Columbia Valley Community Health
Remote Access Agreement

To ensure the integrity, confidentiality and security of the Columbia Valley Community Health ("CVCH") network the following application will be reviewed by the CVCH Privacy Officer for eligibility and need for access. Five (5) business days after the approval of the CVCH Privacy Officer, the applicant will receive an e-mail from Information Technology ("IT") at CVCH with user instructions. Information on how to obtain the user ID and password will also be contained in the body of this email.

To ensure the integrity, confidentiality and security of Protected Health Information ("PHI") as defined under Public Law 104-191 ("HIPAA") and the network, the following agreement will be in effect until terminated by CVCH, the person whose signature appears at the bottom of this agreement (the remote user) or the healthcare organization represented by the remote user.

Remote Access Agreement:

1. I understand and agree that I have been granted remote access to the CVCH network or the EHR via a unique security code. I will not disclose to or share with any other person the security code that has been granted me.
2. I will not use or attempt to use any other security codes to access data in the CVCH systems other than those authorized and assigned to me by CVCH.
3. If I have reason to believe that the security code assigned to me has been breached, I will immediately notify CVCH's IT department at 509.662.6000 ext. 1100 for assignment of a new code.
4. I will access the CVCH network in the manner designated by CVCH:
    a. I will comply with HIPAA regulations and Washington State Law regarding PHI.
    b. I will not leave my computer unattended while still connected in a remote session. When I am finished with a remote session, I will promptly logoff the system and end the connection.
    c. I will not discuss any information, status, treatment or condition of a CVCH patient with anyone, except as required for healthcare treatment, healthcare planning, quality assurance or peer review matters. I will not use or disclose any information other than what is medically necessary or in a manner which may compromise the confidential nature of the information being provided from the CVCH network.
    d. I will not review information within any medical record that is not pertinent to the care of the patient and/or my purpose for reviewing the record. I will not access my own records or records of my family members.
    e. I understand that my access to and use of the CVCH network may be monitored and audited.
5. I understand that CVCH will not be liable to any other persons at off-site locations while I'm accessing the CVCH network.
6. I agree that any documents, reports, or data created as a result of my work-related activities are owned by CVCH.
7. I agree to limit the creation of documents only when necessary and will safeguard PHI in accordance with HIPAA regulations.
8. CVCH is not responsible for maintaining or repairing equipment used for remote access.
9. Any equipment used for remote access will be protected from unauthorized or accidental access, use, or disclosure while being used to access the CVCH network.
10. I agree to only access CVCH information from an approved/designated setting, to protect the confidentially, integrity, and availability of this information.
    a. VPN Access is not readily available to remote vendors or auditors. Access is available through Remote Application framework. VPN access will be evaluated on a case by case basis and minimum requirements below:

b. **By logging in and using CVCH resources, you agree that your device or computer complies with the following requirements:**
    1) Current anti-virus and anti-malware with up-to-date definitions.
    2) Windows updates installed up to the previous month.
    3) Full drive encryption enabled. (FIPS 140-2 certified) i.e.: Bitlocker, Sophos Safe Guard, Check Point FDE, and McAfee Complete Data Protection
c. Athena Remote User Browser requirements:
    1) Google Chrome v89 or higher.
    2) Microsoft Edge

11. I agree to hold CVCH harmless from and against all claims, liabilities, costs, expenses, and damages arising out of or in connection with my failure to adhere to the requirements stated in this application.
12. **I will immediately report any security incidents, breach or possibility of breach of PHI to my Supervisor and the CVCH Privacy Officer at 509-662-6000.**

I hereby affirm by my signature that I have read the above Remote Access Agreement, understand its subject matter and agree to all of the above terms and conditions. I understand that any breach of this agreement may be grounds for disciplinary action including termination of access to the CVCH network. CVCH will also be entitled to all remedies it may have under written agreement or applicable laws, as well as to seek and obtain injunctive and other equitable relief, or contact law enforcement.

(NOTE: All fields below must be filled out; otherwise, access will not be granted)

Where will you be accessing CVCH PHI information from? _____

How will the PHI accessed in the EHR be used? (e.g. care coordination, auditing) _____

Time frame access is requested: **Start Date** _____ to _____ **End Date**

_____
Organization Requesting Remote Access

_____ _____
Applicant's Printed Name **Applicant's Title/Department**

_____ _____
Applicant's Signature **Applicant's Phone Number**

_____
Applicant's E-mail Address

_____ _____
Applicant's Supervisor Signature **Supervisor's Phone Number**

_____ _____
Signature of Requesting Organization's Privacy Officer **Date:**
(If there is no Privacy Officer, then Your Site Representative)

***Once you have completed this form in its entirety please send it via email to: privacy@cvch.org