Access & Confidentiality Agreement

Why I am Being Asked to Sign this Agreement?

You are being given access to Carilion Clinic's ("Carilion") **Confidential Information** in order to perform services for Carilion Clinic. Carilion has legal and ethical responsibilities to **safeguard** the privacy and security of Confidential Information as it relates to its employees, students, patients and business operations.

You are expected to safeguard Carilion's Confidential Information as well.

What is Confidential Information?

Confidential Information is information that is not known to the public. It may be verbal, on paper or in electronic format. When we use the term Confidential Information at Carilion, we are referring to these three (3) types of information:

1) **Protected Health Information (PHI):** PHI is individually identifiable information about our patients. PHI includes information related to the past, present, or future physical or mental health/condition of a patient, the provision of health care to the patient or payment information. Simply being a patient at Carilion is considered PHI.

   Other Examples include:

Name	Date of Birth	Social Security Numbers
Medical Record Numbers	Health Plan Beneficiary Numbers	Full Face or Comparable Photos
Telephone Numbers	Geographic Information	Any Unique Identifier

2) **Employee Confidential Information:** Employee confidential information is *any* information that can be used to identify an employee.

   Examples include:

Full Name	Social Security Number	Drivers' License Number
Bank Account Numbers	Home Address	Email Address
Date of Birth	Telephone Numbers	Earnings Information

3) **Business Confidential Information:** Business Confidential Information is important information about a company that should not be made public.

   Examples include:

Contracts	Financial Data	Strategies
Negotiations	Intellectual property	Inventories
Operations	Processes	Policies

Who is responsible for protecting Carilion's Confidential Information?

EVERYONE at Carilion is responsible for doing their part to safeguard the Privacy and Security of Carilion's Confidential Information, including external parties who perform work for Carilion such as vendors. Carilion's policies are available on the Intranet at PageCenterX, once access has been granted. We want our work with vendors to be successful, so if you have questions, be sure to ask your management team or you may contact Carilion's Privacy Office at privacy@carilionclinic.org.

Access & Confidentiality Agreement

What does it mean to "Safeguard"?

Safeguards refer to reasonable measures Carilion expects you to take to protect the Confidential Information you have been given access to.

Here are some examples:

Reasonable Safeguard	Unreasonable Safeguard
Protecting Carilion's confidential information regardless of your work location (e.g., at work, coffee shop, airport, home).	Leaving your workstation unattended and unsecured while working at home where family or friends have the ability to see or access Carilion's confidential information.
Logging out/tapping out of applications when leaving your workstation unattended to prevent unauthorized access.	Leaving applications open when you step away from your workstation and minimizing your screen.
Choosing a password that you can easily remember.	Writing your active directory ID and password down on a sticky note and putting it in your laptop bag.
Positioning monitors away from the view of the public or using privacy screens.	Allowing a monitor to face outward in a busy hospital corridor with no privacy screen.
Limiting access to confidential information based on job role, including storing servers and other equipment in secure areas with limited access.	Allowing unauthorized individuals into secure or restricted areas, including propping doors open making access available to unauthorized individuals.
Using your workstation for work-related purposes, keeping personal use to a minimum, consistent with department or management guidelines.	Surfing websites for non-business-related reasons on your Carilion devices, especially those that are high-risk and likely to introduce malware into our system (e.g., social media and pornography), or using your workstation for other non-business related reasons, such as to promote, maintain, or run a business that is not affiliated with Carilion Clinic.
Complying with applicable password policies and procedures, including not disabling Carilion set password protected screensavers with preset timeout periods and not sharing password or login information with others.	Allowing a new co-worker whose access has not yet been set-up to use/work under your access.
Installing only authorized software on workstations and using approved hardware.	Bringing your personal flash drive to work and plugging into your workstation.
Storing all confidential information on network servers and secured shared drives.	Storing confidential information on your desktop, personal devices, downloads folder, or unsanctioned cloud-based storage platforms, such as Drop Box or Google Docs.
Secure portable devices by closing your office door or carrying them with you.	Leaving laptops and other portable devices unattended in open classrooms or offices, waiting rooms, your car, etc.
Leaving your workstation on, but logged off, in order to facilitate after-hours updates.	Not following recommended security updates.
Ensuring all Carilion required security settings are maintained and are not disabled or modified.	Disabling encryption on Carilion Devices.
Using my Carilion-issued device to take a photograph of a patient's wound for inclusion in the medical record for treatment related purposes.	Using my personal cell phone to take a video of a patient who is acting erratically to share with co-workers and on social media.

CARILION CLINIC

Access & Confidentiality Agreement

What rules do I need to be aware of regarding obtaining access to Carilion's Confidential Information and how to be sure I keep that access so I can perform my job duties?

As a condition of receiving access to Carilion's Confidential Information, please read each of the following statements and mark the box with an "X" indicating your agreement.

I hereby agree to and understand the following:

General Rules

- ☐ I will report to my Carilion Clinic liaison or to the Carilion Clinic Privacy Office any individual's or entity's activities that I have a good faith belief may compromise the privacy or security of Carilion's Confidential Information.
- ☐ I have no ownership interest in or right to Carilion Confidential Information.
- ☐ Carilion maintains an audit trail of all accesses to Confidential Information and my access may be audited at any time.
- ☐ If I violate this Agreement, I may be subject to disciplinary measures, including revocation of my access to Carilion information, termination of Carilion's contract with the vendor I represent, or similar measures.
- ☐ The conditions of access discussed in this Agreement apply whether I work onsite at a Carilion facility or at a remote location, such as my home.

Protecting Confidential Information

- ☐ I am responsible for all actions that occur with my Carilion access resources including but not limited to, my username and passwords, keys, access codes, badges, and proxy cards. I understand that I may not use these resources for personal gain or knowledge. (e.g., I may not use my Carilion badge to gain entry to a secure floor to go visit an ill relative who is a patient.)
- ☐ That the credentials I have been provided with such as usernames, passwords and my Carilion badge are unique to me and are the equivalent of my legal signature. I will safeguard my access at all times. I will not share my credentials or allow anyone to perform work under my username and passwords, even if I am present. Likewise, I will not request access to, use, or work under any other individual's passwords or access information.
- ☐ If I have reason to believe that any of my accesses have been compromised, I will contact the Technology Service Center at (540) 224-1599 immediately for assistance. (e.g., password hacked)
- ☐ Carilion workstations are supplied for purposes of performing Carilion's work and may only be used for personal use as outlined by Carilion.
- ☐ I am responsible for securing my workstation when I leave it unattended. If I am using a shared workstation, I understand it is my responsibility to log off of applications when I leave the workstation unattended.

- ☐ I may not use or download Confidential Information onto non-authorized devices or unapproved cloud-based storage, even in the performance of my duties.
- ☐ I may not install or operate any non-licensed software on a Carilion device.
- ☐ I will not photograph, video, or make audio recordings of patients or visitors unless it is for care of the patient, identification of the patient, formal education or training, IRB approved research, or as authorized by the patient or their legal representative. I will use only Carilion-approved devices to make such recordings.
- ☐ Confidential Information must be properly disposed of when it is no longer needed according to Carilion Clinic data and record retention policies. I will contact the Privacy Office, Information Security, or HIM if I am unsure how to properly dispose of Confidential Information, or devices containing Confidential Information.

Using Access Appropriately

- ☐ Access to Confidential Information includes information in all formats: paper, electronic and verbal. This means things I may see and hear in the performance of my job duties may be considered confidential. **I understand that simply being a patient here at Carilion is considered protected health information (PHI), which means that is Confidential Information.**
- ☐ I may NOT access, use, disclose, copy, remove from the premises, alter, or destroy Confidential Information, to which I have or had access to, except as clearly permitted and authorized within the scope of my job duties and in accordance with applicable Carilion policies, procedures and applicable laws and regulations.
- ☐ I may only release patient information from the EPIC Release of Information (ROI) module which logs and tracks the release of patient information for HIPAA purposes. I understand that I cannot print from Chart Review or take screenshots of Epic. If I have questions or concerns about ROI, I will contact HIM before releasing requested patient information.
- ☐ I may only access, use, and disclose the minimum necessary amount of Confidential Information as authorized and needed to perform services for Carilion Clinic.
- ☐ **Accessing patients in Carilion's Epic without a business purpose is strictly prohibited.** This includes, even with written/verbal permission or power or attorney, accessing the health information of children, parents, partners, spouses, coworkers, friends, and neighbors.

My signature below indicates that I have read, accept, and agree to abide by all the requirements described above.

Please submit a copy of your government issued, photo ID along with this form.

Company Name:_____ Phone Number:_____

Company Address:_____

Email Address:_____ Carilion ID: _____

Print Name:_____ DOB: _____ Last 4 Digits of SSN:_____

Signature_____ Date: _____