**[Insert Practice Name]**

Remote Access Request Form

|  |  |
| --- | --- |
| **Remote User Details** | |
| Company Name (if applicable): | |
| First Name: | Last Name: |
| Requestor Signature: | |

**Safe Computing Requirements:**

# Remote access users accessing **[Practice Name]** IT systems must always follow safe computing practices. Unsafe computing will be considered a violation of **[Practice Name]** policy, and subject to discipline up to and including termination under **[Practice Name’s]** employee manual. Safe computing practices include the following:

## Remote access devices must always use up-to-date antivirus protection.

* Antivirus protection must run in real time, with daily updates turned on, spyware detection turned on, firewall turned on. Full virus scans must be run on at least a weekly basis. (Tip: These requirements are typically the default settings when virus software is first installed.)
* Remote access devices must have current operating system versions, set to either regularly apply system updates and patches automatically or notify the user of their availability.
* Web browser pop-up blocking must be turned on.
* No password or PIN should ever be stored on the remote access device in an unencrypted format.
* The user complies with **[Practice Name]** policy regarding password changes and strength.
* Remote access devices should be locked down before being left unattended. (For example, setting up the screensaver to require a password on resume.)
* Remote access device’s networking capabilities, such as Bluetooth, must be deactivated in public areas.
* No PHI or **[Practice Name]** confidential or trade information may be stored on the remote device or on removable media such as flash drives or CDs.
* Remote access users who print PHI or **[Practice Name]** confidential or trade information must abide by all HIPAA security measures as to the use, handling, storing, and disposition of protected documentation.

**[Practice Name]** | Remote Access Confidentiality and Security Agreement

### I understand that **[Practice Name]** (the “Practice”) in which and for whom I work, volunteer, or provide services, or with whom the entity for which I work has a relationship (contractual or otherwise) involving the exchange of health information has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients’ health information. Additionally, the practice must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, information or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, “Confidential Information”).

During my employment/assignment at the practice, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job duties in accordance with the practices privacy and security policies, which are available on Practice’s intranet. I further understand I must sign and comply with this Agreement to obtain authorization for access to Confidential Information or to the Internet through systems provided by the practice.

* I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.
* I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
* I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if

the patient’s name is not used.

* I will not make any unauthorized transmissions, inquiries, modifications, or deletions of Confidential Information.
* I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the practice for any reason.
* Upon termination, I will immediately return any documents or media containing Confidential Information to the Practice.
* I understand that I have no right to any ownership interest in any information accessed or created by me during and in the scope of my relationship with the Practice.
* I will act in the best interest of the Practice and in accordance with this code of conduct at all times during my relationship with the Practice.
* I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss

of privileges, and or termination of authorization to work within the Practice, in accordance with the Practice’s policies

* I will only access or use systems or devices that I’m officially authorized access, will only do so for the purpose of delivery of medical services, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
* I understand that I should have no expectation of privacy when using Practice information systems. The Practice may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
* I will practice good workstation security measures such as locking up portable media when not in use, using screensavers with activated passwords appropriately, positioning screens away from public view, and not leaving reports with Confidential Information lying unsecured.
* I will practice secure electronic indications by transmitting Confidential Information only to authorized entities in an encrypted format.
* I will use only officially assigned user ID and password information.
* I will only use devices that meet the Safe Computing Requirements.
* I will never disclose passwords, PINs, or access codes to anyone else.
* I will never use tools or techniques to break or exploit security measures.
* I will never use unsecured public devices and/or networks to access Practice data and/or systems.
* I will immediately notify the Practice administrator or IT if my password has been seen, disclose, or otherwise compromise, and I will report activity that violates this agreement, privacy and security rules, or any other incident that could have any adverse impact on Confidential Information.

## Vendors requesting access under a corporate account (multiple people utilizing a single corporate login) are required to keep detailed records of who utilize the account including dates, start and stop times, and who/what was being worked on. These reports must be submitted to Practice administrator monthly. They may be audited against actual connection logs. The vendor’s inability to produce these reports or vendor’s noncompliance will result in revocation of access privileges.

By accessing a patient’s record or Confidential Information, I am affirmatively representing to the Practice at the time of each access that I have the requisite business need to know and appropriate consent and the Practice may rely on that representation in granting such access to me.

**By signing this document, I acknowledge that I have read this Agreement and agree to comply with all the terms and conditions stated above.**

### Signature / Date Printed Name

**[Practice Name]** | Remote Access User Information

|  |  |
| --- | --- |
| Company Name (if applicable): | |
| Remote Access User First Name: | User Last Name: |
| Emergency Contact Phone Number: | Personal Email Address: |
| Access type: (check one)   * Employee * Vendor * External Physician | |
| Physical Information About Remote Access Location and Device   * Photographs Attached * Operating system: version: Automatic updates activated  * Malware application:   + Real-time virus protection activated   + Virus definitions set to update at least daily   + Full-system scan set to run at least weekly | |
| [Practice Name] Systems to be Accessed:   * O365 (including Email, calendar, Word, Excel, PowerPoint, and Access) * [Insert EHR and/or PM system name] * Other Imaging Systems (such as OCT, clinical photography, IOL, and similar) * QuickBooks Accounting * Other: | |
|  | |
| Administrator Approval:    Signature Date | |

**CREDIT STATEMENT**

The COVID-19 Employee Guidance for Operational Safety was adopted from policies provided by:

* Peter D Berger, MBA, Administrator, Orion Eye Center, LLC, Redmond, Oregon.

