SAMPLE CLINIC CONFIDENTIALITY AND TECHNOLOGY ACCESS AGREEMENT

For employees, contractors, volunteers, students, and other authorized users

Organization:	_____	**Effective date:**	_____
User name:	_____	**Role/department:**	_____

Important: This sample is provided for operational planning and educational use. It is not legal advice and is not a substitute for review by the organization's legal counsel, compliance officer, privacy officer, or human-resources advisor. Adapt it to the organization's policies, workforce, systems, and applicable requirements.

Purpose and acknowledgment. I understand that access to the organization's patients, workforce, business information, technology systems, networks, cloud services, facilities, and equipment is a privilege. I agree to follow this agreement and all related organizational policies. Violations may result in loss of access, disciplinary action, termination of employment or association, and possible civil or criminal consequences.

Confidential information

"Confidential information" includes information in any format that:

- relates to patients, prospective patients, or their families;
- concerns the organization, its workforce, vendors, business operations, finances, security, or technology and is not public;
- belongs to another company or person and was provided in confidence;
- includes usernames, authentication methods, recovery codes, network details, system configurations, or security procedures.

I agree to the following

1. **Authorized access only.** I will access, use, create, transmit, or disclose confidential information only as required for my authorized duties and only through approved systems and workflows.
2. **Minimum necessary use.** I will use only the minimum information and access reasonably needed to perform my duties. I will not access records concerning myself, relatives, friends, coworkers, public figures, or other persons without an authorized job-related reason.
3. **No credential sharing.** My username, password, passkey, security key, and MFA approval are equivalent to my electronic signature. I will not share them, approve another person's sign-in, or use another person's credentials.
4. **MFA safety.** I will not approve an unexpected MFA prompt. I will report repeated or suspicious prompts, lost authentication devices, or suspected account compromise immediately.
5. **Password and recovery protection.** I will not store passwords or recovery codes in unapproved documents, browser notes, email, text messages, or shared files. I will use the organization's approved password-management and recovery process.
6. **Device security.** I will lock my screen when unattended, protect devices from unauthorized viewing or use, and follow requirements for passwords, encryption, updates, antivirus, and automatic timeouts.
7. **Software and browser controls.** I will not install, remove, modify, or bypass software, browser extensions, security controls, remote-access tools, or device settings unless authorized.
8. **Approved communications and storage.** I will use only approved email, messaging, file-sharing, cloud-storage, and collaboration systems. I will not forward confidential information to personal email, store it in personal cloud accounts, or copy it to unauthorized media.

9. **Microsoft, Google, and Zoho services.** I will use Microsoft 365, Google Workspace, Zoho Workplace, OneDrive, Google Drive, Zoho WorkDrive, and similar services only as configured and approved by the organization. I will not create public links or external sharing without authorization.
10. **AI and online services.** I will not enter patient information, confidential business information, credentials, internal documents, or screenshots into public or unapproved artificial-intelligence tools, transcription services, websites, or browser-based utilities.
11. **Remote work and remote access.** I will use only approved VPN, remote-support, remote-desktop, and telework methods. I will not bypass access restrictions, connect through unapproved remote tools, or allow another person to observe or use an active session.
12. **Networks and guest access.** I will connect clinic devices only to approved networks. I will not move devices between guest, staff, clinical, medical-device, or management networks or alter network connections without authorization.
13. **Personal devices and removable media.** I will not use a personal computer, phone, tablet, USB drive, external drive, or other removable media for organizational information unless specifically authorized and secured under organizational policy.
14. **Printing, scanning, and disposal.** I will protect printed, scanned, photographed, faxed, and copied information; retrieve output promptly; use approved scan destinations; and dispose of records and media using approved secure methods.
15. **Screen sharing and meetings.** Before screen sharing, recording, presenting, or participating in a remote meeting, I will prevent unauthorized disclosure of patient information, notifications, files, browser tabs, and credentials.
16. **Monitoring and audit.** I understand that the organization may monitor and audit activity on its networks, systems, applications, accounts, and devices as permitted by policy and law. I have no expectation of privacy when using organizational technology except as provided by law or written policy.
17. **Incident reporting.** I will promptly report suspected phishing, misdirected messages, lost or stolen devices, unauthorized access, malware, accidental disclosure, inappropriate access, or other security and privacy concerns.
18. **Cooperation with safeguards.** I will attend required training and follow organizational policies, security procedures, and applicable state and federal requirements concerning confidentiality, technology use, and remote access.
19. **Access changes and supervision.** If I supervise others, I will promptly follow the organization's process when a person's duties change or access is no longer needed. I will not keep access active for convenience.
20. **Separation from the organization.** When my employment, contract, training, volunteer role, or other relationship ends, I will return all equipment, keys, badges, records, software, and confidential information. I will delete organizational information from approved personal devices as directed and will not retain copies.
21. **Continuing obligation.** My duty not to use or disclose confidential information continues after my relationship with the organization ends.
22. **Protected employment rights.** Nothing in this agreement is intended to prohibit lawful discussion of wages, hours, working conditions, or other activity protected by applicable law.

Acknowledgment and signatures

I have received a copy of this agreement, have had an opportunity to ask questions, and understand that compliance is a condition of my access to the organization's confidential information and technology resources.

_____	_____
User signature	Date
_____	_____
Printed name	Employee/contractor ID (if applicable)
_____	_____
Manager or witness	Date
_____	_____
Organization representative	Date

Suggested review cycle: Review this agreement at onboarding, when systems or policies materially change, and periodically with legal, compliance, privacy, and human-resources advisors.