby agrees to immediately Client and UW Medicine Supply Chain of any threatened, proposed, or actual sanctions, debarment action, suspension, or exclusion by or from any federally funded healthcare program during the term of this MSA.

21. FORCE MAJEURE – Neither Contractor nor Client shall be liable for damages arising from causes beyond reasonable control and without the fault or negligence of either Contractor or the Client. Such causes, may include, but are not restricted to, acts of God or of the public enemy, acts of a governmental body other than Hospitals acting in either its sovereign or contractual capacity, war, explosions, fires, floods, earthquakes, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the delays must be beyond the reasonable control and without fault or negligence of Contractor, Client, or their respective Subcontractors.

22. GOVERNING LAW – This MSA shall be interpreted in accordance with the laws of the State of Washington, and the venue of any action brought hereunder shall be in the Superior Court for King County.

23. HIPAA BUSINESS ASSOCIATE – If, during the course of the performance, administration, or maintenance of this MSA, or any extension or renewal thereof, Contractor acquires, uses, or otherwise obtains access to Protected Health Information ("PHI"), as that term is defined in the UW Business Associate Agreement, incorporated herein, and 45 CFR Parts 160 and 164, then Client and Contractor agree that Contractor is a "Business Associate" as defined in 45 CFR 160.103 and that all the terms and conditions of the UW's Business Associate Agreement shall apply. Contractor shall not use or disclose PHI except as explicitly permitted or required by this MSA or as required by law. See Exhibit B University of Washington Business Associate Agreement which can also be found at the following website: http://depts.washington.edu/comply/compliance-programs/hipaa-program/business-associates/.

24. INDEMNIFICATION – Contractor shall indemnify, defend, and hold the UW, the Board of Regents of the University of Washington, Client, and their officers, employees, students and agents, harmless from and against all claims for damages, costs (including attorney's fees), or liability, relating to the death or injury to any persons or the damage of any property resulting from or arising out of the acts or omissions of Contractor or its employees, agents, or Subcontractors in connection with this MSA.

    Contractor expressly agrees to indemnify, defend, and hold harmless Client for any claim arising out of or incident to Contractor's or any Subcontractor's performance or failure to perform this MSA.

    Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify UWM, the Board of Regents of the UW, and their officers, employees, students, and agents as provided herein.

    Client shall indemnify, defend, and hold Contractor harmless against any damage, cost, or liability, including reasonable attorney's fees, for all injuries to persons or property arising from negligent acts or omissions attributable to that specific Client or its employees or agents.

    In no event shall Client be required to indemnify Contractor for any injury to person or property that is not attributable to an act or omission by that specific Client.

25. INDEPENDENT CONTRACTOR – The parties intend that an independent contractor relationship is created by this MSA. Contractor and his or her employees or agents performing under this MSA are not employees or agents of Client. Contractor, his or her employees, or agents performing under this MSA will not hold himself/herself out as, or claim to be, an officer or employee of the University of Washington, Client or of the State of Washington by reason hereof, or act as an attorney in fact, nor will Contractor make any claim of right, privilege or benefit that would accrue to such employee. Conduct and control of the work will be solely with Contractor.

26. INFRINGEMENTS – Contractor agrees to defend, indemnify, and hold harmless Client against all claims for patent, copyright, or franchising infringements arising from the purchase, installation, or use of material ordered under this MSA, and to assume all expense and damage arising from such claims.

27. INSPECTION – In addition to any rights of access or inspection that may be included in the Special Terms and Conditions (MSA document), Contractor shall provide reasonable access to Contractor's place of business, Contractor records, and client records, to Client and to any authorized agent of the State of Washington or the federal government in order to monitor, audit, and evaluate Contractor's performance and compliance with applicable regulations, and these MSA terms during the term of this MSA and for one-year (1-year) following completion, termination or expiration of this MSA. If any litigation or audit is started before the expiration of the one-year (1-year) period, the records shall be retained until all litigation, claims, and/or audit findings involving the records have been resolved.

28. INSURANCE – If Contractor's performance of this MSA will involve Work falling into any of the categories enumerated within this section, Contractor shall at its own expense maintain in force with insurance companies acceptable to the University the kinds of insurance and minimum amounts of coverage set forth in subsection "a" through "f."

    Cognizant of the variety of policy forms currently within the insurance industry, the coverage provided under this section may be maintained in one or more types of insurance policies. However, regardless of the types of types and forms all policies shall:

    i. Name the Board of Regents of the University of Washington as an additional insured and contain an appropriate severability of interests' clause. This requirement is waived for Professional Liability Policies.

    ii. Include a waiver of subrogation in favor of the University.

    iii. Include cross-liability coverage.

    iv. Be primary as to any other insurance or self-insurance programs afforded to or maintained by the University.

    Upon request, Contractor shall, prior to the commencement of Work under this MSA, provide UW Medicine Supply Chain Contracting at **SCMHELP@UW.EDU** with a certificate of insurance evidencing proof of insurance coverage, and shall name the Board of Regents of the UW as an additional insured. The additional insured endorsement may be either specific to the UW or may be "blanket" or "automatic" addressing any person or entity as required by the MSA.

    Client reserves the right to require additional types of insurance, and/or higher insurance limits, as circumstances require.

    Contractor shall maintain insurance of at least the following types and amounts:

    a. Commercial General Liability Insurance

        For service MSA in which Contractor will perform a significant portion of Work under this MSA on Client's campuses, within Hospitals' or UW facilities, in contact with Client's employees or UW students, or upon request, Contractor shall maintain Commercial General Liability Insurance ("CGL"), and provide proof of such insurance, upon request, in no less than the following amounts:

        i. $1,000,000 per occurrence.

        ii. $3,000,000 aggregate.

        iii. $100,000 fire legal liability.

b. Automobile Liability Insurance:

For MSA including services delivered pursuant to this MSA involving the use of vehicles, either owned, unowned or hired by Contractor, Contractor shall maintain Automobile Liability Insurance, and provide proof of such, in the following amount:

i. $1,000,000 per occurrence; owned, unowned and hired vehicles shall be covered.

ii. Contractor may provide Combined Single Limit for bodily injury and property damage.

c. Professional Liability/Errors and Omissions Insurance, including Internet Professional Liability:

i. For services delivered pursuant to this MSA, either directly or indirectly that involves or requires professional services, skill, and/or judgment, or upon request, Contractor shall maintain Professional Liability/Errors and Omissions Insurance, and provide proof of such upon request in the following amounts:

1. $2,000,000 per claim.

2. $3,000,000 aggregate.

ii. For Internet Professional Liability, relevant policies must include coverages for claims arising out of a failure of the insured's internet professional services or claims arising out of the rendering or failure technology services by insured; claims arising from the failure of insured technology products (including hardware and software) to perform its intended function or purposes, and; claims arising from insured security / privacy controls failure including but not limited to: failure of contractor to prevent the transmission of Malicious Code; failure to prevent unauthorized host or network use; failure to prevent unauthorized host or network access; failure to handle, manage, store, destroy, or otherwise control University data (data that is provided by or processed at the direction of the University); failure to prevent collection of protected personal information.

d. Foreign Liability Insurance

i. For services provided under this MSA which will be performed outside of the United States, or upon request, Contractor shall maintain the following types and levels of insurance, and provide proof of such upon request:

1. International Commercial General Liability coverage with a limit of at least $5,000,000 per occurrence, including products/completed operations coverage.

2. International voluntary workers' compensation coverage per statutory requirements.

3. International automobile liability insurance with limits of at least $1,000,000 per occurrence; Contractor shall submit to UW Medicine Supply Chain Contracting within 15 days of the contract effective date, a certificate of insurance that outlines the coverage and limits defined in this section. Contractor shall submit renewal certificates as appropriate during the term of the MSA.

e. Cyber Liability/ID Theft and Extortion Insurance

i. For services provided under this MSA which include the use of the UW PDPA and/or the UW's Business Associate Agreement, Contractor shall maintain Cyber Liability/ID Theft and Extortion Insurance with limits of at least $2 million each claim and in the aggregate.

ii. The cyber risk/privacy policy shall provide coverage for (i) liability incurred from alleged or actual theft, dissemination, and/or use of personal or confidential information and any related first party forensic and legal costs, required to investigate the cyber incident; (ii) network security liability arising from the unauthorized access to, use of, or tampering with computer systems, including hacker attacks or inability of an authorized third party to gain access to services, including denial of service, unless caused by a mechanical or electrical failure; (iii) liability arising from the introduction of a computer virus into, or otherwise causing damage to,

a customer's or third person's computer, computer system, network, or similar computer related property and the data, software, and programs thereon; (iv) any government investigations resulting from the alleged or actual disclosure of personal or confidential information or network security liability event; and (v) non-physical business interruption.

f. Worker's Compensation – as required by statute.

29. LICENSING, ACCREDITATION AND REGISTRATION – Contractor shall comply with all applicable local, state, and federal licensing, accreditation, and registration requirements and standards necessary for the performance of this MSA.

30. LIENS, CLAIMS AND ENCUMBRANCES – Contractor warrants and represents that all the services provided herein are free and clear of all liens, claims, or encumbrances of any kind.

31. LIMITATION OF LIABILITY – Client shall not be liable to Contractor or to any Subcontractor, regardless of the form of action, for any consequential, incidental, indirect, or special damages, or for any claim or demand based on a release of information, or patent, copyright, or other intellectual property right infringement. This section does not modify any specific agreement regarding liquidated damages or any other conditions as are elsewhere expressly agreed to between the parties.

32. ORDER IDENTIFICATION - All invoices, and other written documentation affecting any services delivered under this MSA shall contain the applicable purchase order number. . Invoices will not be processed for payment until all services invoiced are provided.

33. ORDER OF PRECEDENCE - In the event of any inconsistencies or conflicting terms and conditions in this MSA, such inconsistency or conflict shall be resolved by giving precedence in the following order: federal, state or local laws or regulations, the UW Medicine special terms and conditions, the UW Medicine General Terms and Conditions Federal Flowdown Terms and Conditions, if applicable. Contractor's terms proposed are rejected, unless otherwise provided in writing by UW Medicine Supply Chain Contracting.

34. MISCELLANEOUS FEES/CHARGES –Client reserves the right to short pay invoices that include unidentified or miscellaneous fees and charges not included in Contractor's quote, proposal, or MSA with the Client. Miscellaneous fees/charges may include, but are not limited to tariffs, special handling or packaging, fuel surcharge, compliance charge, paper invoice fee, merchant bank fee, energy surcharge, additional time fee, etc.

35. PAYMENT, CASH DISCOUNT –Client shall not process invoices for payment, and the period of computation for cash discount will not commence until Client receives a properly completed invoice or receives and accepts invoiced items, whichever is later. If an adjustment in payment is necessary due to damage or dispute, the cash discount period shall commence on the date final approval for payment is authorized. If Purchaser fails to timely pay, Contractor may invoice a minimum of $1 or a maximum of 1% per month on the amount overdue (RCW 39.76.011). Payment shall not be considered late if a check or warrant is available or mailed within the time specified, or if no terms are specified, within thirty (30) days from date of receipt of a properly completed invoice for goods or services, whichever is later.

    UWMC utilizes a Bank of America ePayables credit card for purchase order transactions. Contractors will be expected to accept payment via this method, if requested, at no additional charge to UWMC. More information about the ePayables process can be found at http://f2.washington.edu/fm/ps/epayables.

    HMC's utilizes JP Morgan Chase Single Use Account ("SUA") credit card for purchase order transactions. Contractors will be expected to accept payment via this method, if requested, at no additional charge to HMC. Contractors accepting SUA payments will be paid Net15 instead of our typical Net30. Additional information about the SUA may be requested by emailing hmcsua@uw.edu.

36. PUBLICITY – Contractor shall submit to Client all advertising and publicity matters relating to this MSA in which, Client's names or the names of other Client's Units, including the name "University of

Washington" and "UW Medicine," are specifically named or implied. Contractor agrees not to publish or use such advertising, and publicity matters without the prior written consent of UW Marketing and Communications. Client's names and the names of other Client's Units, including "University of Washington" and "UW Medicine", may be included in a company's website, press release, brochure, presentation, or annual report on a customer list, so long as the listing does not include any descriptive language which could be interpreted as an endorsement by the Client and no logos are used.

37. PUBLIC RECORDS ACT -- Notwithstanding any of the foregoing provisions of this section or any other provisions in this MSA regarding confidentiality, Contractor acknowledges that Client is an agency of the State of Washington, and that VMC is a public hospital district, and as such all are subject to Washington's Public Record Act, RCW 42.56 ("PRA"). If Client receives a public records request covering information that may be considered confidential under this MSA, the sole obligation of Client hereunder shall be to provide Contractor with no less than two (2) weeks' notice prior to any disclosure so as to enable Contractor, if it should so choose, to seek an injunction or other court order against disclosure. If Contractor has not obtained and served on Client, as applicable, an injunction or temporary restraining order against disclosure by the disclosure date indicated in the notice to Client, then Client may disclose the requested information without further obligation under this MSA.

38. PROPRIETARY INFORMATION –Contractor must clearly identify any material such as, but not restricted to, valuable formulae, designs, drawings, and research data claimed to be exempt from public records request, as allowable by law (RCW 42.56.270), along with a statement of the basis for such claim of exemption. Pricing and entire bid packages are not considered proprietary and are subject to public record requests. Client will give notice to Contractor of any request for disclosure of such information. Failure to so label such material or to timely respond after such notice of request for public disclosure has been given shall be deemed a waiver by the submitting Contractor of any claim that such materials are, in fact, exempt.

39. RECORDS MAINTENANCE –To the extent that Contractor, on behalf of Client uses or retains any records/data subject to the requirements for preservation and destruction of records under RCW 40.14, Contractor shall retain records in accordance with the current, authorized UW Medicine records retention schedules. Additionally, after retention requirements for records/data received/produced under this MSA have been met, Contractor shall destroy the records/data at no cost. If any litigation, claim, or audit is started before the legal retention requirement has been met, the records/data shall be placed on legal hold until the litigation/claim/audit has been resolved. At end/termination of this MSA, Contractor shall, at no cost, return any remaining data/records (in any and all formats) still within legal retention period to Client, at no cost.

    Additionally, at end/termination of MSA, Contractor shall destroy any remaining records/data (in any and all formats) relating to this MSA, that are outside of the legal retention period, as well as any copies of records/data (in any and all formats) produced or received from Hospitals/UWM Component Units during this MSA. Questions regarding retention are addressed to UW Medicine Records and Information Governance at hrc@uw.edu.

40. REFERRALS NOT REQUIRED – This MSA does not impose an obligation on any party to refer patients to any other person or entity to maintain this MSA. No person shall receive any payment hereunder for referral of any patient or ordering of any services.

41. REGISTRATION WITH DEPARTMENT OF REVENUE –To the extent required by law, Contractor shall complete registration with the Washington State Department of Revenue.

42. REJECTION – Intentionally Omitted.

43. SEVERABILITY – If any term or condition is deemed invalid by any court, such invalidity shall not affect the validity of the other terms and conditions of this MSA.

44. SHIPPING INSTRUCTIONS – Intentionally Omitted.

45. SITE SECURITY – While on Client premises, Contractor and its agents, employees, or subcontractors shall conform in all respects with all applicable policies, rules, or regulations, including those of Client.

    In addition to the foregoing provisions of this section, Contractor and its agents, employees, representatives, and/or subcontractors shall display the computer-generated badge received from current UW Medicine authorized vendor registration management system. This badge must be obtained daily from the authorized entry point for each UWM location and must be displayed in a visible location on the person at all times while on-site at any of the UWM locations. Expired badges will not be considered acceptable. Failure to follow this policy may include refusal to be permitted on any UW Medicine locations.

46. SUBCONTRACTING – Neither Contractor nor any Subcontractor shall enter into subcontracts for any of the Work contemplated under this MSA without obtaining prior written approval of Client.

47. TAXES – All payments accrued on account of payroll taxes, property taxes, unemployment contributions, any other taxes, insurance or other expenses for Contractor or its staff shall be the sole responsibility of Contractor.

    Where required by state statute or regulation, Contractor shall pay for and maintain in current status all taxes that are necessary for MSA performance. Unless otherwise indicated, Client agrees to pay State of Washington sales or use taxes on all applicable consumer services and materials purchased. No charge by Contractor shall be made for federal excise taxes and Client agrees to furnish Contractor with an exemption certificate where appropriate. Contractor shall calculate and enter the appropriate Washington State and local sales tax on the invoice. Tax is to be computed on new items after deduction of any trade in in accordance with WAC 458-20-247.

48. TERMINATION PROCEDURES – Upon termination of this MSA or SOW, Client, in addition to any other rights provided in this MSA, may require Contractor to deliver to Client any products specifically produced or acquired for the performance of the part of this MSA that has been terminated. Client shall pay to Contractor the agreed upon price for such products.

    The rights and remedies of Client provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this MSA.

    After receipt of a notice of termination, and except as otherwise directed by Client, Contractor shall:

    a. Stop work under this MSA or SOW on the date, and to the extent specified, in the notice.

    b. Place no further orders or subcontracts for p services, or facilities except as may be necessary for completion of such portion of the work under this MSA that is not terminated.

    c. Assign to Client, in the manner, at the times, and to the extent directed by Client, all of the rights, title, and interest of Contractor under the orders and subcontracts so terminated, in which case Client have the right, at its/their discretion, to settle or pay any or all claims arising out of the termination of all such orders or subcontracts;

    d. Settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of Client to the extent Client may require, which approval or ratification shall be final for all the purposes of this clause.

    e. Transfer title to Client and deliver in the manner, at the times, and to the extent directed by Client any property which, if this MSA had been completed, would have been required to be furnished to Client.

    f. Complete performance of such part of the work as shall not have been terminated by Client; and

    g. Take such action as may be necessary, or as Client may direct, for the protection and preservation of the products related to this MSA which is in the possession of Contractor and in which Client has or may acquire an interest.

49. TREATMENT OF ASSETS

    a. Title to all property furnished by Client shall remain in Client. Title to all property furnished by Contractor, for the cost of which Contractor is entitled to be reimbursed as a direct item of cost under this MSA, shall pass to and vest in Client upon delivery of such property by Contractor. Title to other property, the cost of which is reimbursable to Contractor under this MSA, shall pass to and vest in Client upon (1) issuance for use of such property in the perform of this MSA, or (2) commencement of use of such property in the performance of this MSA, or (3) reimbursement of the cost thereof by Client in whole or in part, whichever first occurs.

    b. Any property of Client furnished to Contractor shall, unless otherwise provided herein or approved by Client, be used only for the performance of this MSA.

    c. Contractor shall be responsible for any loss or damage to property of Client that results from the negligence of Contractor from the failure on the part of Contractor to maintain and administer that property in accordance with sound management practices.

    d. If any Client property is lost, destroyed, or damaged, Contractor shall immediately notify Client and shall take all reasonable steps to protect the property from further damage.

    e. Contractor shall surrender to Client all property of Client before settlement upon completion, termination, or cancellation of this MSA.

50. WAIVER – Any failure by Client to insist upon strict performance of any term or condition of this MSA, or failure to exercise or delay in exercising any right or remedy provided in this MSA or by law, or the acceptance of (or payment for) products, goods or services, shall not be deemed a waiver of any right of Client hereunder or of Client's rights to insist upon strict performance of any term or condition of this MSA. A waiver of one default or breach shall not be deemed a waiver of any subsequent default or breach. In no event shall any waiver be construed as a modification of the terms of this MSA unless so stated in a writing signed by Client.

51. WARRANTY

    a. Services: Contractor warrants that: (a) Services will be performed in a timely, efficient, and professional manner; (b) all Contractor personnel assigned to perform Services will have the necessary skill and training; and (c) Services will be performed in a manner consistent with the stand of care in the industry ("Services Warranty"). The Services Warranty will survive for a period of twelve (12) months after the date when Services are completed ("Services Warranty Period").

    b. Financial Status: Contractor warrants that at the time of the commencement of its performance under this MSA, it has not commenced bankruptcy proceedings.

UW Medicine
SUPPLY CHAIN

Exhibit B

Business Associate Agreement

Revised 11.01.2016

This Agreement is entered into between the University of Washington (hereinafter "Covered Entity") and **V GROUP INC** (hereinafter "Business Associate"). The University of Washington is a hybrid entity and has designated its healthcare components and non-healthcare components as described in COMP.101 Patient Information Privacy and Security Compliance Program and Administrative Requirements. Pursuant to 45 CFR §164.103 and §164.105(a) (2) (iii) (C), the University's designation includes the entities listed at http://depts.washington.edu/comply/docs/101_G1.pdf (hereinafter "Covered Entity"). Business Associate includes any agents and subcontractors of the Business Associate that receive, create, maintain, or transmit protected health information on behalf of the business associate.

This Agreement is incorporated into all existing and current MSA(s) between the parties (the "Underlying MSA(s)") under which Business Associate is carrying out activities or functions involving the use of protected health information (PHI), as this term is defined in 45 CFR Parts 160 and 164, and it replaces any prior agreement(s) entered concerning such PHI. Business Associates must reasonably and appropriately implement the standards and implementation specifications for safeguarding PHI and ensure the confidentiality, integrity, and availability of all electronic protected health information the business associate creates, receives, maintains, or transmits under federal Privacy and Information Security regulations (45 CFR Parts 160 and 164 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act) and are subject to the application of civil and criminal penalties under sections 1176 and 1177 of the Social Security Act and financial penalties under 45 CFR Sections 160.402, 160.404, 160.408, 160.410, 160.412, and 160.418. Business Associates must also comply with all requirements for protecting patient information under State Privacy regulations including but not limited to RCW 70.02. Covered Entity is committed to providing high quality patient care, education, and research. In furtherance of its mission, Covered Entity wishes to conduct transactions involving the disclosure of PHI to Business Associate for the purpose of conducting the activities set forth in the Underlying MSA(s).

Some or all of the information to be disclosed is required by law to be protected against unauthorized use, disclosure, modification, or loss. In order to comply with applicable legal requirements for the protection of information, the parties agree as follows:

A. ALLOWABLE USES OF PHI

Only the minimum necessary PHI to accomplish the intended purpose of this agreement can be used or disclosed only for the following purposes (accurately describe how and why PHI will be created, received, maintained, and/or transmitted):

1. As described in the Statement of Work.

B. OBLIGATIONS OF BUSINESS ASSOCIATE

Section 1. **Safeguarding Information**.

A. Business Associate shall only use, store, disclose, or access PHI:
   (1) In accordance with, and only to the extent permissible under the Underlying MSA; and
   (2) In full compliance with all applicable laws, regulations, rules, or standards, including, but without limitation HIPAA and RCW 70.02.

B. Business Associate shall have in place policies and procedures to implement and maintain all safeguards necessary to ensure the confidentiality, availability, and integrity of all Covered

Entity data. Business Associate shall deploy appropriate safeguards to implement the Secretary of Health and Human Services' annual guidance on the most effective and appropriate technical safeguards for use in carrying out security standards.

C. Where applicable Business Associate shall report to the Covered Entity possible existence of identity theft (The Federal Trade Commission has regulations known as the Red Flag Rules which are part of the Fair and Accurate Credit Transactions (FACT) Act of 2003).

Section 2. **Use or disclosure of Protected Health Information.** Business Associate shall not use or disclose PHI received from Covered Entity in any manner that would constitute a violation of federal law, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and any regulations enacted pursuant to its provisions ("HIPAA Standards"), or applicable provisions of Washington state law. Business Associate shall ensure that any use or disclosure by its directors, officers, employees, contractors, and agents of PHI received from Covered Entity, or created or received on behalf of Covered Entity is in accordance with the provisions of this Agreement and applicable federal and state law. Business Associate shall not use or disclose PHI in any manner other than that permitted or required by the Covered Entity for the purpose of accomplishing services to or on behalf of Covered Entity in accordance with the Underlying MSAs. Notwithstanding the foregoing, Business Associate may use PHI for the proper management and administration of the Business Associate and to carry out its legal responsibilities.

Section 3. **Reporting Unauthorized Use or Disclosure of PHI**.

A. Business Associate shall, within five (5) working days of becoming aware of an unauthorized use or disclosure of PHI by Business Associate, its officers, directors, employees, contractors, agents or by a third party to which Business Associate disclosed PHI, report any such disclosure to Covered Entity. Such notice shall be made to the following:

UW Medicine Compliance
Box 358049
Seattle WA 98195-9210
(206) 543.3098
comply@uw.edu

B. Business Associate shall report to the Covered Entity any Security Incident of which it becomes aware without unreasonable delay, but not later than ten (10) days, following Business Associate's discovery of any such incident.

Section 4. **Agreements by Third Parties.** Business Associate shall enter into a MSA or other arrangement with agents or subcontractor(s) to ensure that the same restrictions and conditions including the implementation of reasonable and appropriate safeguards to protect PHI that apply to the BA also apply to the agents or subcontractor(s).

Section 5. **Access to Information.** If Business Associate maintains Designated Record Set (DRS) documentation on behalf of Covered Entity, Business Associate agrees to provide access to the documentation maintained by the Covered Entity. Business Associate shall make available to Covered Entity such information for so long as it is maintained. If any individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to the Covered Entity. Business Associate shall not deny any individual's request for access to the individual's PHI. A denial of access to PHI requested is the responsibility of the Covered Entity.

Section 6. **Availability of PHI for Amendment.** Within five days of a request from Covered Entity for the amendment of an individual's PHI or a record regarding an individual contained in a DRS (for so long as the PHI is maintained in the DRS), Business Associate shall provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 CFR. §164.526.

Section 7. **Accounting of Disclosures.** Business Associate agrees to implement an appropriate record keeping and reporting process to enable it to provide the following information regarding disclosures of PHI: (i) the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. If Business Associate receives a request for an accounting of disclosures, Business Associate shall forward such request to Covered Entity within a reasonable time frame to allow Covered Entity to prepare and deliver any required accounting of disclosures.

Section 8. **Restrictions on Certain Disclosure of Health Information.** Business Associate agrees to restrict the disclosure of the protected health information of an individual if Covered Entity agrees to a requested restriction by an individual. If Business Associate receives a request for a restriction, Business Associate shall forward such request to Covered Entity within five business days to allow Covered Entity to respond to the requested restriction.

Section 9. **Availability of Books and Records.** Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from Covered Entity, or created or received on behalf of Covered Entity, available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining Covered Entity's and Business Associate's compliance with the HIPAA Standards. Business Associate shall provide to Covered Entity a copy of any documentation that Business Associate provides to the Secretary within five business days.

Section 10. **Return or Destruction of Information.** At the termination of the Underlying MSA(s), Business Associate shall return or destroy all PHI received from Covered Entity, or created or received on behalf of Covered Entity, that Business Associate maintains in any form. Business Associate will retain no copies of PHI. If Business Associate determines that return or destruction of any PHI is not feasible, Business Associate shall notify Covered Entity of the reasons why return or destruction is not feasible. If destruction or return of PHI is not feasible, Business Associate shall not use PHI received from Covered Entity, or created or received on behalf of Covered Entity, in a manner other than those permitted or required by state and federal laws or for the purposes described herein.

Section 11. **Electronic Protected Health Information ("ePHI").** If Business Associate creates, receives, maintains or transmits ePHI on behalf of Covered Entity, Business Associate agrees to (1) implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Covered Entity's ePHI in accordance with 45 CFR Sections 164.308, 164.310, 164.312, and 164.316 of title 45; (2) ensure that any third party agent or subcontractor who receives Covered Entity's ePHI from Business Associate agrees to implement equivalent administrative, physical and technical safeguards; and (3) deploy appropriate safeguards to implement the Secretary of Health and Human Services' annual guidance on the most effective and appropriate technical safeguards for use in carrying out security standards; and (4) report any security breaches involving Covered Entity's ePHI within five business days of discovery.

Section 12. **Breaches Involving Unsecured PHI.**

A. A breach is when unsecured PHI may have been used, accessed, disclosed, or acquired in a manner not permissible under the terms of this Agreement. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5. If Business Associate has reason to believe that a breach has occurred, Business Associate will, within five business days of discovery, give Covered Entity notice.
A breach shall be treated as discovered by the Business Associate as of the first day on which such breach is known to the Business Associate, (which includes any person, other than the individual committing the breach, who is an employee, officer, or other agent of the Business Associate) or should reasonably have been known to the Business Associate to have occurred. Business Associate shall give highest priority to immediately mitigate and remediate any unauthorized access and shall devote such resources as may be required to accomplish that goal. The Business Associate shall cooperate with all Covered Entity efforts, including providing any and all information necessary to enable Covered Entity to fully understand the nature and scope of the breach including but not limited to identification of each individual who has been affected by the breach.

B. The Business Associate will investigate a breach of unsecured PHI to determine if the PHI has been compromised based upon a risk assessment in accordance with Section 164.402 (2).

C. If it is determined that the PHI has been compromised, Covered Entity is required to provide notice to any or all individuals affected. In such case, Business Associate shall consult with Covered Entity regarding appropriate steps required to notify third parties. In the event that the Business Associate's assistance is required, such assistance shall be provided at no cost to Covered Entity and in accordance with the Covered Entity's policies and standards. Business Associate must coordinate with Covered Entity any public notification to any individual, media outlet, or the Secretary of Health and Human Services.

D. If it is determined that notification is required, the Business Associate shall pay the full costs of notice to affected individuals, including the costs to retain an outside consulting firm to undertake the notification effort and will supply UW Medicine Compliance with the following information to make such notification:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
(2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
(3) A brief description of what the Business Associate is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

Section 13. If the Underlying MSA does not include a provision for indemnification, then the Business Associate shall indemnify, hold harmless and defend Covered Entity from and against any penalties, claims, actions, loss, liability, damage, costs, or expenses, including but not limited to reasonable attorneys' fees.

Section 14. Covered Entity has the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance therewith, within the limits of Business Associate's technical capabilities.

C. MISCELLANEOUS

Section 15. **Termination.** Notwithstanding any provision to the contrary in the Underlying MSA(s), Covered Entity may terminate its participation in the Underlying MSA(s) immediately upon written notice to Business Associate without liability for such termination, in the event that Covered Entity determines that Business Associate has committed a material breach or violated a provision of this Agreement.

Section 16. **Definitions.** All terms herein shall be defined in accordance with 45 CFR Parts 160, 162, and 164 and state laws governing healthcare privacy including but not limited to Public Records - Personal Information – Notice of Security Breaches (RCW 42.56.590), the Uniform Healthcare Information Act (RCW 70.02), mental illness (RCW 71.05), mental health services for minors (RCW 71.34), drug and alcohol abuse (RCW 70.96A, 42 CRF part 2), and HIV/AID/STDs (RCW 70.24).

UW Medicine
SUPPLY CHAIN

Exhibit C

DATA PROCESSING AGREEMENT

A. INTRODUCTION, PARTIES, AND EFFECTIVE DATE

This Data Processing Agreement (the "DPA") is hereby incorporated into and amends the MSA. With respect to Data Processing performed under the MSA and this DPA, the Client (the "University") is the Controller and the Contractor is the Processor. The Parties agree as follows:

B. DEFINITIONS

1. **"Controller"** refers to the person or entity that determines the purpose and means for Data Processing.

2. "**Data Breach**" means any technical or physical incident or set of circumstances that leads to the unauthorized, accidental, or unlawful access to, or destruction, loss, alteration, or disclosure of, University Personal Data undergoing Data Processing by the Processor.

3. "**Data Processing**" means any operation(s) performed on University Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, access, use, disclosure by transmission, dissemination, combination, restriction, or destruction.

4. **"Data Request"** means a request to exercise rights available under any applicable law with respect to University Personal Data.

5. **"Processor"** refers to the person or entity that performs Data Processing on behalf of the Controller.

6. "**Sub-processor**" means any person or entity appointed by or on behalf of the Processor to carry out any portion of the Work.

7. "**University Personal Data**" **or "UPD"** means any records or information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or factor(s) specific to physical, physiological, genetic, mental, economic, cultural, or social identity or characteristics, or is identified as personally identifiable data (or a similar term) by any applicable law, that:

    a. Is created, received, or maintained by the University and transmitted to, accessed by, or otherwise made available to the Processor in connection with the Processor's performance of the Work.

    b. Is created or compiled by the Processor in performing the Work; or

    c. Is appended to, aggregated with, or associated with any University Personal Data originating from the University that was transmitted to or accessed by the Processor in connection with the Processor's performance of the Work.

    Notwithstanding the foregoing, UPD does not include personal data relating to the Processor's or Sub- processor's personnel or personal data that is acquired from non-UW sources and is processed by the Processor not in association with the Work.

8. "**Processor**" as used in this DPA includes both the Processor identified above, and any third party and/or entity that owns or controls, is owned or controlled by, or is under common ownership or

control with the Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting security, by contract, or otherwise.

9. "**Work**" refers to any and all activities carried out by the Processor or a Sub-processor in providing services, work product or deliverables under the Agreement, or in fulfilling any other obligations set forth in the Agreement.

C. STANDARD OF CARE

The Processor represents and warrants that any Data Processing shall be by personnel who (a) are obligated to maintain confidentiality under applicable law or job expectations, and (b) are sufficiently trained and experienced to use reasonable care commensurate with state-of-the-art professional practices to comply with the obligations in this DPA.

The Processor shall ensure that there are appropriate personnel-vetting processes, and appropriate policies and/or controls over activities as necessary to safeguard UPD per this DPA and applicable law.

Prior to the disclosure of UPD to, or the commencement of Data Processing by any Sub-processor, the Processor shall cause each Sub-processor to execute an agreement with the Processor that includes terms and conditions which establish at least the same level of protection for UPD as those set out in this DPA and applicable law. If a Sub-processor fails to fulfill its data protection obligations under this DPA or applicable law, the Processor shall remain fully liable to the University for the performance of that Sub-processor's obligations.

D. PURPOSE AND LIMITS OF DATA PROCESSING

1. The Description of Data Processing Exhibit to this DPA sets forth certain information relating to the Data Processing by the Processor for the purpose of carrying out the Work. The Processor may only engage in Data Processing for the limited purpose described in the Description of Data Processing Exhibit (the "Purpose"). The Processor shall limit its Data Processing to include only the minimum UPD needed to fulfill the Purpose. The Processor's Data Processing will not involve any secondary uses of UPD beyond the Purpose. Without limiting the generality of the foregoing, the Processor shall not use any UPD to market or sell goods or services to persons named or otherwise identified in UPD.

2. When the University reasonably deems necessary to meet its own requirements and/or applicable laws, the University may make reasonable changes to the Data Processing by amending the Description of Data Processing Exhibit or providing the Processor with an additional exhibit in the same form as the Description of Data Processing Exhibit. Any material changes to the Description of Data Processing Exhibit that increase the cost of the Work shall be subject to the mutual agreement of the parties.

3. The University shall have sole control over determinations related to (a) the lawfulness of the Data Processing, and (b) the necessity of any privacy notice to and/or solicitation of consent from individuals whose personal data will undergo Data Processing in relation to the Work.

E. NON-DISCLOSURE AND DATA REQUESTS

1. UPD shall not be disclosed by the Processor (or any Sub-processor) to a third party, unless the University grants permission in writing to the Processor to disclose, or unless such disclosure is required by applicable law.

2. If the Processor receives any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any UPD, then the Processor shall promptly notify the University unless specifically prohibited by law from doing so. The Processor's notification shall give the University sufficient time to object to the disclosure, obtain a protective order, or otherwise protect UPD by limiting disclosure. The Processor shall provide the University with prompt and full assistance in the University's efforts to protect UPD. Any disclosure pursuant to this section shall be limited to the minimum disclosure required by law.

3. The Processor shall assist the University by implementing technical and organizational measures, to the extent practicable, in order for the University to meet its obligations (as understood by the University) to respond to Data Requests relating to UPD held by the Processor. The Processor shall promptly notify the University if the Processor receives a Data Request, assist the University in the University's response, and respond to the Data Request directly only on the documented instructions of the University or as required by applicable laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by applicable laws, inform the University of the Processor's legal obligations before any response to the Data Request.

F. COMPLIANCE AND DATA TRANSFERS

1. The Processor shall conduct all Work and Data Processing in full compliance with any and all applicable statutes, regulations, rules, standards, and orders of any official body with jurisdiction over the Processor or the University. Applicable statutes, regulations, rules, or orders may include, but are not necessarily limited to:

    a. The Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. §1232g; 34 CFR Part 99.

    b. The Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.; and/or the Washington Health Care Information Act, Ch. 70.02 RCW; and

    c. European Union General Protection Data Regulation ("GDPR"), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. The University's obligations and rights with respect to GDPR are set forth in the Agreement and this DPA. The Agreement, this DPA, and any directions contained in notices from the University to the Processor pursuant to § J.4 together constitute the University's documented instructions to the Processor for the purposes of GDPR. The subject matter of the Data Processing with respect to GDPR is the Work, as defined above, in the Agreement, and/or in the Description of Data Processing Exhibit to this DPA (including any change(s) pursuant to § D.1). Compliance with GDPR includes, without limitation, the following:

        i. The Processor shall provide the University with assistance and information required by GDPR, to the extent applicable, as it relates to Data Processing. As contemplated by GDPR, the Processor's provision of assistance may relate to data protection impact assessments, prior consultations, demonstration of compliance with Article 28 of GDPR, and audits. The Processor will also immediately notify the University if, in its opinion, a University instruction infringes GDPR.

        ii. The Sub-processors that are identified and described by the Processor in the Description of Data Processing Exhibit of this DPA are the only Sub-processors

permitted to perform Data Processing. Prior to engaging a new Sub-processor for Data Processing, the Processor shall: (1) notify the University in writing of the intended addition or replacement of the Sub-processor; and (2) give the University the opportunity to object to such change.

2. For Data Processing that involves transfers of UPD from the European Economic Area, Switzerland, or the United Kingdom to a country that does not ensure an adequate level of data protection (including, but not limited to, the United States) within the meaning of the applicable laws of the foregoing territories, the Standard Contractual Clauses (accessible at https://privacy.uw.edu/design/agreements/dpa/ shall govern such transfers.

G. SAFEGUARDING DATA

1. Taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of the Data Processing, the likelihood and potential severity of risks to the rights and freedoms of natural persons, and the risk of Data Breach, the Processor represents and warrants that it shall implement technical, physical, and administrative security measures appropriate to such risks, which may include, but are not necessarily limited to:

    a. The de-identification, anonymization, pseudonymization, and encryption of UPD.
    b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems, facilities, and services.
    c. The ability to restore the availability of and access to UPD in a timely manner in the event of a physical or technical incident; and
    d. A process for regularly testing, assessing, and evaluating the effectiveness of technical, physical, and administrative measures for ensuring the security of the Data Processing.

2. The Processor's measures for protecting UPD shall (a) meet or exceed industry best practices for safeguarding personal data, and (b) be based on the concepts of privacy by design and by default.

H. DATA BREACH RESPONSE

1. The Processor shall have sufficient capabilities for detecting, identifying, and responding to a Data Breach.
2. If the Processor has reason to believe that a Data Breach has occurred, then, without undue delay, the Processor shall notify the University of said Data Breach. Such notification to the University shall include sufficient information to enable the University to meet its obligations under applicable law.
3. In the event of a Data Breach, the Processor shall cooperate with the University and immediately:
    a. Investigate and identify the nature of the Data Breach.
    b. Preserve relevant evidence.
    c. Contain, remediate, and mitigate the Data Breach; and
    d. Notify the University of any additional or newly emerged information beyond the initial Data Breach notification to the University described in § H.2.
4. In the event of a Data Breach caused in whole or part by the Processor:
    a. The University may instruct the Processor, at the Processor's expense, to provide:
        i. Notice when required by applicable law, or when a Data Breach could result in harm to individuals and/or risk to the University; and/or
        ii. Services such as credit monitoring or identity theft protection to individuals when the absence of such services could result in harm to individuals and/or individuals would have a reasonable expectation that such services be provided.

   b. Alternatively, the University may elect to provide the aforementioned notice and services itself.
5. Notwithstanding the foregoing, unless the Processor is required by law to provide the aforementioned notice and/or services in a particular manner, the University shall control the time, place, content, and manner of such notice and services.

I. DISPOSITION OF UPD UPON TERMINATION OR FULFILLMENT OF PURPOSE

1. The duration of Data Processing by the Processor shall be no longer than the expiration or termination of the Agreement or fulfillment of the Purpose with respect to UPD, whichever is earlier.
2. Upon expiration or termination of the Agreement, or fulfillment of the Purpose with respect to UPD, whichever is earlier, the Processor shall transfer to the University any and all UPD, unless otherwise instructed by the University in writing.

J. GENERAL TERMS

1. SURVIVAL AND ORDER OF PRECEDENCE. This DPA shall survive the expiration or earlier termination of the Agreement. In the event the provisions of this DPA conflict with any provision of the Agreement, or the Processor's warranties, support agreement, or service level agreement, the provisions of this DPA shall prevail.
2. SEVERABILITY. If any provision of this DPA is found to be unenforceable, the remainder of the Agreement and this DPA shall remain in effect.
3. HEADINGS FOR CONVENIENCE ONLY. Any and all subject headings are not substantive and are for convenience only.
4. NOTICES. Any notices or communications required or permitted to be given by this DPA must be (a) given in writing, and (b) personally delivered; mailed by prepaid, certified mail, or overnight courier; or transmitted by electronic mail (including PDF) with receipt acknowledged, to the party to whom such notice or communication is directed, or to the mailing address or regularly monitored electronic email address of such party.

UW Medicine
SUPPLY CHAIN

DESCRIPTION OF DATA PROCESSING EXHIBIT

This Description of Data Processing Exhibit to the Data Processing Agreement (the "DPA") sets forth certain information relating to the Data Processing, current as of the date of the last signature below (including in a countersigned version of this Description of Data Processing Exhibit), that the Parties anticipate will be carried out in connection with the Work as defined in the DPA. This version of this Description of Data Processing Exhibit may be superseded by subsequent versions issued in accordance with Section § D.2 of the DPA.

1. **NATURE AND PURPOSE**
   [Describe the nature (such as the operations to be undertaken by the Processor, volume of personal data, etc.) and the purpose (such as the University's mission and the University department or unit's specific objectives that will be fulfilled through the Processor's Data Processing)]

2. **CATEGORIES OF DATA SUBJECTS**
   [List the categories of individuals about whom personal data relates (such as currently enrolled undergraduate students, prospective academic personnel, alumni who have donated to the University between 2008-2018, etc.)]

3. **TYPES OF PERSONAL DATA**
   [List the personal data points that will undergo Data Processing including any special categories of personal data. NOTE: special categories of personal data include information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.]

4. **PROCESSOR CONTACT PERSON**
   [Insert name, title, mailing address, email address, and phone number]

5. **UNIVERSITY DEPT/UNIT CONTACT PERSON**
   [Insert name, title, mailing address, email address, and phone number]

6. **SUB-PROCESSORS**
   [The Processor must list all Sub-processors that will perform any GDPR-governed Data Processing (such as cloud storage providers, hosting providers, etc.), with an explanation of each Sub-processor's Data Processing activities. If GDPR does not apply or the Processor does not use any Sub-processors for GDPR-governed Data Processing, insert "Not Applicable".]

University:	**Processor:**
Signature	Signature
Name and Title	Name and Title

UW Medicine
SUPPLY CHAIN

Date Date

Exhibit D

IT SECURITY TERMS

INTRODUCTION, PARTIES, AND EFFECTIVE DATE

THESE IT SECURITY TERMS ARE HEREBY INCORPORATED INTO THE AGREEMENT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND CONTRACTOR, AS OF THE "EFFECTIVE DATE" OF THE AGREEMENT. IN CONSIDERATION OF THE MUTUAL PROMISES IN THE AGREEMENT AND OTHER GOOD AND VALUABLE CONSIDERATION, THE PARTIES AGREE AS FOLLOWS:

I. DEFINITIONS

1. **"Incident"** means for the purposes of this Agreement, any adverse event (including technical or physical incidents) where there is harm to University Data, individuals, host(s), or network(s). This includes, but not by way of exclusion, events indicating that University Data may have been accessed, disclosed, or acquired without proper authorization, unlawfully, or contrary to the terms of the Agreement.
2. **"Malicious Code"** refers to malware, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, bot, or other code or mechanism designed to, without consent collect information, gain access, assert control, alter, and/or cause harm to the system or data of an effected host, network, or environment.
3. **"University Data"** means all records and information created, received, maintained, or transmitted by the University, which are accessed, created, used, stored, copied, or distributed by Contractor, in connection with the Work under the Agreement. University Data which meets the criteria for the definition of University Personal Data, as defined within the University Data Processing Agreement (DPA), herein incorporated by reference, should be first interpreted under the DPA, and only interpreted as University Data to the extent that the DPA is not dispositive of the issue.
4. **"Contractor Group"** includes any person or entity appointed by or on behalf of the Contractor to carry out any portion of the Work.
5. **"Contractor"** has the same meaning as "The Contractor" as the term is defined within the University of Washington General Terms and Conditions.
6. **"Work"** is the solution as described in the underlying contract

II. DECLARATIONS

Parties understand and acknowledge:

1. University retains all ownership, title, rights, and control over all forms of University Data. Any privileges or license granted to Contractor Group under these IT Security Terms, or the Agreement shall be narrowly construed, to permit only the least amount of access, creation, use, storage, copying, and/or distribution of University Data that is necessary for the Work. University control over University Data specifically includes determining notification requirements in a potential Incident.
2. Contractor is in the best position to control the manner and means of how the Work is performed. Therefore, the express intent of the parties is to hold Contractor accountable for

information security standards and practices of Contractor Group, but only as they pertain to the Work.

3. Contractor is already familiar with the compliance requirements of applicable information and security statutes, rules, and regulations related to the Work or University Data. Contractor conducts business consistent with leading principles and practices of information security.

4. University has a continuing valid interest in obtaining current records and information from Contractor as assurance that Contractor Group is meeting expected standards of performance, and to substantiate Contractor's representations.

III. OPERATIVE PROVISIONS

1. **STANDARD OF CARE**

   a. Contractor represents and warrants that, with regard to protecting the confidentiality, availability, and integrity of University Data, the Work shall be undertaken with all due care, skill, and judgment commensurate with good professional practices.

   b. Contractor represents and warrants that the Work shall be undertaken by personnel capable of performing work commensurate with the required standard of care.

2. **UNIVERSITY DATA OWNERSHIP**

   a. UNIVERSITY DATA SHALL NOT BE DISCLOSED BY CONTRACTOR GROUP TO A THIRD PARTY, UNLESS THE UNIVERSITY GRANTS PERMISSION IN WRITING TO THE CONTRACTOR TO DISCLOSE, OR UNLESS SUCH DISCLOSURE IS REQUIRED BY APPLICABLE LAW.

   b. MARKINGS ON ALL UNIVERSITY DATA - INDICATING COPYRIGHT, TRADEMARK, OTHER PROPRIETARY INTELLECTUAL PROPERTY INTEREST, REASON FOR CONFIDENTIALITY, OR REASON ON DISTRIBUTION SHALL BE PRESERVED.

3. **COMPLIANCE**

   a. Contractor represents and warrants the Work, the handling of University Data, and the general conduct of business with University, shall be undertaken in full compliance with all applicable statutes, regulations, rules, standards, and orders of any official body with jurisdiction over Contractor Group or University.

   b. Where the Work or University Data is subject to the Export Administration Regulations (EAR), or International Traffic in Arms Regulations (ITAR), Contractor shall provide the University Office of Sponsored Programs such assistance as necessary to ensure compliance.

4. **COMPELLED DISCLOSURE**

   a. If the Contractor receives any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any University Data, then the Contractor shall promptly notify the University unless specifically prohibited by law from doing so. The Contractor's notification shall give the University sufficient time to object to the disclosure, obtain a protective order, or otherwise protect University Data by limiting disclosure. The Contractor shall provide the University with prompt and full assistance in the University's efforts to protect University Data. Any disclosure pursuant to this section shall be limited to the minimum disclosure required by law.

b. The Contractor shall assist the University by implementing technical and organizational measures, to the extent practicable, in order for the University to meet its obligations (as understood by the University) to respond to requests for production or disclosure of University Data held by the Contractor. The Contractor shall promptly notify the University if the Contractor receives a request for University Data, assist the University in the University's response, and respond to the request for University Data directly only on the documented instructions of the University or as required by applicable laws to which the Contractor is subject, in which case the Contractor shall, to the extent permitted by applicable laws, inform the University of the Contractor's legal obligations before any response to the request for University Data.

5. INCIDENT RESPONSE

If the nature of an Incident involves University Personal Data, as defined in the DPA, then the DPA incident response process shall apply instead of the provisions of these IT Security Terms.

a. If the nature of the Work involves Contractor Group equipment, software, product(s), host(s), network(s), or environment(s) that may expose University Data to a potential Incident, then Contractor shall have an appropriate incident response plan. University may, at its discretion, request Contractor to participate in "lessons learned" activities following an incident.

b. If the Contractor has reason to believe that an Incident has occurred, then, without undue delay, the Contractor shall notify the University of said Incident. Such notification to the University shall include sufficient information to enable the University to meet its obligations under applicable law.

c. In the event of an Incident, the Contractor shall cooperate with the University to:
   i. Investigate and identify the nature of the Incident.
   ii. Preserve relevant evidence.
   iii. Contain, remediate, and mitigate the Incident; and
   iv. Notify the University of any additional or newly emerged information beyond the initial Incident notification to the University described above.

d. In the event of an Incident caused in whole or part by the CONTRACTOR, the University may
   i. instruct the CONTRACTOR, at the CONTRACTOR's expense, to provide notice when required by applicable law, or when an Incident could result in harm to individuals and/or risk to the University.
   ii. and/or Services such as credit monitoring or identity theft protection to individuals when the absence of such services could result in harm to individuals and/or individuals would have a reasonable expectation that such services be provided.
   iii. Alternatively, the University may elect to provide the notice and services itself.

e. If recovery from the adverse effects of the Incident necessitates Contractor's assistance in the reinstallation of Contractor Group's technology product(s) (including hardware or software) that relate to the Work, then Contractor shall cause such assistance in reinstallation to be provided. If Contractor Group is responsible for the Incident, then reinstallation assistance shall be at no cost to the University.

f. If it appears to the University, in its sole discretion, that services or technology provided by the Contractor are a source of the Incident, and present an unreasonable risk, then

the University may opt to discontinue use of that source of the Incident and the University's corresponding payment obligations under the Agreement shall be adjusted equitably.

6. INFORMATION SECURITY ARCHITECTURE

a. This section III.6 applies to the extent that Contractor Group owns, supports, or is otherwise responsible for host(s), network(s), environment(s), or the Work involves services wherein Contractor has care, custody, or control of University Data. For avoidance of doubt, this section shall apply when Contractor Group provides cloud-hosted infrastructure, platform, or application as a service.

b. Contractor represents and warrants that the design and architecture of Contractor Group's systems (including but not limited to applications and infrastructure) shall be informed by the principle of defense-depth; controls at multiple layers designed to protect the confidentiality, integrity, and availability of data.

c. Contractor shall cause Contractor Group to make appropriate personnel vetting/background checks, have appropriate separation of duties, and undertake other such workflow controls over personnel activities as necessary to safeguard University Data.

d. Contractor shall cause Contractor Group to follow change management procedures designed to keep Contractor Group's systems current on security patches and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to an Incident.

e. To the extent that the Work involves software that was developed, in whole or part, by any of Contractor Group, then Contractor represents and warrants that such portion of the Work was developed within a Software Development Life Cycle process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.

f. Contractor Group shall have appropriate network segmentation and perimeter hardening. Contractor Group shall monitor its system and perimeter configurations and network traffic for vulnerabilities, indicators of activity or compromise by threat actors, and/or the presence of Malicious Code.

g. Contractor Group shall have access, authorization, and authentication technology appropriate for protecting University Data from unauthorized access or modification, and capable of accounting for access to University Data. The overall access control model of Contractor Group systems shall follow the principle of least privileges.

h. Contractor Group shall safeguard University Data with encryption controls over University Data both at rest and in transit. Contractor Group shall discontinue use of encryption methods and communication protocols which become obsolete or have become compromised.

i. Contractor Group shall maintain a process for backup and restoration of data. Contractor represents and warrants that within the context of the Work, the appropriate members within Contractor Group are included in and familiar with a business continuity and

disaster recovery plan.

j. Contractor Group facilities will have adequate physical protection, commensurate with leading industry practice for similar Work.

k. Contractor shall maintain a process for regularly testing, assessing, and evaluating the effectiveness of technical, physical, and administrative measures that meet or exceed the requirements set out under these IT Security Terms and Conditions. Upon request, Contractor shall furnish University with an executive summary of the findings of the most recent assessment.

   i. University reserves the right to conduct or commission additional tests, relevant to the Work, to supplement Contractor's assessment. Contractor shall cause Contractor Group to cooperate with such effort.

   ii. If the findings of an assessment identifies either: a potentially significant risk exposure to University Data, or other issue indicating that security standards and practices of Contractor do not meet the requirements set out under these IT Security Terms and Conditions, then Contractor shall notify University to communicate the issues, nature of the risks, and the corrective active plan (including the nature of the remediation, and the time frame to execute the corrective actions).

7. UNIVERSITY RIGHTS AND REMEDIES

All University rights and remedies set out in these Security terms are in addition to, and not instead of, other remedies set out in the Agreement, irrespective of whether the Agreement specifies a waiver, limitation on damages or liability, or exclusion of remedies. The terms of these IT Security Terms and Conditions and the resulting obligations and liabilities imposed on Contractor and Contractor Group shall supersede any provision in the Agreement purporting to limit Contractor or Contractor Group's liability or disclaim any liability for damages arising out of Contractor or Contractor Group's breach of under these IT Security Terms and Conditions.

8. INFORMATION SECURITY INDEMNIFICATION

a. It is the intent of the parties that all indemnity obligations of Contractor with respect to information security be allocated within this section and that any exclusions or limitation of liability language elsewhere within this Agreement does not apply to Contractor's information security indemnification obligations.

b. Contractor agrees to defend, indemnify, and hold University harmless from and against any and all claims, demands, suit, proceedings, judgment, award, damages, costs, expenses, fees, losses, fines of a penal nature, civil penalties, and other liabilities (including the obligation to indemnify others) arising from or connected to:

   i. Any violation by Contractor Group of such information security statutes, ordinances, rules, regulations, and orders of any official body with jurisdiction over Contractor Group or University that are applicable under the compliance provisions of these Security terms and conditions.

   ii. The Work, and/or all information or materials provided by the Contractor Group, with respect to any allegation by a third party of **any infringement of any copyright, trademark, patent, trade secret, or other property**

intellectual property right.

iii. Any **Incident**, in proportion **to the extent of Contractor Group's fault**.

9. INFORMATION SECURITY INSURANCE COVERAGE

Contractor shall, at its own expense, provide and maintain in force the appropriate kinds of insurance and minimum amounts of coverage, sufficient to support Contractor's information security indemnity obligations, as further specified in the attached CYBER LIABILITY RIDER, hereby incorporated by reference.

10. TRANSITION SERVICES

a. As part of the winding up of services, associated with the expiration or termination of the Agreement, the Contractor shall follow the University's instructions as to the preservation, transfer, or destruction of University Data. If, after requesting that University provide instructions, University fails to do so, then the instructions shall be deemed to be that the Contractor shall not destroy and not retain any University Data but shall first transfer to the University any and all University Data in Contractor's possession.

b. If the Agreement terminates due to a material breach or unresolvable dispute, then Contractor shall, at University's written request, be obligated to continue to provide the Work, at Agreement rates listed in Exhibit I, pending University's reasonable efforts to obtain a substitute Contractor to provide the Work.

11. OPPORTUNITY TO CURE

In the event of a material breach of these IT Security Terms and conditions by Contractor Group, the University reserves its right to terminate the Agreement and seek all other available remedies. In lieu of immediately exercising the right to terminate, University may opt to extend to Contractor an opportunity to cure Contractor Group's material breach, and shall contact the Contractor, in writing, to describe issues where corrective action is sought. Within ten (10) business days, Contractor will provide a response, in writing, to explain how Contractor shall address all issues to University's satisfaction. If the Contractor's response is, in whole or part, unacceptable to University, then University may refer the matter to the dispute resolution provision of the Agreement or seek other reasonable means to resolve outstanding issues. To the extent that the Contractor's response describes acceptable corrective actions, then University and Contractor shall coordinate in furtherance of executing Contractor's corrective actions. Contractor shall make a written request to University to confirm that satisfactory performance of corrective actions has cured the material breach. Such acceptance shall not be unreasonably withheld.

12. SURVIVAL: ORDER OF PRECEDENCE

a. With respect to the subject of these provisions, these Security terms and conditions shall supersede the general terms of this contract and shall supersede any terms within this contract that would otherwise limit the remedies set out herein.

b. If the data processing activity includes University Personal Data, then the DPA governs the data processing. University Personal Data and Data Processing Terms are defined in the DPA.

UW Medicine
SUPPLY CHAIN

CYBER LIABILITY RIDER

INTRODUCTION, PARTIES, AND EFFECTIVE DATE

THIS CYBER LIABILITY RIDER IS HEREBY INCORPORATED INTO THE AGREEMENT BETWEEN THE UNIVERSITY OF WASHINGTON (UNIVERSITY) AND CONTRACTOR, AS OF THE "EFFECTIVE DATE" OF THE AGREEMENT. IN CONSIDERATION OF THE MUTUAL PROMISES IN THE AGREEMENT AND OTHER GOOD AND VALUABLE CONSIDERATION, THE PARTIES AGREE AS FOLLOWS:

13. INFORMATION SECURITY INSURANCE COVERAGE

a. In addition to the types of insurance, and limits of insurance required by Agreement, Contractor shall, at its own expense, provide and maintain in force the kinds of insurance and minimum amounts of coverage, sufficient to support Contractor's information security indemnity
obligations, not less than as set forth in subsection "b." Cognizant of the variety of policy forms currently within the insurance industry, the coverages provided under this section may be maintained in one or more types of insurance policies, irrespective of the name of the type of policy or coverage, such that Contractor is in material compliance with the requirements of this rider.

b. The types of coverages required under the Agreement by this Cyber Liability Rider are:

i. **Internet Professional Liability/ Media Liability/ Errors and Omissions Coverage**, with limits of at least $2 million per occurrence / in the aggregate. Relevant policies must include coverages for:

1. Where the nature of Work includes providing a service for a fee: claims arising out of a failure of the insured's **internet professional services** or claims arising out of the rendering or failure of **technology services** by insured. Works requiring cover include, without limitations, activities by Contractor's as an internet service provider, application service provider, web portal, web content developer, web site or web-facing application designer, professional services provider that delivers some portion of such services over the internet. Types of claims include, without limitation: any form of improper "deep-linking," plagiarism, misappropriation of intellectual property, and/or unauthorized disclosure of trade secrets, confidential, or other protected private or personal information.
2. Where the nature of the Work includes providing or relying upon a product: claims arising from the failure of **insured technology products** (including hardware and software) to perform its intended function or purpose.
3. Where the nature of the Work includes any activities involving access by Contractor to University's hosts or networks, and/or requires Contractor Group to store University Data: claims arising from insured **security** controls failure including but not limited to: failure of contractor to prevent the transmission of Malicious Code; failure to prevent unauthorized host or network use; failure to prevent unauthorized host or network access; failure to handle, manage, store, destroy, or otherwise control University Data; failure to prevent collection of

protected personal information, and failure to provide individuals access to information and controls about their personal data as required by law.

ii. **Cyber Liability/ID Theft and Extortion Insurance**, with limits of at least $2 million per occurrence and in the aggregate. Relevant policies must include coverages for:

1. Claims arising from first- and third-person **Cyber Extortion** or any credible threat or series of related threats to attack insured hosts or networks in a specific way.
2. Claims arising from **Crisis management, response costs and public relations expense**, including liability arising from failure to notify, legal expenses, and computer forensic expenses.
3. Claims arising from **Unauthorized Access to or use of data,** a **Loss of Data** or **Denial of Service** incident effecting insured host(s) or network(s)

Where the Agreement includes IT Special Terms and Conditions and the potential net aggregate compensation paid or to be paid by University to Contractor over the term of the Agreement exceeds $25,000: **Umbrella liability**, with limits of at least $1 million in the aggregate, which after other coverages required of Contractor Group under the Agreement, shall be primary to any other insurance of the University, but only for the risks and liabilities assumed under the Agreement.

UW Medicine
SUPPLY CHAIN

Exhibit E

TEMPLATE
V GROUP INC
MASTER AGREEMENT NO. 1420-5430
SOW NO.XXXX

This Statement of Work (SOW) No. XXXX is made and entered by and between University of Washington, on behalf of UW Medicine ("UW Medicine") and V Group, Inc. ("Contractor"). This SOW incorporates by reference the terms and conditions of Master Services Agreement No. MSA 1420-5430 in effect between UW Medicine and Contractor. In case of any conflict between this SOW and the Master Agreement, the Master Agreement shall prevail. UW Medicine and Contractor agree as follows:

1. GENERAL BACKGROUND

UW Medicine's Information Technology Services (ITS) department is a shared services organization, which supports all of UW Medicine. UW Medicine is an integrated clinical, research and learning health system comprised of multiple entities that are managed together as a health system. UW Medicine consists of the following components: University of Washington Medical Center, operating at two separate campuses, Montlake and Northwest, and its associated clinics ("UWMC"); UW Physicians Network dba UW Medicine Primary Care ("UWMPC"); The Association of University Physicians dba UW Physicians ("UWP"); Fred Hutchinson Cancer Center, a separate entity that serves as the Cancer Center of UW Medicine ("FHCC"); Harborview Medical Center as managed by UW pursuant to a Hospital Services Contract between the UW and King County and its associated clinics ("HMC"); Public Hospitals District No. 1 dba Valley Medical Center and its associated clinics ("VMC"); University of Washington School of Medicine ("UW SoM"); and Airlift Northwest ("ALNW"). The IT Services organization is responsible for ongoing support and maintenance of the infrastructure and applications which support these institutions, along with the implementation of new services and applications that are used to support and further the mission of patient care, research, and teaching.

2. PROJECT TASK or OBJECTIVES

(Brief description of project.)

3. SCOPE OF WORK AND CONTRACTOR'S DELIVERABLES

Contractor shall provide services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below:
(list of requirements/deliverables)

4. PERIOD OF PERFORMANCE AND TERM

The period of performance for this project will start on Date, and the work tasks are estimated to continue through Date. The Contractor is expected to complete the deliverables of the project during this period.
The term of this SOW is twelve (12) months, expiring mm/dd/yyyy. The UW Medicine has the right to extend or terminate this SOW at its sole discretion at any time with fourteen (14) business days written notice during the twelve-month (12 month) term.

5. COMPENSATION AND PAYMENT

A rate of XX per hour for the performance of activities necessary for or incidental to performance of work as set forth in this SOW. This rate will be utilized for all hours when the consultant is not working on UW Medicine premises.
Based on current projections, the role is anticipated to require on average 40 hours/week throughout the engagement. Should Contractor identify weeks when the 40-hour week must be exceeded, Contractor staff must request prior approval from ITS.

Additionally, the UW Medicine shall pay Contractor an amount not to exceed $XX for the duration of this SOW.
Contractor can only charge for hours worked at a location approved by UW Medicine. They cannot charge for hours worked traveling to/from that location unless approved by UW Medicine.
No travel expenses are authorized.

6. CONTRACTOR STAFF, ROLES, AND RESPONSIBILITIES

The Contractor staff consultant, XX will serve in the role of (Position Title) and will be tasked with fulfilling the responsibilities and completing the deliverables outlined in Section 3.

7. UW MEDICINE STAFF, ROLES, AND RESPONSIBILITIES

The key stakeholders among UW Medicine staff include

- **Primary contact** – XXX will serve as primary point of contact for engagement logistics and will provide clarifying direction, as necessary.
- **Secondary contact (if applicable)**– XXX will serve as a secondary point of contact for timesheet management and will provide clarifying direction, as necessary.

ACKNOWLEDGMENT.
By signing below, the ITS representative acknowledges and consents to the content in the Statement of Work, the Terms and Conditions of the Master Agreement and execution thereof.
IT SERVICES BUSINESS OWNER

_____
(signature)

_____
(printed name)

_____
(title)

_____
(date)

AUTHORITY TO BIND:

This SOW is executed by persons signing below who warrant they have the authority to execute this SOW.

UNIVERSITY OF WASHINGTON ON BEHALF OF UW MEDICINE	**V GROUP INC**
_____ (signature)	_____ (signature)
_____ (printed name)	_____ (printed name)
_____ (title)	_____ (title)

UW Medicine
SUPPLY CHAIN

Exhibit F

Vendor Credentialing/Green Security information

UW Medicine, including **UW Medicine IT Services,** contracts with Green Security Services for vendor credentialing. As of July 1st, 2023, **ALL** vendors working for or contracting with **UW Medicine IT Services** must be registered with **Green Security LLC** and comply with all applicable UW Medicine background and health screening requirements.

Green Security provides the background screening and credentialing service for all **UW Medicine** vendors, service technicians, consultants, sales reps, and more. ***Due to compliance and regulatory requirements, anyone who will access UW Medicine sites or information systems are required to comply with this requirement.***

Individual contractors are required to register with Green Security and complete required background checks and other requirements (see below). Contractors will be asked to register at https://grn.ac/uw-vendors to start the onboarding process.

Where required, Green Security will also provide smartphone badges and physical badges that can be tracked through Green Security's technology utilizing its QR scanning and tracking service.

Levels of Registration.
Requirements and costs will vary based on the work location of the contractor and direct patient care duties. The information is available when registering at https://www.greensecurityllc.com/vendors/register/step1. Costs are per contract resource. Credentialing and associated fees will reoccur annually for the duration of the engagement.

Level 2A
- Non-Clinical
- Fully remote Contractors

Level 2B
- Non-Clinical Vendor/Contractor
- Onsite for any duration of time
- Not involved in direct patient care

Level 3
- Clinical Vendor/Contractor
- Onsite for any duration of time
- Involved in direct patient care

*Annual registration fee covers access to any Green Security member hospitals.
Company registrations are required prior to submitting an individual registration. Contact Green Security Customer Service for assistance if your Company is not already registered with Green Security. Companies can also request to have company manager accounts established to manage all their vendors and contractors in the Green Security web portal.

A background screening will begin once the corresponding request has been filled out and sent for processing. Contractors will need to have their registration completed one week in advance to avoid delays to the anticipated start date.

Additional Green Security Background Check information:
Green Security obtains Social Security Numbers (SSN) to complete a thorough and accurate background screening. The SSN is encrypted in motion and at rest and is only accessible to the background

screening professional completing the check. Additionally, the SSN is removed from the system once the screening has been completed.

Please note the following:

- Green Security does not accept 3rd-party background checks.
- For vendors renewing their credentialing subscription, the background check will not take place until the invoice for the renewal has been paid.
- Additional fees will apply for international checks.
- Screening typically takes 1 to 2 business days but may take longer depending on the general volume Green Security is experiencing and the complexity of any uploaded documents. If there are findings in the background screening that require additional investigation, the turnaround time may be extended significantly.

Green Security does the following background checks:

- **National Criminal Database**
  - Sex Offender Search
  - FBI's most wanted
  - Wants & Warrants
  - Terrorist Watch List
  - Information from all 50 states
  - OFAC
  - Prohibited Parties
  - System of Awards Management (SAM)
  - GSA
  - Office of Inspector General (OIG)
  - 500 million + data sets
- County Criminal Search – 7 YR
  - One name/ all counties up to 7 years
- National Federal Search

Please direct all other inquiries to Green Security Customer Service.
Please contact Green Security at **866-750-3373** or email them at **support@greensecurityllc.com**. to learn more or with additional questions regarding the vendor registration process. The customer service team will be happy to guide you through the transition. Their hours of operation are Monday through Friday 8am – 5pm EST. For an overview of the process, here is also a video link to help you get started. **https://youtu.be/1GyFnWPkWOw**

UW Medicine
SUPPLY CHAIN

Exhibit G

Workday Requirements

Minimum Requirement:
Agree to meet requirements for adding contractors to UW's contingent worker management information system (Workday).

Background information:
Effective July 1, 2024, UW Medicine IT Services (UWMITS) will require all consultants (AKA "Contractors") to provide personal information to UWMITS Contractor Program staff that is needed to create a "Contingent Worker" record in UW's workforce management information system, Workday.

This requirement will enable UWMITS to manage and track Contractors, and accurately report UWMITS contracting activity and spending.

Please note the following:

- The collection of this information is separate from the vendor credentialing and background checks process managed by Green Security LLC (see Exhibit for details of Green Security's vendor credentialing requirements and process).
- The UWMITS Contractor Program is managed by the UWMITS Human Resources team.
- UWMITS Contractor Program staff will collect the required information directly from individual contractors.
- UWMITS recognizes the Personal Identity Information (PII) needed (including Social Security Number and Date of Birth) are highly sensitive and confidential. The information will be collected one time, protected, and will be accessible only by Human Resources staff with high-level Workday security roles and only as needed.
- Workday is a cloud-based platform that requires employee credentials and 2-Factor Authentication (2FA) to log in.
- This change is not precedent setting; several UW departments utilize the "Contingent Worker" designation for contractors hired through vendors.

Process:
During the onboarding process, the UWMITS Contractor Program will collect personal information directly from the Contractor ("Contingent Worker") to create a Workday record.

Information required and how it will be collected:

Attribute	Provided By	How to source
Legal Name	Contingent Worker	Via e-mail
NetID* (If already exists, if not will be prompted with onboarding to Workday)	Contingent Worker	Via e-mail
E-Mail Address **(at vendor)**	Contingent Worker	Via e-mail
Social Security Number (SSN)	Contingent Worker	**By Phone**
Date of Birth	Contingent Worker	**By Phone**

Questions about the "Contingent Worker" process can be directed to the UW Medicine IT Services Contractor Program at itscontractoronboard@uw.edu.

*The UW NetID is the username and email address each member of the University of Washington's workforce creates upon affiliation or hire. The NetID is required to access specific UW information and online services.

In addition, UW Medicine workforce members are assigned a UW Medicine account ("AMC"), which is separate from the NetID. The AMC account is used to access specific UW Medicine applications and information.

UW Medicine
SUPPLY CHAIN

Exhibit H

Contractor's Staff Level and Cost

ATTACHMENT E		Staffing levels			Cost information						Markup Percentage Rate
					Certified			Un-Certified			
Category	Role	Total staffing level	Epic-certified staffing	% of staff available to be in the Greater Seattle Area	On-site rate	Remote rate	Offshore rate	On-Site rate	Remote rate	Offshore rate	48%
Technical	Applications Analyst	5	0	1%	$ 84.91	$ 70.76		$ 77.19	$ 64.33		
	Senior Applications Analyst	2	0	1%	$ 93.40	$ 77.83		$ 84.91	$ 70.76		
	Applications Architect	1	0	1%	$ 102.74	$ 85.62		$ 93.40	$ 77.83		
	Business Intelligence (BI) Administrator	0	0	1%	$ 95.64	$ 79.70	$ 70.84	$ 86.95	$ 72.45	$ 64.40	
	Business Intelligence (BI) Developer	1	0	1%	$ 84.91	$ 70.76		$ 77.19	$ 64.33		
	Senior Business Intelligence (BI) Developer	1	0	1%	$ 93.40	$ 77.83	$ 69.19	$ 84.91	$ 70.76	$ 62.90	
	Cloud Architect	1	0	1%	$ 115.25	$ 96.04	$ 85.37	$ 104.77	$ 87.31	$ 77.61	
	Cyber Security Analyst	0	0	1%	$ 110.48	$ 92.07	$ 81.84	$ 100.44	$ 83.70	$ 74.40	
	Cyber Security Engineer	0	0	1%	$ 105.25	$ 87.71	$ 77.96	$ 95.68	$ 79.73	$ 70.88	
	Senior Cyber Security Engineer	1	0	1%	$ 115.78	$ 96.48	$ 85.76	$ 105.25	$ 87.71	$ 77.96	
	Epic and Data Warehouse Architect - Analytics	0	0	1%	$ 101.55	$ 84.63		$ 92.32	$ 76.93		
	Epic Database Administrator	0	0	1%	$ 102.33	$ 85.28		$ 93.03	$ 77.52		
	Epic Interface Analyst	0	0	1%	$ 98.56	$ 82.13		$ 89.60	$ 74.67		
	Identity and Access Management (IAM) Analyst	0	0	1%	$ 97.65	$ 81.38	$ 72.33	$ 88.77	$ 73.98	$ 65.76	
	Identity and Access Management (IAM) Systems Engineer	1	0	1%	$ 99.55	$ 82.96	$ 73.74	$ 90.50	$ 75.42	$ 67.04	
	Senior Identity Access Management (IAM) Epic Security Analyst	0	0	1%	$ 109.51	$ 91.25	$ 81.11	$ 99.55	$ 82.96	$ 73.74	
	IT Service Management (ITSM) Process Analyst	2	0	1%	$ 84.91	$ 70.76	$ 62.90	$ 77.19	$ 64.33	$ 57.18	
	Quality Assurance Specialist	5	0	1%	$ 78.49	$ 65.41	$ 58.14	$ 71.35	$ 59.46	$ 52.86	
	Senior Quality Assurance Specialist	3	0	1%	$ 86.34	$ 71.95	$ 63.95	$ 78.49	$ 65.41	$ 58.14	
	Senior Test Automation Engineer	3	0	1%	$ 93.40	$ 77.83	$ 69.19	$ 84.91	$ 70.76	$ 62.90	
	Software Engineer	5	0	1%	$ 84.91	$ 70.76	$ 62.90	$ 77.19	$ 64.33	$ 57.18	
	Systems Database Administrator	1	0	1%	$ 99.54	$ 82.95	$ 73.73	$ 90.49	$ 75.41	$ 67.03	
	Senior Network Security Engineer	2	0	1%	$ 87.54	$ 72.95	$ 64.84	$ 79.58	$ 66.32	$ 58.95	
	Senior Data Center Operations Analyst	2	0	1%	$ 89.66	$ 74.72	$ 66.41	$ 81.51	$ 67.92	$ 60.38	
	Senior Software Defined Data Center Engineer	2	0	1%	$ 98.63	$ 82.19	$ 73.06	$ 89.66	$ 74.72	$ 66.41	
Communication	Principal, Release Manager	1	0	1%	$ 115.78			$ 105.25			
	Unified Communications Systems Engineer	0	0	1%	$ 75.64			$ 68.76			
Education	Educational Technology Specialist-Instructional Design	0	0	1%	$ 65.45			$ 59.50			
	Senior Educational Technology Specialist-Instructional Design	0	0	1%	$ 72.00	$ 60.00	$ 53.33	$ 65.45	$ 54.54	$ 48.48	
	Training Logistics Coordinator	0	0	1%	$ 55.64	$ 46.37	$ 41.21	$ 50.58	$ 42.15	$ 37.47	
	Training Specialist – Delivery	0	0	1%	$ 55.64			$ 50.58			
	Training Specialist – Development	0	0	1%	$ 55.64	$ 46.37	$ 41.21	$ 50.58	$ 42.15	$ 37.47	
Project Management & Business Analysis	Business Analyst – Analytics	5	0	1%	$ 78.49	$ 65.41	$ 58.14	$ 71.35	$ 59.46	$ 52.86	
	Business Analyst – Project Management Office (PMO)	3	0	1%	$ 86.34	$ 71.95	$ 63.95	$ 78.49	$ 65.41	$ 58.14	
	Portfolio Manager	1	0	1%	$ 90.66			$ 82.41			
	PowerBI Developer	2	0	1%	$ 84.91			$ 77.19			
	Product Management Analyst - Analytics	1	0	1%	$ 97.65			$ 88.77			
	Program Manager	2	0	1%	$ 112.29	$ 93.58	$ 83.18	$ 102.08	$ 85.07	$ 75.62	
	Project Manager	6	0	1%	$ 106.95	$ 89.12	$ 79.22	$ 97.22	$ 81.02	$ 72.02	
	Project Portfolio Management Applications Administrator	1	0	1%	$ 97.65	$ 81.38	$ 72.33	$ 88.77	$ 73.98	$ 65.76	
	Technical Services Coordinator	1	0	1%	$ 65.45	$ 54.54	$ 48.48	$ 59.50	$ 49.58	$ 44.07	

Exhibit I

Roles and Categories

1. **Technical Role**

   a. **Applications Analyst:**
   Collaborates with other Applications Team members and internal UW Medicine customers to provide a service oriented, cross-functional, knowledgeable, single point of technical leadership for application tools and workflows.

   Experience required:
   Three plus (3+) years recent healthcare or IT experience in an area relevant to the role, including:
   - i. One plus (1+) years providing Electronic Health Record (EHR) systems application maintenance/support.
   - ii. One plus (1+) experience with application/system configuration and implementation of clinical information systems (and/or healthcare applications).
   - iii. Experience participating in defining customer requirements, translating them into design specifications.
   - iv. Recent experience with formal project management methods.
   - v. Experience significantly contributing to multidisciplinary work groups in an application development or support setting.
   - vi. Experience independently outlining work plans and meeting deadlines.
   - vii. Experience executing test plans and test cases.
   - viii. Experience supporting small scale enterprise customers, both internal and external.
   - ix. Experience walking clients using systems, preferably in a healthcare environment.
   - x. If Epic: Currently Epic certified in a relevant application.

   b. **Senior Applications Analyst:**
   Collaborates with other Applications Team members and internal UW Medicine customers to provide a service oriented, cross-functional, knowledgeable, single point of technical leadership for application tools and workflows.

   Experience required:
   Five plus (5+) years recent healthcare or IT experience, including:
   - i. Two plus (2+) years' experience with application/system configuration and implementation of clinical information systems (and/or healthcare applications).
   - ii. Demonstrated ability to translate business requirements into design specifications, follow technical change control processes, and maintain technical documentation.
   - iii. Experience mentoring others to increase overall professional effectiveness.
   - iv. Demonstrated ability to manage small to medium sized IT projects and/or process improvement initiatives.
   - v. Demonstrated ability to facilitate and influence multidisciplinary work groups in an application development or support setting.
   - vi. Demonstrated ability to independently outline small project work plans and meet deadlines.
   - vii. Experience developing and executing test plans and test cases.
   - viii. Experience supporting large scale enterprise customers, both internal and external.
   - ix. Experience supporting large scale enterprise customers, both internal and external.

c. Applications Architect:
Provides technical leadership and consultation to the application leadership team and ITS broadly, designs major aspects of the architecture of key applications, including components such as human factors design, application configuration, integration, middleware, and infrastructure, provides architectural review of new applications and solutions that are proposed adds to the UW Medicine application portfolio, in collaboration with other ITS architects, defines, promotes, and educates aspects of an enterprise architecture, and collaborates with governance structures and stakeholders to solve business problems and to ensure that the overall architecture of the application portfolio is continually optimized to support the long-term needs of the organization.

Experience required:
Has consistently demonstrated technical competencies for nine plus (9+) years in relevant functional/business area and must include:

i. Analyzing customer business and technical requirements and issues, recommending solutions.
ii. Designing, building, testing, and implementing enhancements to meet functional requirements.
iii. Providing production support and ongoing system troubleshooting, maintenance, monitoring, and training.
iv. Coordinating design of key UW Medicine applications at a functional and systems level through the development of defined architectural standards.
v. Acting as a knowledgeable resource regarding the Epic Electronic Medical Records (EMR) and other key applications, ensuring effective problem resolution at an application and technical level.
vi. Experience with application/system configuration and implementation of healthcare information technology.
vii. Demonstrate ability to translate business requirements into design specifications, follow technical change control processes, and maintain technical documentation.
viii. Experience mentoring others to increase overall professional effectiveness.
ix. Demonstrate ability to facilitate and influence multidisciplinary work groups in an application development or support setting.
x. Demonstrated ability to independently outline small project work plans and meet deadlines.
xi. Experience developing and executing test plans and test cases.
xii. Experience supporting large scale enterprise customers, both internal and external.
xiii. Experience walking clients using systems, preferably in a healthcare environment.

d. Business Intelligence (BI) Administrator:
Performs the various technical roles in the application administration, development and maintenance of tools, technologies and interfaces between various source systems, support systems, and the Analytics group.

Experience required:
Two plus (2+) years' experience must include, but are not limited to:

i. Performing the various technical roles in the application administration, development and maintenance of tools, technologies and interfaces between various source systems, support systems, and the Analytics group.
ii. Key applications include Tableau, BusinessObjects (WebI and Crystal) Syntellis Performance Solutions (formerly Kaufman Hall Software, Axiom, and Change

Healthcare) Data Warehouse (Horizon Performance Manager) and BI (Horizon Business Intelligence) tools and various custom-developed web-based applications.

iii. Supporting more senior Admins on the Analytics Data Services Team who are responsible for the end-to-end platforms supporting the data solutions we provide for enterprise data warehouse, reporting, visualization, and decision support. The platforms include Microsoft SQL Server, Caradigm Intelligence Platform, Syntellis financial support and reporting tools, Basis of Estimate (BOE), and Tableau, with ongoing efforts to consolidate and simplify this stack.
iv. Two plus (2+) years of recent IT experience.
v. One plus (1+) years of hands-on, enterprise level Windows, Network, and/or Applications Administration and Operations experience.
vi. One plus (1+) years of experience administering tools and technologies in one or more of the following:
vii. BI Admin focus: Architecting and administration of SAP Business Objects (Crystal Reports, Crystal Report for Enterprise, Webi and Cubes), APOS and Tableau application (Tableau Desktop, Tableau Server, Tableau Server Management Add on, Tableau Content Management Tool, and Tableau Services Manager).
viii. Syntellis Performance Analytics Suite (Performance Manager, HBI/Spotfire).

e. **Business Intelligence (BI) Developer**:
Identifies business and technical impacts of user requirements and creates ad hoc queries, data source, extracts, and Clarity-based reports to support the business. The BI Developer works in close collaboration with other Analytics Team members and internal UW Medicine customers to provide a service oriented, cross-functional, knowledgeable, single point of technical leadership for application tools and workflows.

Experienced required:
Three plus (3+) years' experience must include, but are not limited to:

i. Working with other developers and customers to gather, analyze, and document BI requirements.
ii. Utilizing Epic's Cogito suite of tools to deliver data solutions.
iii. Designing, coding, testing, and maintaining BI reporting and analytics objects, including extracts, utilizing industry best practices.
iv. Two plus (2+) years recent healthcare or IT experience.
v. One plus (1+) years' experience with BI reporting tools.
vi. One plus (1+) years' experience with SQL writing complex, highly optimized queries across large volumes of data, database design, data warehouse design, query performance tuning and writing stored procedures.
vii. Apply experience with Epic Cogito tools (SlicerDicer, SQL Metrics, Reporting Workbench, Radar Dashboards, Epic BI Integration).
viii. Demonstrate experience independently working with Epic Clarity Data Model and Reporting for small to medium scale projects.
ix. Demonstrate experience working through the complete report development lifecycle for small to medium scale projects.
x. Strong understanding of BI reporting best practices.
xi. Proficiency with desktop computers and Microsoft Office, and familiarity with Visio and Project applications.

f. **Senior Business Intelligence (BI) Developer**
Identifies business and technical impacts of user requirements and creates ad hoc queries, data source, extracts, and Clarity-based reports to support the business. The BI

Developer works in close collaboration with other Analytics Team members and internal UW Medicine customers to provide a service oriented, cross-functional, knowledgeable, single point of technical leadership for application tools and workflows.

Experience Required:
Four years (4+) years' experience must include, but are not limited to:

i. Collaborating with Analytics leadership to help set direction, standards, process for a team of BI Developers.
ii. Working with Business Analysts and customers to gather, analyze, and document BI requirements.
iii. Designing, coding, testing, and maintaining BI reporting and analytics objects, including extracts, utilizing industry best practices.
iv. Utilizing Epic's Cogito suite of tools to deliver data solutions.
v. Providing production support and responding to help desk tickets related to the BI development tool set.
vi. Four years (4+) years recent healthcare or IT experience.
vii. Three years (3+) years' experience with BI reporting tools.
viii. Three years (3+) years' experience with SQL writing complex, highly optimized queries across large volumes of data, database design, data warehouse design, query performance tuning and writing stored procedures.
ix. Strong, applied experience with Epic Clarity Data Model and Reporting for medium to large scale projects.
x. Strong, applied experience with Epic Cogito tools (Slicer Dicer, SQL Metrics, Reporting Workbench, Radar Dashboards, Epic BI Integration).
xi. Strong, applied experience working through the complete report development lifecycle for medium to la scale projects.
xii. Complete and demonstrable understanding of BI reporting best practices.
xiii. High level of awareness of the current and future BI technologies.
xiv. Advance understanding of basic database structures, data definitions, and data relationships.
xv. If Epic: certification in the applicable data model.

g. **Cloud Architect**
Provides technical cloud subject matter expertise of major cloud providers in designs, leadership, and consultation to the ITS leadership team and ITS broadly, designs major aspects of the architecture including components such databases, data pipelines, governance, security, applications, tools, configuration, integration, middleware, and infrastructure, and provides architectural review of existing and new data integrations and solutions that are proposed adds to the UW Medicine cloud infrastructure.

Experience required:
Nine plus (9+) years of experience must include:

i. Nine plus (9+) years of experience spanning at least two IT disciplines, including technical solution architecture, network management, software defined technologies, application development, middleware, database management or operations.
ii. Five plus (5+) years' experience with solution architecture and deployment within Amazon Web Services (AWS), Azure and/or other public cloud environments.
iii. Experience with Infrastructure as Code and provisioning automation.
iv. Exposure to multiple, diverse technologies and processing environments.
v. Knowledge of all components of technical architecture.
vi. Knowledge of business process re-engineering principles and processes.

vii. Strong understanding of network architecture and application development methodologies.
viii. Strong understanding of SOA, object-oriented analysis, design, and/or client/server systems.
ix. Experience working in a research or academic environment preferred.
x. Nine plus (9+) years' experience in designing large and complex IT operations in large organizations.
xi. Eight plus (8+) years of experience with administering systems, including Four plus (4+) years of experience administering systems that support critical operations.
xii. Six plus (6+) years of experience providing advanced support for the overall health of enterprise systems and technologies.
xiii. Two plus (2+) years of experience developing and leading technical training for teams and mentoring less experienced technical staff members.
xiv. Two plus (2+) years of experience primarily responsible for an enterprise technology.
xv. One plus (1+) years of managing vendor relationships, including negotiating maintenance contracts, reviewing periodic service reviews, and coordinating escalations.
xvi. One plus (1+) years of implementing and improving processes.
xvii. Active member in local technology user groups and/or other professional organizations related to area of expertise.
xviii. Demonstrate experience creating and maintaining detailed documentation, including standard operating procedures, system diagrams, and any other technical documentation including 1+ years of managing technical requirements of an enterprise system.

h. Cogito Developer

Identifies business and technical impacts of user requirements and creates ad hoc and ongoing reports and other data outputs to support the clinical and business needs for the enterprise. The Cogito Developer works closely to collaborate with other Analytics Team members, Epic Applications teams, Clinical Informatics, and internal UW Medicine customers to provide a service oriented, cross-functional, knowledgeable, single point of technical leadership to support Epic data and reporting needs across UW Medicine.

Experience required:

Three plus (3+) years' experience must include the following:

i. Two plus (2+) years recent healthcare or IT experience.
ii. One plus (1+) years' experience with BI reporting tools.
iii. One plus (1+) years' experience with Epic Cogito reporting tools (SlicerDicer, SQL Metrics, Reporting Workbench, Radar Dashboards).
iv. A minimum of one Epic certification OR has obtained Epic proficiency and has consistently demonstrated competencies for 1+ years in relevant/functional business area.
v. Demonstrate experience independently working with Epic Clarity Data Model and Reporting for small to medium scale projects.
vi. Demonstrate experience working through the complete report development lifecycle for small to medium scale projects.
vii. Strong understanding of BI reporting best practices.

i. **Cyber Security Analyst**

Collaborates with Cyber Security Analysts and Engineers to conduct vulnerability and risk management activities, with significant impact to business operations for all UW Medicine

entities and vendors; implementing security tools, platforms and methodologies drawing from industry requirements and frameworks such as Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), and National Institute of Standards and Technology (NIST) to identify and support the mitigation of risks to patient care and critical operations.

Experience required:
Three plus (3+) years of experience must include but are not limited to:

i. Supporting business and executive leadership decisions and prioritization through risk assessment, compliance, and reporting.
ii. Tracking and mitigating known and emergent threats to UW Medicine information assets to support institutional threat awareness, risk assessments, threat detection and analysis, incident response, and cyber security operations.
iii. Supporting projects, applications, and other ITS technology efforts with information security expertise to ensure that design and implementation of technical solutions align with organizational risk management goals.
iv. Consulting with technical and non-technical stakeholders, including internal and external entities, on security best practices to reduce the risk of compromise across people, processes, and technology.
v. Monitoring and developing monitoring processes to proactively identify and respond to threats, vulnerabilities, or risks within UW Medicine.
vi. Supporting Cyber Security Engineers in information security incident triage, containment, and investigative activities, as needed.
vii. Three plus (3+) years' information security experience to include experience in one or more of the following areas: Security Audit, Compliance, Security Engineering, Security Analysis, Security Project Management, Security Architecture, implementing best practices, tools, and technology and/or demonstrated Information Security aptitude.
viii. Strong work experience independently designing, implementing, or maintaining security tools (including threat assessment tools, risk management tools, or vulnerability management scanning systems).
ix. Strong work experience independently conducting security assessments, security control analysis, risk assessments, vulnerability assessments, awareness & training activities, or penetration tests.
x. Strong understanding of, and demonstrated experience with, security security-related technologies, systems, and tools.
xi. Strong understanding of information security threats and vulnerabilities and how they translate to risks.
xii. Demonstrate knowledge of common information security regulations and/or standards such as NIST 800-53/CSF, International Organization for Standardization (ISO) 27001/2, HIPAA, Payment Card Industry Data Security Standard (PCI DSS), and Service Organization Controls (SOC) and how to apply them.
xiii. Strong applied understanding of major operating systems including Windows, Mac OS, Linux, and Mobile Platforms.
xiv. Preferred, but not required: one or more of the following certificates: CEH, CISSP or Academic degree in Cyber Security.

j. Cyber Security Engineer
Collaborates with fellow Cyber Security Engineers and Analysts to conduct vulnerability assessments, threat intelligence, and incident response activities across UW Medicine, with our partner organizations (FHCC, UW Campus, etc.) and vendors, designing,

developing, and implementing security tools and configuration baselines, drawing from industry requirements and frameworks such as HIPAA, HITRUST, and NIST.

Experience required:
Four plus (4+) years' experience must include but are not limited to:

i. Tracking and mitigating known and emergent threats to UW Medicine information assets by leveraging threat intelligence and conducting internal monitoring.
ii. Supporting projects, applications, and other ITS technology efforts with security engineering and design expertise to reduce the risk of compromise across people, processes, and technology.
iii. Monitoring and developing monitoring to proactively identify and respond to threats and vulnerabilities within UW Medicine.
iv. Executing information security incident triage, containment, and investigative activities – including digital forensic efforts – as part of the incident management process to reduce the likelihood of impact to patient care and critical operations in the event of compromise of UW Medicine IT systems or information.
v. Four plus (4+) years' information security experience to include experience in one or more of the following areas: Security Engineering, Security Operations, Security Analysis, Security Project Management, Security Architecture, implementing security best practices, tools, and technologies.
vi. Strong work experience independently designing, implementing, or maintaining security tools (including threat detection tools or vulnerability management scanning systems).
vii. Strong work experience independently performing security assessments, security control analyses, vulnerability assessments, or penetration tests.
viii. Strong understanding of, and demonstrated experience with, security-related technologies, systems, and tools used for the protection of computer networks and information. Strong understanding of information security threats and vulnerabilities and how they translate to risks.
ix. Strong understanding of leveraging - monitoring tools to review and analyze operating system outputs such as authentication logs.
x. Demonstrate application of common information security regulations and/or standards such as NIST 800-53/CSF, ISO 27001/2, HIPAA, PCI DSS, and SOC.
xi. Strong knowledge of multiple applications and major operating systems/platforms.
xii. Strong understanding of risk management concepts, methodologies, metrics, and reporting.
xiii. Experience conducting incident response and forensic investigations with minimal oversight.
xiv. Proficiency with Python, Hypertext Preprocessor (PHP), Perl, or similar scripting languages.

k. **Senior Cyber Security Engineer**
Provides technical leadership and expertise in the following: conducting highly advanced analysis and creating unprecedented solutions to mitigate emergent security threats; enhancing and improving cybersecurity detection and response capabilities; training and providing technical mentorship to junior staff and student workers; acting as a point of escalation for advanced analysis and problem solving; engineering, configuring, testing, and implementing information security products and solutions for unprecedented projects; enterprise efforts on the secure design of technical solutions, applications, and network architecture; and information security projects and initiatives throughout UW Medicine at both operational and strategic levels.

Experience required:
Six plus (6+) years' experience must include, but are not limited to:

i. Independently tracking and mitigating known and emergent threats to UW Medicine information assets by leveraging institutional threat awareness, vulnerability assessments, threat detection and analysis, incident response, cyber security operations, and security education and awareness.
ii. Leading projects, application support, and other ITS technology efforts with security engineering and design expertise to reduce the risk of compromise across people, processes, and technology.
iii. Monitoring and developing monitoring to proactively identify and respond to threats and vulnerabilities within UW Medicine.
iv. Executing information security incident triage, containment, and investigative activities – including digital forensic efforts – as part of the incident management process to reduce the likelihood of impact to patient care and critical operations in the event of compromise of UW Medicine IT systems or information.
v. Six plus (6+) years' information security experience to include experience in one or more of the following areas: Security Engineering, Security Operations, Security Analysis, Security Project Management, Security Architecture, implementing security best practices, tools, and technologies.
vi. Extensive experience designing and implementing security tools (including threat detection tools or vulnerability management scanning systems) at scale in large organizations.
vii. Extensive work experience performing security assessments, security control analyses, vulnerability assessments, or penetration tests.
viii. Advance understanding of, and demonstrated experience with, security-related technologies, systems, and tools used for the protection of computer networks and information.
ix. Demonstrate experience performing threat modeling and vulnerability reviews to make architecture and risk-based design decisions.
x. Demonstrate experience recommending and designing custom signatures, patterns, and configurations for monitoring platforms/tools to review and analyze data, logs, and intelligence.
xi. Advance knowledge of common information security regulations and/or standards such as NIST 800-53/CSF, ISO 27001/2, HIPAA, PCI DSS, and SOC and how to apply them.
xii. Strong knowledge of multiple applications and major operating systems/platforms.
xiii. Experience conducting incident response and forensic investigations with minimal oversight.
xiv. Proficiency with Python, PHP, Perl, or similar scripting languages.
xv. Preferred, but not required: one or more of the following certificates: CEH, CISSP or Academic degree in Cyber Security.

l. **Epic and Data Warehouse Architect – Analytics**

Experience required:
Four years (4+) years of experience includes, but are not limited to:

i. Defining business requirements and creating dimensional model phases of the data warehousing lifecycle.
ii. Supporting Principle and Lead Data Architects in project planning, technical architecture design, end-user application specification and the data staging design and development phases.

iii. Performing design, development, testing and deployment, utilizing industry best practices.
iv. Serving as a subject matter expert for one or more of the following business areas: UW ITS Billing (HB), Professional Billing (PB), Admission/Discharge/Transfer (ADT), and Clinical and Business Operations.
v. Collaborating with analytics solution consumers, business analysts, and report developers to create initial model requirements (grains, additive and non-additive measures, conformed attributes, etc.).
vi. Working directly with business users to define the source application and its data.
vii. Working directly with business users and the reporting team to define reporting needs.
viii. Designing persistent reporting structures, such as data marts, used by the reporting team and other affiliated developers.
ix. Defining mapping between source systems and target reporting objects.
x. Collaborating with Exact, Transform, and Load (ETL) developers to build the reporting structures.
xi. Collaborating with the ETL Architect to provide specifications for a robust ETL system.
xii. Two plus (2+) years of SQL development experience, including complex query optimization & performance tuning.
xiii. Two plus (2+) years SQL Server – T-SQL and SSIS.
xiv. Two plus (2+) years; experience with the design and development of scalable ETL solutions.
xv. Familiarity with Epic's Cogito stack including Clarity or Caboodle.
xvi. Experience with modeling methodologies and demonstrated understanding of principles for data.
xvii. Normalization/denormalization, abstraction, dimensionality as interface, etc.
xviii. Demonstrate knowledge of how data in a relational database is stored, retrieved, and processed, including experience.
xix. Analyzing query statistics and the query plan.
xx. Exposure to project management skills.
xxi. Experience with formal software engineering practices (source code version control, validation / deployment /maintaining Microsoft-based applications).
xxii. Understanding of database design, expertise in several data domains.
xxiii. Demonstrate problem solving & debugging skills.
xxiv. Demonstrate understanding of data warehousing concepts and architecture.

m. **Epic Database Administrator**
Develops, maintains, and monitors the Epic database and associated programming and ensures the reliability, security, and performance of major UW enterprise systems.

Experience required:
Four plus (4+) years recent IT experience that include, but are not limited to:
i. Work with a small team of experts in Epic systems to support to build, configure, deploy, implement, operate, support, and maintain the database of the highly complex, fast-growing Epic environment.
ii. Production, development, testing, and training environments.
iii. Administering enterprise databases at UW Medicine, including operational, technical, and administrative responsibilities.
iv. Implementing data models and database designs.
v. Providing data access and security activities
vi. Resolving database performance issues.

vii. Managing database capacity needs, replication, and other distributed data issues; and
viii. Providing advice, consultation and support to partners, systems managers, senior computing specialists and operations personnel of varying levels of expertise.
ix. Four plus (4+) years programming experience with Cache.
x. Four plus (4+) years of primary database administration experience on large scale database systems providing critical business functions, preferably with Cache, and including:
xi. Complexities of installation of a database on large-scale hardware and storage platforms.
xii. Familiarity with basic UNIX/Linux systems administration.
xiii. Experience of administering databases in a highly available environment.
xiv. Experience with effective database backup and recovery technologies.
xv. Experience with database replication technologies.
xvi. Four plus (4+) years of experience administering Cache/IRIS databases.
xvii. Four plus (4+) years of progressively responsible systems administration, analysis, and programming experience on a broad range of platforms.
xviii. Two plus (2+) years of relational database systems administration and programming experience in a distributed networked client/server environment.
xix. Proven record of system administration and application support in a complex, multi-platform environment.
xx. Demonstrated experience in relational database systems and other technologies.
xxi. Demonstrated experience working with teams in the development and support of applications.

n. **Epic Interface Analyst**
Provides intermediate to advanced level support in the overall development and management of complex, mission critical, enterprise information systems, with an emphasis on clinical and financial system interfaces across all of UW Medicine.

Experience required:
Four plus (4+) years of recent healthcare or IT experience must include:
i. Providing intermediate to advanced level support to the UW Medicine medical community by correlating user needs with information system design.
ii. Performing intermediate to advanced analytical, design, development, operational, and administrative functions associated with the implementation of intermediate to advanced information system solutions.
iii. Participating in and leading small to intermediate level Data Integration Services Team projects and ITS department level projects using project management principles to plan, design, test, execute, and monitor efforts necessary to enhance production systems and implement interfaces.
iv. Participating in team process improvements and personal development activities.
v. Two plus (2+) years providing EHR systems application maintenance/support, configuration, and implementation.
vi. Experience with formal project management methods in conjunction with the management of small to medium clinical information system projects.
vii. Two plus (2+) years of experience with a major electronic health record system with an understanding of UW ITS/clinic workflows such as scheduling/Reg/ADT, orders of ancillary systems, patient care.
viii. Two plus (2+) years of experience with successful systems analysis and/or programming on mission-critical, clinical information systems.

ix. Two plus (2+) years' experience implementing and managing clinical information system interfaces using HL7/X12
x. Currently holds Bridge Certification or proficiency.
xi. Demonstrated understanding of database structures, data definitions, and data relationships.
xii. Demonstrated experience with multiple applications, multiple operating systems and hardware platforms, and their integration into various applications and equipment.
xiii. Knowledge of Health Care regulatory environment and fluent in computer and healthcare related concepts and vernacular.
xiv. Extensive knowledge and applied understanding of Health Level 7 (HL7), Electronic Data Interchange (EDI) American National Standards Institute (ANSI), HyperText Markup Language (HTML), and other healthcare system standards.
xv. Extensive experience with software development lifecycle.
xvi. Extensive understanding of migration methodology between Test and Production domains of an application.
xvii. Extensive knowledge of networked environments, TCP/IP network protocols, and Interconnect.

o. Identity and Access Management (IAM) Analyst
Provides access, maintenance, user support, and additional identity
Services for the UW Medicine workforce in a 24/7/365 UW ITS and Clinical environment.
Experience required:
i. Two plus (2+) years of experience in programming or computer support services of a technical nature OR equivalent education/experience.
ii. Exposure to identifying, troubleshooting, and resolving standard problems with data quality and data analysis.
iii. Exposure to working with end users to identify, understand, and resolve account issues.

p. **Identity and Access Management (IAM) Systems Engineer**
Provides technical engineering, automation, feature development, and integration of critical identity systems and solutions including Active Directory, SailPoint, Okta, Duo/Twilio, Exchange, and Epic and other clinical applications.

Experience required:
Four plus (4+) years of experience must include, but are not limited to:
i. Delivering products and solutions for Single Sign-On, Federated SSO, Multi-factor Authentication, and IAM services.
ii. Developing IAM strategy, architectural blueprint, and implementation roadmap across on premise, cloud, and mobile systems.
iii. Developing, documenting, and maintaining process workflow, dataflow, and requirements for user accounts and practitioner information with a focus on compliance and quality.
iv. Developing requirements and facilitating the implementation of new tools to support the replacement of current provider directory applications.
v. Collaborating on enterprise application projects that require user accounts and/or practitioner information.
vi. Participating in team projects related to process and quality improvements.
vii. Providing exemplary customer service to colleagues and customers.
viii. Four plus (4+) years IT experience within one or a combination of the following: data analysis, data management, programming, or application support services.

ix. One plus (1+) years' professional work experience in identity services, to include more than one of the following: identity governance, IAM architecture, access control, provisioning, IAM data management, or similar areas.
x. Strong experience, and the ability to work independently, in gathering requirements for, designing, developing, automating, and implementing workflows.
xi. Strong experience conducting, and the ability to guide customers through, identity data structures, personnel data, user accounts, and user access levels.
xii. Strong experience in Epic and Active Directory provisioning, or similar tools.
xiii. Demonstrated experience analyzing and updating personnel and/or healthcare practitioner data using IAM applications.
xiv. Strong knowledge, and the ability to work independently, in creating scripts and tools to automate tasks.
xv. Applied knowledge and understanding of IAM platforms and applications, preferably SailPoint IIQ and Okta.
xvi. Applied knowledge of common information security regulations and standards of HIPAA.
xvii. Demonstrated knowledge of SQL skills.
xviii. Applied understanding of the role programming languages play in process improvement (i.e., data validation, data automation, data manipulation, etc.)

q. **Senior Identity and Access Management (IAM) Epic Security Analyst**
Provides technical expertise and servers as the technical lead for Epic security build, testing, and record creation processes, provides technical expertise in access decisions in conjunction with application coordinators/analyst and operations, and provides technical expertise and serving as technical lead on Epic Security projects/initiatives for change management and master file management.

Experience required:
Four plus (4+) years of experience must include, but are not limited to:
i. Training other analysts in technical expertise for performing independent and complex troubleshooting, business analysis, and data analysis.
ii. Providing technical expertise and serving as technical lead for Epic security build, testing, and record creation processes.
iii. Providing technical expertise in access decisions in conjunction with application coordinators/analyst and operations.
i. Providing technical expertise and serving as technical lead on Epic Security projects/initiatives for change management and master file management.
ii. Serving as a liaison between Epic Security and Epic Application teams.
iii. Using business and data analysis, independently troubleshoot and resolve complex Epic security related issues.
iv. Performing user provisioning, integrations, audits, and other daily operations of the Epic Security team.
v. Ensuring compliance with HIPAA, other regulatory requirements, and policy and procedure are met.
vi. Identifying risks and collaborating with Epic Security team on resolution and ITS Leadership on recommendations for risk mitigation enhancements.
vii. Managing on-going security roles and controls for Epic and interconnected applications, including:
viii. Development, implementation, and maintenance.
ix. Collaborating with Epic application teams to create, monitor, and maintain operational configurations of Epic security for efficient and appropriate operations.

x. Managing access and authorization activities across the identity lifecycle.
xi. Identifying and analyzing customer system requirements for continuous improvements.
xii. Maintaining knowledge of vendor application architecture as it relates to the UW Medicine's systems environment as well as any new or modified vendor solutions that could benefit our organization.
xiii. Epic Chronicles and/or Epic Security certification.
xiv. Four plus (4+) years of IT experience.
xv. Four plus (4+) years' experience in systems analysis, administration, or support; preferably on mission-critical clinical information systems.
xvi. Demonstrated experience with project management.
xvii. Advanced experience working with Epic or comparable EHR system for small to medium scale projects.
xviii. Advanced experience independently gathering requirements for the creation of new or changes to existing roles in a healthcare application.
xix. Advanced experience with database management, programming, or access for small to medium scale projects.
xx. Advanced experience independently creating and managing end user workflows.

r. IT Service Management (ITSM) Process Analyst

Assesses, develops, implements, improves, and manages all ITSM policies, processes, and procedures and drives continuous improvements through Key Performance Indicators (KPI's) and customer satisfaction survey results.

Experience required:

Three plus (3+) years' experience must include, but are not limited to:

i. Providing intermediate process design, development, maintenance, and improvement input for Information Technology Infrastructure Library (ITIL) processes used by UW Medicine including Service Level Management, Asset Management, Release Management, Change Enablement, Measurement and Reporting, Request Management, Configuration Management, Incident Management, and Problem Management.
ii. Executing basic facets of one or more key ITIL processes, including running CAB for change enablement, leading RCA (Root Cause Analyses) for problem management, and CI (configuration item) governance for Configuration Management.
iii. Maintaining, and continuously improving, the effectiveness of the CMDB and the portfolio of services tracked and maintained within UW Medicine's ITSM ticket tracking tool (ServiceNow).
iv. Collaborating with service owners, the service desk, and other delivery and support entities to ensure the continual effectiveness of the information stored in the service catalog and the Configuration Management Database (CMDB).
v. Partnering with service owners and other key stakeholders to maintain the continuous integrity of information stored and tracked within ServiceNow.
vi. Employing a structured approach to process design and improvement, including performing a gap analysis between current and future processes.
vii. Assisting in developing and implementing best practices, systems, and tools, and providing guidance and collaborative process management of processes and procedures.
viii. Developing and implementing best practice processes, tools, and metrics for integrating the CMDB with various delivery and support processes, such as: knowledge, incident, problem, change, service request, asset, and other ITSM processes, as required.

ix. Providing collaborative process management of the day-to-day ITSM knowledge in such areas as: service request, incident, problem, change, release, and configuration management processes.
x. Providing data and metrics for decision-making and driving continuous process improvements for all ITSM processes, particularly for the CMDB and service catalog.
xi. Working closely with ITSM process team and stakeholders to solution and propose process, tool and metric, and reporting improvements to ITSM Lead and leaders, as appropriate.
xii. Developing and improving the process and procedures to assist IT teams in maintaining the CMDB and continuously developing the Service Catalog.
xiii. Intermediate level responsibilities are defined by progressively more complex and responsible technical analysis and project tasks, including being the primary point of contact for medium-scale automation, application administration, and system administration. These tasks usually have multi-department impacts and impact 50%-85% of end users and pose a moderate project risk.
xiv. Two plus (2+) years' experience in ITIL-based process, such as: Service Level Management, Asset Management, Release Management, Change Enablement, Measurement and Reporting, Request Management, Configuration Management, Incident Management, and Problem Management.
xv. Possesses ITIL v3 or v4 Foundation Certification (or willing to commit to achieving within 6 months of start date).
xvi. Strong information systems technology process background.
xvii. Demonstrated experience as process owner or practitioner with one or more ITIL processes, including Service Level Management, Asset Management, Release Management, Change Enablement, Measurement and Reporting, Request Management, Configuration Management, Incident Management, and Problem Management
xviii. Understanding of the implementation process and tasks to create a service catalog and CMDB.
xix. Demonstrated experience working and communicating with all levels of leadership.
xx. Demonstrated experience using data and metrics to tell a story and drive for continuous improvement.
xxi. Demonstrated knowledge of IT software and hardware and related licensing agreements.
xxii. Demonstrated knowledge of how Configuration Management integrates and interacts with other ITIL processes, including Service Request, Incident, Problem and Change Management.
xxiii. Demonstrated ability to produce written material (Policies, Process, Procedures, Work Instructions, presentations, reports etc.) to a high standard.

s. **Quality Assurance Specialist**
ensures the quality of applications and systems by developing and executing test scripts to verify solution meets the documented acceptance criteria and design.

Experience required:
Four plus (4+) years' experience must include, but are not limited to:
i. Collaborating with and providing guidance to project teams in medium to large scale testing tools, strategies, methodologies, and processes.
ii. Guide medium to large scale projects through the testing life cycle.
iii. Work closely with users, stakeholders, and project teams to analyze business processes and data.

iv. Utilize user requirements and functional specifications to drive testing decisions.
v. Plan and guide all phases of testing for medium to large scale projects.
vi. Assist business stakeholders and project teams to deliver on time and high-quality applications and systems.
vii. Identify and build service management improvements.
viii. Serve as the manager's delegate to represent the team for automation vendor management, including strategic vendor meetings; architecture meetings; meetings with technical account managers; project design meetings; large scale incident resolution; and other technical leadership needs.
ix. Certified in at least one system testing practice (Computerized system validation (CSV), International Software Testing Qualifications Board (ISTQB) or similar).
x. Two plus (2+) years of experience in testing consulting, coaching, and formal mentorship for technology professionals.
xi. Two plus (2+) years of experience guiding the development, documentation, coordination and maintenance of test processes, standards, templates, and guidelines, including 1+ years of experience serving in a large-scale application testing analyst role.
xii. Demonstrated ability to implement test process improvement effort and enforce testing standards, policies, and procedures.
xiii. Experience working with one or more test management tools (e.g., HP Application LifeCycle Management (HP ALM).
xiv. Intermediate level application testing experience working in a multi-tiered client server environment.
xv. Intermediate level testing experience within a vendor-packaged software environment.
xvi. Demonstrated ability to facilitate and participate in cross-functional, cross organizational work groups to implement clinical or business information systems.
xvii. Demonstrated interpersonal skills including communication, facilitation, and effective meeting management along with strong verbal and written skills.

t. Senior Quality Assurance Specialist

Contributes technical expertise to the successful implementation and support of application systems and infrastructure of UW Medicine.

Experience required:

Six plus 6+ years' experience must include, but are not limited to:

i. Coach and provide consultation to project teams in large scale testing tools, strategies, methodologies, and processes.
ii. Guide large scale projects through the testing life cycle.
iii. Guide work and interactions with users, stakeholders, project teams, and leadership to analyze business processes and data.
iv. Utilize user requirements and functional specifications to drive complex testing decisions.
v. Plan and guide all phases of testing for large scale work.
vi. Collaborate with business stakeholders and project teams to deliver on time and high-Quality applications and systems.
vii. Providing advice, training, coaching and mentorship to team on work techniques, best practices, and operational expertise.
viii. Serve as the manager's delegate to represent the team to customers, project managers, technical leadership, and organizational management.
ix. Certified in at least one system testing practice (CSV, ISTQB or similar).

x. Four plus (4+) years of experience in testing consulting, coaching, and formal mentorship for technology professionals.
xi. Four (4+) years of experience guiding the development, documentation, coordination and maintenance of test processes, standards, templates, and guidelines, including 3+ years of experience serving in a large-scale application testing analyst role.
xii. Demonstrated ability to guide test process improvement effort and enforce testing standards, policies, and procedures.
xiii. Advanced experience working with one or more test management tools (e.g., HP ALM).
xiv. Advanced application testing experience working in a multi-tiered client server environment.
xv. Advanced testing experience within a vendor-packaged software environment.
xvi. Demonstrated ability to guide, facilitate and participate in cross-functional, cross organizational work groups to implement clinical or business information systems.
xvii. Demonstrated interpersonal skills including communication, facilitation, and effective meeting management along with strong verbal and written skills.

u. **Senior Test Automation Engineer**
Defines strategy and process, bringing automation in line with Existing functional aspect of the test effort.

Experience required:
Eight plus 8+ years of experience must include but are not limited to:
i. Design and develop automated testing using the identified automation tool (ALM-UFT, UiPath or other) as an Application Lifecycle Management solution for functional automation.
ii. Design a complex test automation framework to create, execute and maintain simple automated tests.
iii. Create metrics and increase test coverage using the automated systems.
iv. Provide a high level of expertise across the department in testing automation.
v. Strategize, develop, enhance, and govern testing standards.
vi. Create 1-3-5-year technology roadmaps, and present recommendations to leadership.
vii. Optimize the use of technologies and perform cost analysis.
viii. Leverage technical expertise in impactful, enterprise-level projects.
ix. Develop and deliver training across the department in area of expertise.
x. Lead large scale incident resolution.
xi. Identify and build service management improvements.
xii. Certified in at least one system testing practice (CSV, ISTQB or similar).
xiii. Six plus (6+) years of experience developing automated test systems.
xiv. Two plus (2+) years of experience developing and leading technical training for teams and mentoring less experienced technical staff members.
xv. Six plus (6+) years of experience providing advanced support for the overall health of enterprise systems and technologies.
xvi. Two plus (2+) years of experience primarily responsible for an enterprise technology. Proven ability to deliver quality results in a busy and dynamic business focused environment.
xvii. One plus (1+) years of managing vendor relationships, including negotiating maintenance contracts, reviewing periodic service reviews, and coordinating escalations.
xviii. Three (3+) years of implementing and improving processes.

xix. Advanced experience creating scripts beyond record and playback (using C# and/or VB.NET). Specifically developing functions, adding control flow logic, loops etc.
xx. Expert understanding of object-oriented programming, design and debugging skills.
xxi. Expert understanding of software design techniques in healthcare.
xxii. Experience of source control systems and configuration management.
xxiii. Demonstrated experience creating and maintaining detailed documentation, including standard operating procedures, system diagrams, and any other technical documentation, including three plus (3+) years of managing technical requirements of an enterprise system.

v. Software Engineer

Develops and implements a set of medical and non-medical. applications and functions following technical specification used by UW Medicine user population and supports and maintains vendor systems for UW Medicine.

Experience required:

Four (4+) years of experience should include, but are not limited to:

i. Independently providing development and implementation intermediate level tasks such as one or more of the elements among business process analysis, programming, testing, production installation/configuration and system support, documentation, and maintenance of applications/systems.
ii. Independently providing intermediate level system support, implementation, documentation, and maintenance of complex applications, infrastructure, vendor-packaged systems, and technical solutions for UW Medicine internal and external customers across many different functional areas.
iii. 4+ years of recent software engineering experience.
iv. 4+ years hands-on experience with a combination of the following:
    1. Client and Server-side
    2. JavaScript
    3. Procedural programming language, preferably C.
    4. XML
    5. HTML
    6. Relational databases: SQL Server, Oracle, or Ingres.
v. Four plus (4+) years systems analysis experience, including requirements gathering, functional design, and technical design.
vi. Strong understanding of most phases of software development or lifecycle.
vii. Familiarity with the operations of Unix, iOS, and Android
viii. operating system.
ix. Working knowledge of Internet Explorer and Mozilla-based internet browser technology, features, and functionality.
x. Proven experience with unit and systems testing.
xi. Demonstrated ability to produce documentation for:
    1. Functional Requirements
    2. Technical Requirements
    3. System test plans
    4. Operational System documentation
    5. User Guides / documentation
xii. Knowledge of database structures, data definitions and data relationships.

xiii. Demonstrated ability to work with and facilitate multidisciplinary work groups in an application development or support setting.

w. **Systems Database Administrator**
Maintains the enterprise database environments and data content to support the administrative, clinical, and financial computing requirements of UW Medicine.

Experience required:
Four plus (4+) years technology experience should include, but are not limited to:

i. Administer databases supporting clinical, financial, and administrative applications which support patient care.
ii. Providing data access and security activities.
iii. Resolving database performance issues.
iv. Managing database capacity needs, replication, and other distributed data issues; and
v. Providing advice, consultation and support to partners, systems managers, senior computing specialists and operations personnel of varying levels of expertise.
vi. Four plus (4+) years of progressively responsible systems administration, analysis, and programming experience on a broad range of platforms.
vii. Two plus (2+) years of relational database systems administration and programming experience in a distributed networked client/server environment.
viii. Demonstrated experience in relational database systems and other technologies.
ix. Demonstrated communication skills and ability to work with personnel of various levels of technical background.

x. **Senior Network Security Engineer**
Expected to have expertise in contemporary network technologies and protocols including those such as Transmission Control Protocol/Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP), Routing protocols, IPv4, IPv6, QoS, VoIP, and informational security practices.

Experience required:
Six plus (6+) years technology experience should include, but are not limited to:

i. Provide support for all network related services and systems including: L3 firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Data Loss Prevention (DLP), Virtual Private Network (VPN), user remote access, network switches, load balancers and a variety of monitoring, management, and notification systems.
ii. Design and implement network infrastructure solutions, configurations, and architecture, including hardware and software technology in support of UW Medicine datacenter and enterprise network operations.
iii. Designed and implemented the following routing protocols: Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Virtual Routing and Forwarding (VRF), Protocol-Independent Multicast (Multicast PIM), on Juniper equipment.
iv. Designed and implemented the following features Virtual Chassis, First Hop Redundancy Protocols, on Juniper equipment.
v. Provide support for complex network problems and outages.
vi. Analyze network performance, traffic patterns, and capacity planning analysis.
vii. Interface with various customers to determine customer needs.

viii. Provide guidance to on-site technical and operation support in the installation of communications equipment and systems.
ix. Preferred does not require proficiency with Python, PHP, Perl, or similar scripting languages.
x. *Preferred, but not required:* one or more of the following certificates Cisco Certified Internetwork Expert (CCIE), Juniper Networks Certified Expert Lab Exams (JNCIE), Checkpoint Certification for firewalls.
xi. *Preferred by not required*: Experience with Checkpoint firewalls, Palo Alto firewalls, Cisco firewalls, Juniper switches, Juniper routers, Cisco Adaptive Security Appliance Virtual Private Network (ASA VPN), F5 load balancing, Citrix NetScaler, Solarwinds, Cradlepoint, and Ivanti/Pulse Secure Socket Layer Virtual Private Network (SSLVPN).

y. **Senior Data Center Operations Analyst**
Delivers critical data center monitoring and complex logistical and technical support for data center infrastructure, and various computer systems, networks, and backups in the data centers.

Experience required:
3+ years' experience must include, but are not limited to:

i. Coordinate placement, installation, and maintenance/ troubleshooting of systems within UW Medicine data centers ~~a~~according to industry and UWM standards.
ii. Coordinate and complete Break/Fix hardware replacement of components for servers, network, and Storage Area Network (SAN) equipment in any UWM data center.
iii. Install/de-install, troubleshoot/resolve network and other fiber optic cabling for server, infrastructure components or systems.
iv. Respond to data center alarms and identify solutions/remediation for unplanned downtime, outages, or disasters.
v. Coordinate with system manufacturer's representatives to diagnose equipment problems.
vi. Monitor and respond to environmental alarms generated from monitoring tools that support Infrastructure components such as HVAC, Uninterruptible Power Supplies, Fire Alarms, Water, etc.
vii. Perform analysis and configuration of infrastructure monitoring settings.
viii. *Preferred but not required*: Experience with data center management tools such as Cormant Data center infrastructure management (DCIM), Data Communication Equipment (DCE), Nagios, OpenGear.

z. **Senior Software Defined Data Center Engineer**

Experience required:
3+ years' (3+) experience must include, but are not limited to:

i. VMware Experience
    1. VMware virtual infrastructure (at least 6 years' experience with large, complex, multi-site VMware installations)
    2. VRealize Operations (VROPS)

3. Distributed Switches
4. Network File System (NFS) and Virtual Machine File System (VMFS) datastore management, VROPs/Aria, vSAN
5. Lifecycle management (upgrades, patching, security, bugfixes)

ii. Nutanix Experience
1. Nutanix virtual infrastructure (at least 6 years' experience with large, complex, multi-site Nutanix installations), Nutanix Acropolis HyperVisor (AHV).
2. And/or VMware environments (primary virtualization platform: Nutanix/AHV).
3. Nutanix Foundation server,
4. Monitoring and capacity management,
5. Lifecycle management/LCM (upgrades, patching, security, bug fixes), AHV and Elastic Sky X Integrated (ESXi) hypervisors (ESXi/Acropolis Operating System (AOS) clusters),
6. Flow, Nutanix File Services.

iii. Storage focused Software-Defined Data Center (SDDC) Engineer
1. NetApp,
2. ActiveIQ,
3. BlueXP NetApp Cloud Management,
4. NetApp StorageGrid,
5. HP/Brocade SAN switches,
6. SANNav,
7. IBM StorWize FlashSystems
8. IBM SAN Volume Controller (SVC),
9. Spectrum Control monitoring,
10. Storage Insights cloud storage management.

iv. Cloud Experience: AWS, Azure, and/or Google clouds. Nutanix IaaS, Hybrid cloud. Cloud native VM deployment and management

v. Automation: Ansible, Terraform, shell scripts (Linux), PowerShell (Windows).

vi. Knowledge of backup/restore products such as Veeam, IBM Spectrum Protect.

vii. Familiar with Hewlett Packard Enterprises (HPE) ProLiant servers, firmware updates, HPE OneView, iLO, and security management.

2. <u>Communications</u>

a. **Principal, Release Manager**

Coordinates all Epic system upgrades, updates, and downtimes across UW Medicine including the communication of these.

Experience required:

Six plus (6+) years of experience must include, but are not limited to:

i. Coordinate all Epic system upgrades, updates, and downtimes across UW Medicine.
ii. Provide a high level of expertise in assigned domains.
iii. Strategize, develop, enhance, and govern architectural standards.
iv. Manage technical portfolios, research trends, create 1-3-5-year technology roadmaps, and present recommendations to leadership.

v. Provide consultation to leadership and staff on timelines and impacts, release schedules, requirements, and accountability.
vi. Provide consultation and support to other system updates and upgrades that affect Epic users and systems.
vii. Act as a liaison to the Epic vendor regarding issues of support or quality assurance.
viii. Optimize the use of technologies and perform cost analysis.
ix. Leverage technical expertise in impactful, enterprise-level projects.
x. Develop and deliver training across the department in area of expertise.
xi. Lead large scale incident resolution.
xii. Identify and build service management improvements.
xiii. Provide advice, coaching and mentorship to team members on technical expertise.
xiv. Serve as the manager's delegate to represent the team for vendor management, including strategic vendor meetings; architecture meetings; meetings with technical account managers; project design meetings; large scale incident resolution; and other technical leadership needs.
xv. Six plus (6+) years of IT or healthcare experience, including a combination of program management, maintenance, analysis, and administration for mission-critical systems.
xvi. Two plus (2+) years of experience providing consultation to staff and leadership for major system activation, upgrades, updates, maintenance, or similar.
xvii. Six plus (6+) years of experience with administering systems, including 4+ years of experience administering systems that support critical operations.
xviii. Two plus (2+) years of experience developing and leading technical training for teams and mentoring less experienced technical staff members.
xix. Six plus (6+) years of experience providing advanced support for the overall health of enterprise systems and technologies.
xx. Two plus (2+) years of experience primarily responsible for an enterprise technology.
xxi. One plus (1+) years of managing vendor relationships, including negotiating maintenance contracts, reviewing periodic service reviews, and coordinating escalations, project management techniques.
xxii. Advanced knowledge of the systems development lifecycle. One plus (1+) years of implementing and improving processes.
xxiii. Active member in local technology user groups and/or other professional organizations related to area of expertise.
xxiv. Demonstrated experience creating and maintaining detailed documentation, including standard operating procedures, system diagrams, and any other technical documentation, including, one plus (1+) years of managing technical requirements of an enterprise system.
xxv. Demonstrated experience leading, and ability to advise and mentor others in, decision-making and risk assessment for an enterprise level system.
xxvi. Demonstrated experience leading teams in change and release management for an integrated healthcare system such as Epic, IDX, Cerner, or similar system.
xxvii. Direct working experience with Epic upgrades and updates.
xxviii. Demonstrated experience leading teams in application upgrade planning.
xxix. Demonstrated ability to develop system implementation project plans and meet deadlines, preferably with formal project management techniques.
xxx. Advanced knowledge of the systems development lifecycle.

b. **Unified Communications Systems Engineer**

Develops and implements a set of Communication applications and systems used by UW Medicine user population, to provide communication services for UW Medicine.

Experience required:

4+ years communications systems experience. include, but are not limited to:

i. Responsible for the entire lifecycle of intermediate to advanced level communication systems and applications.
ii. Providing intermediate to advanced level business process analysis, requirement gathering, technical specification/design, programming, testing, and production installation/configuration.
iii. Providing intermediate to advanced level system support, implementation, documentation and maintenance of complex applications, infrastructure, vendor-packaged systems, and technical solutions for UW Medicine internal & external customers across many different functional areas.
iv. Evaluating and making recommendations concerning various communication systems. Intermediate to advanced level is defined as:
    1. Being a subject matter expert in 2 to 4 areas used by UW Medicine Telecommunication Systems and being able to provide support to more senior engineers on more complex issues.
    2. Performing the role of technical lead in small to medium scale level projects that impact the telecommunications systems used in a Medical Center and have a duration of 3 to 6 months; these systems may be parts of larger more complex systems.
    3. Troubleshooting and collaborating with a vendor or support engineer using vendor provided documentation and processes and creating departmental procedures as required.
    4. Using system logs and network monitoring tools across multiple systems and networks to resolve complex issues.

v. Experience should include: Four 4+ years hands-on experience with a combination of the following:
    1. Expertise PBX communication platform.
    2. SIP routing configuration.
    3. Communications voice routing configuration and implementation.
    4. VoIP and SIP device programming and Deployment.
    5. Integration of communications systems with middleware applications.
    6. Client and Server applications management and integration.
    7. Communications systems application maintenance/support, configuration, and implementation.
    8. Two plus (2+) years system analysis experience, including requirements gathering, functional design, and technical design.
    9. Two plus (2+) hands-on experience with the following:
        a) Communications systems call center technologies.

3. <u>Education</u>

a. **Educational Technology Specialist – Instructional Design**
Supports UW Medicine's strategy for eLearning curriculum design and development, emphasizing the need to modernize training and re-skill our end users, effectively supplementing our traditional classroom training with online learning options, and applying modern digital solutions appropriately. Applies adult learning principles to analyze, design, develop, implement, evaluate, and maintain all online training modules.

Experience required:

i. 2+ years designing and developing web-based trainings/eLearnings.
ii. 2+ years of experience designing and developing curricula using standardized instructional design methodology and adult learning theory.
iii. 2+ years of experience creating multi-media and eLearning programs using authoring tools such as Articulate Storyline, Adobe Captivate, or Lectora Inspire.
iv. Proficiency in the following:
    1. Microsoft Office Suite (i.e., Word, Excel, Outlook, PowerPoint)
    2. Adobe Photoshop and/or Adobe InDesign
    3. Adobe Captivate
    4. Articulate Storyline 360
    5. Video and audio editing tools such as Camtasia and Audacity
    6. SharePoint
v. Demonstrated experience collaborating with internal teams, external teams, and management to ensure requirements are being met and projects are kept on schedule.
vi. Demonstrated analytical and problem-solving skills.
vii. Demonstrated experience writing, proofing, and editing courseware content for grammar, accuracy, and clarity.
viii. Familiarity with building training programs from the ground up.
ix. Familiarity with synthesizing operational data, regulations, applicable literature and verbal input into appropriate policy and procedure.
x. Some experience with web development and interface development, including developing, bug-testing and troubleshooting web-based content.
xi. Working knowledge of project planning and control techniques, such as work breakdown structures, critical path analysis and conflict resolution.
xii. Ability to coordinate several projects simultaneously.
xiii. Demonstrated experience working with a learning management system such as SumTotal, Canvas, Blackboard, etc.

b. **Senior Educational Technology Specialist – Instructional Design**

The Senior Specialist will provide advanced level responsibilities, which are defined by being a lead resource for multiple, large-scale projects simultaneously and performing progressively more complex and responsible curriculum upgrade tasks. Projects have increased visibility and impact at the department leadership level.

Experience required:

i. 3+ years designing and developing web-based trainings/eLearning.
ii. 3+ years of experience designing and developing curricula using standardized instructional design methodology and adult learning theory.
iii. 3+ years of experience creating multi-media and eLearning programs using authoring tools such as Articulate Storyline, Adobe Captivate, or Lectora Inspire.
iv. Proficiency in the following:
    1. Microsoft Office Suite (i.e., Word, Excel, Outlook, PowerPoint)
    2. Adobe Photoshop and/or Adobe InDesign
    3. Adobe Captivate
    4. Articulate Storyline 360
    5. Video and audio editing tools such as Camtasia and Audacity
    6. SharePoint
v. Extensive experience collaborating with internal teams, external teams, and management to ensure requirements are being met and projects are kept on schedule.
vi. Strong analytical and problem-solving skills.

vii. Extensive experience writing, proofing and editing courseware content for grammar, accuracy and clarity.
viii. Demonstrated experience with building training programs from the ground up.
ix. Demonstrated history of synthesizing operational data, regulations, applicable literature and verbal input into appropriate policy and procedure.
x. Extensive experience with web development and interface development, including developing, bug-testing and troubleshooting web-based content.
xi. Strong knowledge of project planning and control techniques, such as work breakdown structures, critical path analysis and conflict resolution.
xii. Ability to coordinate several projects simultaneously.
xiii. Extensive experience working with learning management systems such as SumTotal, Canvas, Blackboard, etc.

c. **Training Logistics Coordinator**

Develops medical center staffing plans and office processes in support of the training and go-live phases of medium- to large-sized projects, gains and utilizes subject matter knowledge expert on the education logistics of the CIS/ERC departments, Learning Management Systems, and complex logistics for, various departments across UW Medicine and its affiliates as well as the Medical School establishes, refines, and maintains standards for EHR education scheduling and delivery logistics, captures statistics and recommends programmatic changes after analysis of data, coordinates computer training room use and reservation requests from a wide array of UW Medicine departments and resources, and collaborates with educators, analysts, inpatient and ambulatory clinical managers, UW Graduate Medical Education liaisons, UW School of Medicine liaisons, and UW School of Nursing liaisons to develop and maintain class schedules and classroom reservations.

Experience required:

Two plus (2+) years of experience must include but are not limited to:

i. Collaborating with the various onboarding groups to identify and assign training tracks for end users.
ii. Creating EHR classes and registering students in the Learning Hub.
iii. Maintaining, organizing, and distributing participant materials for instructor-led classroom courses.
iv. Preparing and tracking equipment and supplying purchase requisitions for the CIS office and educational offerings.
v. Utilizing MS Office software applications to complete required activities, including the generation of reports and statistics related to training operations.
vi. Two plus (2+) years of healthcare operational or clinical background in a large academic medical center or other health care setting.
vii. Demonstrated experience independently providing technical, end-user support on system applications.
viii. Familiarity with EHR clinical applications in an inpatient, acute or ambulatory care organization.
ix. Demonstrated experience in organizing, planning, and executing projects from vision through implementation, involving internal personnel, contractors, and vendors.

d. **Training Specialist – Delivery**

Develops and delivers effective application courses for a diverse audience of multidisciplinary faculty, staff, and clinical medical students. The Training Specialist – Delivery will apply adult learning principles and a strong working knowledge of Electronic

Health Record ('EHR') functionality and features to deliver effective training. This role will also assist in the development, implementation, and evaluation of EHR training materials on information systems application courses using a standardized instructional design methodology.

Experience required:
Three plus (3+) years of experience must include:

i. Deliver new curriculum and materials to support EHR application projects.
ii. Utilize continuous quality improvement principles to assist in the evaluation of existing curricula as part of the routine maintenance of the EHR application training programs and materials.
iii. Deliver course content for a variety of learning modalities including instructor-led classroom and virtual courses, and "in-service" sessions in outpatient and inpatient settings.
iv. Two plus (2+) years of experience in delivering course content in a variety of learning delivery modalities including instructor-led classroom and virtual courses, e-Learning solutions, and "in-service" sessions in outpatient and inpatient settings.
v. Two plus (2+) years of experience presenting information in a clear and interesting manner, commanding the audience's attention, and handling questions or challenges from the audience.
vi. Excellent verbal and written communication skills, including:
    1. Experience writing, proofing, and editing courseware, content for grammar, accuracy, and clarity.
    2. Experience presenting effectively and confidently, tailoring delivery for desired results.
vii. Proficiency in MS Outlook, Word, Excel, PowerPoint, Publisher, Adobe Acrobat Professional, and Sharepoint.
viii. Familiarity with project planning and control techniques, such as work breakdown structures, critical path analysis, resource analysis, and conflict resolution.
ix. Familiarity with project risk management.
x. Recent experience training EHR clinical applications in an inpatient, acute or ambulatory care organization.
xi. Ability to synthesize operational data, literature and verbal input into appropriate policy and procedure.
xii. Previous experience in business process re-engineering or process improvement is desirable, involving broad-based information systems and utilizing tools and techniques to effect business change.
xiii. Experience in organizing, planning, and executing projects from vision through implementation, involving internal personnel, contractors, and vendors.

e. **Training Specialist – Development**
Supports the development and delivery of effective application courses for a diverse audience of multidisciplinary faculty, staff, and clinical medical students. The Training Specialist – Development will apply adult learning principles and a strong working knowledge of Electronic Health Record ('EHR') functionality and features to analyze, design, develop, implement, evaluate, and maintain effective information systems application courses using a standardized instructional design methodology.

Experience required:
Three plus (3+) years of experience must include:

i. Develop new curricula and materials to support EHR application projects.

ii. Develop new curricula and materials to support EHR application projects.
iii. Utilize continuous quality improvement principles to evaluate and revise existing curricula as part of the routine maintenance of the EHR application training programs and materials.
iv. Deliver course content for a variety of learning modalities including instructor-led classroom and virtual courses, e-Learning solutions and "in-service" sessions in outpatient and inpatient settings.
v. Educational Technology Specialist-Instructional Design.
vi. Two plus (2+) years of experience designing and developing curricula in a complex environment, using standardized instructional design methodology and adult learning theory.
vii. Two plus 2+ years of experience designing and developing curricula that integrate information technology solutions with end user workflow.
viii. Excellent verbal and written communication skills, including:
    1. Experience writing, proofing, and editing courseware content for grammar, accuracy, and clarity.
    2. Experience presenting effectively and confidently, tailoring delivery for desired results.
ix. Experience creating multi-media and eLearning programs using authoring tools such as Captivate, Lectora, Camtasia, Storyline, and Firefly and experience with designing education that incorporates web technologies.
x. Proficiency in MS Outlook, Word, Excel, PowerPoint, Publisher, Adobe Acrobat Professional, and SharePoint.
xi. Familiarity with project planning and control techniques, such as work breakdown structures, critical path analysis, resource analysis and conflict resolution.
xii. Familiarity with project risk management.
xiii. Ability to synthesize operational data, literature and verbal input into appropriate policy and procedure.
xiv. Experience in organizing, planning, and executing projects from vision through implementation, involving internal personnel, contractors, and vendors.

4. <u>Project Management & Business Analysis</u>

a. **Business Analyst – Analytics**
Coordinates the design, development, deployment, and support of all Analytics solutions to support Harborview Medical Center, UW Medicine Montlake Campus, UW Physicians and multiple affiliate organizations.

Experience required:
Two plus (2+) years' experience must include, but are not limited to:
i. Coordinating the design, development, deployment, and support of all Analytics solutions, in conjunction with team members.
ii. Creating and owning development and deployment processes.
iii. Data analysis.
iv. Participating in the communications strategy and plan for Analytics.
v. Participating in internal team development projects, enhancements, and processes.
vi. Completing the intake of ITS projects by providing time estimates, attending project meetings, assigning work to team members, providing updates to manager and Project Management Office (PMO) and ensuring projects are successful.
vii. May support Cogito solutions.
viii. Two plus (2+) years of recent healthcare or IT experience.

ix. One plus (1+) years' experience performing progressively more complex and responsible Business Analysis and Project Management tasks. This includes the ability to lead a project with a duration longer than 3-months, and a level of effort estimate <500 hours.
x. Strong experience with healthcare data analytics. Applied practical knowledge of healthcare data and terminology.
xi. Strong, applied experience with formal project management.
xii. Strong, applied experience supporting a team of developers.
xiii. Demonstrated experience working through the complete report development lifecycle, including leading requirements gathering and documentation.
xiv. Exposure to various systems application maintenance/support, configuration, and implementation.
xv. If Epic: certified in the applicable application or data model.

b. **Business Analyst – Project Management Office (PMO)**
is responsible for working with Project Managers, Technical Analysts, and customers to ensure that the technical solutions implemented by ITS consistently meet the needs of our customers. The Business Analysts in the PMO are the drivers behind UW Medicine's continued growth and success in information technology; with our commitment to continuous process improvement, the Analyst will develop and help implement strategic initiatives for improved efficiency and productivity. The PMO Business Analyst communicates responsibilities and expectations to project team members; manages daily work assignments; identifies and manages issues, risks, and decisions; and ensures quality deliverables and outcomes.

Experience required:
Three plus (3+) years' experience must include, but are not limited to:
i. Conceptualize and communicate solutions to both business and IT partners, providing translation and connection between them, but comfortable straddling both worlds.
ii. With a sense of strong intellectual curiosity, constructively question and influence thought partners across functional areas and end-user audiences due to the level of ambiguity and complexity of requirements.
iii. Work with and across all staff, leadership, and executive levels to accomplish assignments.
iv. Identify and manage organization-wide impacts to ensure alignment with enterprise strategic goals, influencing business policies and practices.
v. Create and drive adoption of new Business Analyst methodologies as appropriate.
vi. Executing progressively more complex business analyses within an information technology environment including scope definition, requirements gathering, performing cost/benefit analysis, business process re-engineering, etc.
vii. Demonstrated experience with a variety of research and analysis techniques, ideally including a mix of both quantitative and qualitative methods for understanding and documenting end-user and business owner requirements.
viii. Defining and translating users' requests into effective, functional/non-functional, and technical specifications and documentation
ix. Takes personal responsibility for meeting customer commitments and correcting customer problems.
x. Demonstrated ability to support and participate in cross-functional, cross organizational work groups to implement projects or organizational changes.
xi. Knowledge of various software development and service management methodologies/concepts (e.g., Agile, Kanban, ITIL, Waterfall).

xii. Awareness of the industry standard Business Analyst best practices (e.g., IIBA BABOK).
xiii. Ability to apply financial concepts such as Total Cost of Ownership (TCO) and Return on Investment (ROI) in practice.
xiv. Experience developing traceability matrixes from requirements and/or assisting with user testing of a software solution.

c. **Portfolio Manager**
Is responsible for leading an ITS team in delivering program projects that span across a service-line.

Experience required:
Eight plus (8+) years of experience which should include:

i. Eight plus (8+) years of experience leading, managing, and coaching technology and/or business professionals in progressively more complicated vendor-packaged system deployment and/or process improvement projects. Progressive, relevant experience related to IT portfolio, program, and project management. This must include demonstrated experience serving a single service line.
ii. Demonstrated experience leading, motivating, and managing various project and program team sizes, including internal and external constituents, while holding all teams accountable for performance.
iii. Demonstrated leadership, diplomatic, and motivational skills including the ability to lead multiple business and technology organizations/business units.
iv. Experience maintaining relationships by engaging business leaders to establish credibility, solve problems, build consensus, and achieve objectives.
v. Demonstrated experience effectively working with multiple, diverse stakeholders in a complex project environment within a cross-functional matrix environment. Experience gaining buy-in from executives, sponsors, team members, stakeholders, and peers.
vi. Proven ability to make independent administrative/procedural decisions and provide guidance and leadership to staff.
vii. Demonstrated experience managing project work and/or work of others within an established standard project lifecycle framework and cognizant of budgetary and resource constraints.
viii. Strong experience presenting to executive sponsors and demonstrated written and oral communication skills with technical staff, non-technical staff, and all levels of management.
ix. Strong experience in Project Methodologies (e.g., Agile, SCRUM, SDLC/Waterfall).
x. Prior experience in a role with significant customer service component.
xi. Experience negotiating vendor contracts.
xii. Experience drafting and submitting budget proposals and recommending subsequent budget changes where necessary.
xiii. Experience researching best practices within and outside the organization to establish benchmark data and using continuous process improvement disciplines to achieve results.
xiv. Technically competent with various software programs including MS Office tools (e.g., Project, Word, Excel, Visio, PowerPoint, and Outlook).

d. **PowerBI Developer**
Is responsible for collaborating and participating in the management of the processes, tools, and data used by our project managers, resource managers, and the PMO to

analyze and collectively manage current or proposed projects. Project Portfolio Management (PPM) areas addressed by the Developer include enterprise information technology governance, project selection, project management, resource management, financial management, and time management. Project portfolio management functions will be performed in partnership with medical center business partners, customer groups, and internal ITS groups.

Experience required:
Four plus (4+) years' experience should include:

i. Four plus (4+) years of business analysis experience in a technical and/or IT environment.
ii. One plus (1+) years' experience with BI reporting/data visualization tools (such as Tableau or Power BI).
iii. One plus (1+) years' experience with SQL to write complex, highly optimized queries across large volumes of data, database design, data warehouse design, query performance tuning and writing stored procedures.
iv. Ability to complete complex project work proficiently using industry standard PPM tools (e.g., MS Project Online/Server, ServiceNow IT Business Management, Clarity, and Planview).
v. Demonstrated experience with report development and data normalization using BI Tools such as Tableau and Power BI for more complex projects.
vi. Ability to develop more complex applications and solutions using MS Suite (Power Automate (Flow), Power Apps, Power BI, SharePoint).Experience leading the development and implementation of process improvement and standards development.
vii. Strong, applied experience working through the complete development lifecycle for analytics solutions including reports and applications, or interfaces.
viii. Strong understanding of visualization reporting development best practices.
ix. Strong understanding of current and future visualization development technologies.
x. Demonstrated knowledge of technical architecture including applications, server, databases and networks with healthcare IT.
xi. Demonstrates proficient knowledge and experience with Microsoft Office suite and project applications.
xii. Ability to apply financial concepts such as Total Cost of Ownership (TCO) and Return on Investment (ROI) in practice.
xiii. Demonstrates understanding of basic database structures. Ability to process data sets using tools such as SQL and MS Excel.

e. **Product Management Analyst – Analytics**
Is responsible for planning, directing, and coordinating a data warehouse to support Harborview Medical Center, UW Medicine Montlake Campus, UW Physicians and multiple affiliate organizations.

Experience required:
Four plus (4+) years of experience must include the following:

i. Four plus (4+) years recent healthcare or IT experience.
ii. Three plus (3+) years' experience performing progressively more complex and responsible Product Management, Business Analysis and Project Management tasks.
iii. Ability to independently lead small projects for healthcare data analytics and apply advanced knowledge of healthcare data and terminology.

iv. Two plus (2+) years being a lead resource in projects using formal project management.
v. Strong experience coordinating a team of analysts or developers.
vi. Advanced experience working through the complete report development lifecycle, including leading requirements gathering and documentation.
vii. Advanced experience providing, and the ability to independently guide customers through, various systems application maintenance/support, configuration and implementation.
viii. Exposure to various systems application maintenance/support, configuration and implementation.

f. **Program Manager**

Is responsible for program outputs and outcomes to align with UW goals and objectives. Program Manager is required to define, create, and maximize and deliver benefits. Program Manager identifies and analyzes stakeholders' needs and expectations to foster stakeholder support through expert communications. Program Manager performs program level decision making, establishes practices to support the program and maintains program oversight. Manages program activities required to facilitate program definition, program delivery, and program closure.

Experience required:

Seven plus 7+ years' experience should include:

i. Seven plus (7+) years of experience serving in a project leadership role with responsibility for managing progressively more complicated vendor-packaged system deployment and/or process improvement projects.
ii. Demonstrated experience leading, motivating, and managing various project and program team sizes, including internal and external resources, while holding all teams accountable for performance.
iii. Demonstrated leadership, diplomatic, and motivational skills including the ability to lead up, across, and down multiple business and technology organizations/business units.
iv. Demonstrated experience effectively working with multiple, diverse stakeholders in a complex project environment within a cross-functional matrix environment.
v. Demonstrated experience managing project work and/or work of others within an established standard project lifecycle framework.
vi. Strong experience presenting to executive sponsors and demonstrated communication skills; both written and oral with technical and non-technical staff, all levels of management.
vii. Strong experience in successfully leading projects and programs to on-time, on-schedule and within budget close.
viii. Strong experience in Project Methodologies (e.g., Agile, SCRUM, SDLC/Waterfall).
ix. Experience negotiating vendor contracts.
x. Experience drafting and submitting budget proposals and recommending subsequent budget changes where necessary.
xi. Experience maintaining relationships by engaging business leaders to establish credibility, solve problems, build consensus, and achieve objectives.
xii. Experience influencing and gaining buy-in from executives sponsors, team members, stakeholders and peers.
xiii. Experience researching best practices within and outside the organization to establish benchmark data and using continuous process improvement disciplines to achieve results.

xiv. Technically competent with various software programs including MS Office tools (e.g., Project, Word, Excel, Visio, PowerPoint, and Outlook).

g. **Project Manager**
Is responsible for leading teams to deliver a program or project(s) that span across one or more business units. This includes managing resources, schedules, financials, and approach throughout the full project life cycle. This also includes management of issues, risks, and project change requests to ensure successful and on-time project delivery for UW Medicine entities and affiliates.

Experience required:
Four (4+) years' experience should include:

i. Four plus 4+ years' experience serving in a project team leadership role with responsibility for managing vendor-packaged software deployment projects and/or process improvement projects.
ii. Four plus 4+ years' experience effectively working with multiple, diverse stakeholders in a complex project environment.
iii. Four plus (4+) years' experience managing project work and/or work of others within an established standard project lifecycle framework.
iv. Four plus (4+) years proven experience in a project leadership role with progressively complicated projects.
v. One plus (1+) years of recent experience utilizing MS Project to manage projects.
vi. Experience in SDLC, Waterfall, and Agile Project Methodologies.
vii. Technically competent with various software programs including MS Office tools (e.g., Word, Excel, Visio, PowerPoint, and Outlook).

h. **Project Portfolio Management Applications Administrator**
Is responsible for collaborating and participating in the management of the processes, tools, and data used by our project managers, resource managers, and our PMO to analyze and collectively manage current or proposed projects. Project Portfolio Management (PPM) areas addressed by the Administration include enterprise information technology governance, project selection, project management, resource management, financial management, and time management. Project portfolio management functions will be performed in partnership with medical center business partners, customer groups, and internal ITS groups.

Experience required:
Four plus (4+) years' experience should include:

i. 4+ years recent project or portfolio management experience.
ii. 4+ years of business analysis experience in a technical and/or IT environment.
iii. Ability to complete complex project work proficiently using industry standard PPM tools (e.g., MS Project Online/Server, ServiceNow IT Business Management, Clarity, and Planview).
iv. Supports report development and data normalization using BI Tools such as Tableau and Power BI for more complex projects.
v. Ability to develop more complex applications and solutions using MS suite (Power Automate (Flow), Power Apps, Power BI, SharePoint).Experience leading the development and implementation of process improvement and standards development.
vi. Demonstrated knowledge of technical architecture including applications, server, databases and networks with healthcare IT.
vii. Demonstrates proficient knowledge and experience with Microsoft Office suite and project applications.

viii. Ability to apply financial concepts such as Total Cost of Ownership (TCO) and Return on Investment (ROI) in practice.
ix. Demonstrates understanding of basic database structures. Ability to process data sets using tools such as SQL and MS Excel.

i. **Technical Services Coordinator**
Manages medium level, technical projects for the Enterprise Technology Services and Architecture ('ETS') program, participating in complex ETS-related technical operational activities, and in conjunction with members of the ITS project team, functions as a TSC for larger organizational projects.

Experience required:
Four plus (4+) years' experience must include:
i. 4+ years' project management experience.
ii. 4+ years' experience planning, coordinating, executing, and managing technical activities.
iii. 4+ years hands-on technical experience with Windows and UNIX (preferably IBM AIX or Linux) systems.
iv. Demonstrated experience guiding standard projects for database technologies, preferably Oracle and SQL.
v. Demonstrated experience working with complex systems providing critical business functions for small to medium projects.
vi. Demonstrated skills in facilitation, effective meeting management, and agenda development.