Huron Perth Healthcare Alliance		
HPHA Operations	Original Issue Date:	March 01, 2004
Acceptable Use of HPHA Computers/Electronic Resources	Review/Effective Date:	September 22, 2023
Approved By: President & CEO	Next Review Date:	September 22, 2025

This is a CONTROLLED document for internal use only.
Any documents appearing in paper form are not controlled and should be checked against the document (titled as above) on the file server prior to use.

Purpose

This policy outlines the requirements for acceptable usage of Huron Perth Healthcare Alliance's, hereafter "HPHA", information assets by staff, physicians, volunteers, and third parties, hereafter "Users" and ensures the appropriate use of HPHA information systems in a manner that:

- Protects HPHA from possible cyber events that could lead to privacy risks or loss of information;
- Identifies expectations regarding the appropriate use of HPHA information systems.

The requirements in this policy have been put in place to protect the privacy and security of HPHA information. Only authorized Users can access this information in accordance with legislative and regulatory requirements, their job function and contractual agreements.

HPHA's "Acceptable Use of HPHA Computers/Electronic Resources" policy requires that all Users are required to read the policy carefully, and understand and abide by all requirements. No User account is enabled until the User agrees to the requirements within this policy. Users are expected to sign off on this policy upon commencement of employment with HPHA.

The User will accept full responsibility for any unauthorized use, misuse or illegal use of any HPHA information systems and associated information.

Scope

This policy applies to all Users who access the information systems of HPHA. Information systems shall be understood to include electronic platforms that contain both administrative/corporate, employee, and Personal Health Information (PHI). This includes, but is not limited to, Meditech, PatientKeeper, PACS, Email, Microsoft Teams, Internet, Intranet, network file shares, departmental-specific software, corporately owned cell phones/smart phones, tablets, printers and files residing on individual devices.

Policy

Use of HPHA's computer/electronic resources is a privilege. HPHA Information Technology resources and information systems shall be used for legitimate HPHA patient care and corporate purposes only. HPHA Information Technology resources and information systems must be protected and managed to maintain their integrity and confidentiality, and to prevent their unauthorized disclosure, modification or destruction.

Principles

General use and ownership

- Users should be aware that the data they create on the systems remains the property of HPHA.
- When deemed appropriate, HPHA will have access to any information Users have stored on or transmitted over any network or device belonging to HPHA.
- HPHA reserves the right to audit or review systems on a periodic basis to ensure compliance with this and all other policies.
- HPHA may prohibit access to and/or consider taking disciplinary action if it is determined that any use of HPHA information systems was inappropriate.

Exercising due care towards HPHA patient and corporate information

Users are entrusted with various forms of sensitive information, including but not limited to PHI, confidential corporate data and other systems to interact with this information. HPHA users will accept responsibility to ensure that due diligence is taken to avoid exposure of sensitive information and/or damage to the systems and reputation of HPHA.

Secure access and information handling

- All computing devices must be secured with a password-protected timeout that starts automatically after 30 minutes or less. Timeouts on computing devices will be managed by the HPHA IT Department. Exceptions to devices time-out duration may apply with approval from IT Director.
- Computer sessions must be locked or have the account logged off when the device is unattended. Should users encounter difficulties in locking or logging off of devices, they will contact the HPHA IT Department for assistance.
- All computing device passwords must conform to the requirements as set by the HPHA IT Department.
- HPHA issued computers have been configured with software and features which increase the security of the data accessed and stored using HPHA computers
- When using and exchanging all information, all Users are responsible for ensuring that information is not inappropriately accessed, modified or destroyed.

Corporate email usage

Users will their corporate email primarily for work-related purposes and must use extreme caution when opening e-mail and email attachments received from unknown senders as these may contain malware that could lead to significant damage to HPHA information systems.

For further requirements regarding HPHA email usage and using email to transmit Personal Health Information, see the following policies:

- HPHA policy - Email Management
- HPHA policy – Using Email to Send Personal Health/Patient Information

Microsoft Teams Usage

HPHA utilizes Microsoft Teams as an Instant Message (IM) communication tool for staff. Staff must maintain a level of professionalism when sending any message over Teams.

For further requirements regarding HPHA Teams for messaging or to transmit Personal Health Information (PHI), see the following policies:

- Use of Microsoft Teams for Internal Personal Health Information (PHI) Communication
- Hypercare

HPHA User Responsibilities

HPHA Information Technology resources and information systems have been provisioned to facilitate the conduct of HPHA business. Users are responsible for:

- Ensuring all actions performed using their HPHA accounts, whether by the User or not;
- Supporting HPHA's commitment to security and privacy by adhering to the behaviours outlined in this policy.
- Returning all HPHA assets including all computing devices, portable data storage, smartphones and accessories upon end of employment or change in status as a result of changing departments or temporary or long-term leave.
- Ensuring unverified/unauthorized software updates or hardware modifications are not applied to computers.
- Not installing or utilizing unauthorized software on computers. This includes cloud and web-based services when processing or handling HPHA data.
- Ensuring unauthorized devices are not connected to the HPHA network.
- Ensuring Personal Health Information (PHI) and/or confidential corporate data is not left in written form or displayed on computer devices in areas or locations where unauthorized individuals may access it.
- Locking or logging off of computer devices whenever the device is not in use.

Reporting incidents, breaches and risks

All Users, as a HPHA staff member, physician, volunteer, and/or third-party contractor, have an obligation to report security incidents such as theft, loss or security and privacy breaches/suspected breaches, including but not limited to unauthorized disclosure of HPHA proprietary information, and risks at the first reasonable opportunity via HPHA's RL6 Incident Reporting system. IT must be notified immediately by calling 2222 or via Switchboard after hours.

Know your responsibilities

This policy and the documents referenced above serve as high level information sources for HPHA users to review and understand the generally accepted behaviours with respect to acceptable use of HPHA information systems. It is the responsibility of each user to understand how acceptable use applies to their responsibilities and accountabilities.

All Users must complete all mandatory security awareness training.

Expectations when working from home or out of the office

When working offsite, Users will always keep corporate devices in a secure, attended location.

Remote access to HPHA systems is permitted only via approved access mechanisms, e.g. VPN with multi-factor authentication.

In the event of lost or stolen corporate devices, the incident must be reported to the IT Help Desk immediately (519-272-8210 ext. 2222).

Permitted and Prohibited Uses of HPHA Systems

Permitted Uses

- HPHA systems may be accessed for work purposes and limited and reasonable personal use such as personal electronic mail and internet access, provided that the following are ensured:
    - HPHA policies are not violated,
    - No engagement in any activity that contravenes local, provincial, federal or international law, and
    - The User acts in a reasonable and professional manner as determined by their respective leader and the guiding principles of HPHA.
- Any personal usage must not interfere with work duties and responsibilities or conflict with the best interests of HPHA, nor may such use degrade HPHA systems or the HPHA computing environment.
- For security, performance, and maintenance purposes, HPHA systems, data and network traffic will be monitored at any time in accordance with HPHA monitoring practices. If there is a reasonable suspicion that HPHA resources issued to any User have been involved in the commission of (a) an illegal act, or (b) an act that breaches of HPHA policies, HPHA reserves the right to investigate further as needed. The information stored, or transmitted, using HPHA resources is the property of HPHA.

Prohibited uses

It is the responsibility of all Users to exercise common sense when accessing HPHA systems and data. If unsure about something, ask Leader or contact the HPHA IT Department. Examples of prohibited uses include:

- Accessing personal patient file in any format on any information system. Staff wishing to access their own HPHA personal health information must follow the procedure set out in the Patient Access to Personal Health Information policy. Staff wishing to access their own personal health information in other systems must request access from the source institution.
- Accessing or attempting to access PHI or confidential corporate information except through the course of performing the User's role within the organization.
- Using information systems to partake in fraudulent, harassing or obscene behaviours or to publicly embarrass, expose, criticize or solicit support for personal agendas.
- Compromising or attempting to compromise the integrity of the information resources by accessing or attempting access or alteration of system control programs or files.
- Theft or misappropriation of information resources, such as equipment and information.
- Violation of rights protected by copyrights, trade secret, patent or other intellectual property, or similar laws or regulations. This includes but not limited to unauthorized copying and/or distribution of copyrighted materials, and confidential information.
- Transfer of PHI and/or confidential corporate information outside of organizational and/or technical boundaries via an unauthorized system or device (e.g. copying information to a personal computer, unencrypted mobile storage device, or on-line storage service).
- Storage of PHI directly to PC's, laptops, USB drives, CD/DVD's, smartphones, tablets etc. Staff / affiliates who are considering storage of PHI on any computing device (PC's, laptops, USB drives, CD's, smartphones etc.) require express written approval from the HPHA IT Director. Those who are permitted to store PHI for portability must contact the IT Department for application of encryption software/hardware on all computing devices.
- Communication of PHI outside of HPHA authorized systems. All PHI should be communicated through clinical documentation on approved hospital systems.
- Communication of PHI via email which is susceptible to breaches of confidentiality.
- Using HPHA systems and resources for cryptocurrency mining.
- Processing HPHA information with unauthorized applications, systems or services.
- Sharing HPHA access credentials, e.g. passwords or access tokens.
- Installation of unauthorized applications on HPHA devices.
- Circumvention of HPHA security controls, (e.g. disabling encryption, anti-virus protection, bypassing computer policies, using proxies).
- Using personal Cloud services (e.g. Apple's iCloud, Google's Cloud) or web-based e-mail services (e.g. Gmail, Hotmail) to store any HPHA business information.
- Engaging in any on-line posting that may harm or tarnish the image and reputation of HPHA and/or any of its users.
- Using information resources to access inappropriate electronic content dealing with what would generally be considered to be distasteful or inappropriate material.

Policy Compliance

Compliance Measurement

This Policy supports HPHA's objectives of operating a safe and secure work environment for HPHA employees and physicians, information, and systems. Compliance with this policy is mandatory for all HPHA employees and third-party contractors.

The Information Security team will verify compliance to this standard through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits and feedback to the policy owner.

Exceptions

Any exceptions to the policy must be approved by the Director IT or delegate in advance. If a User is unable to comply with any of the requirements of this policy, a temporary exemption may be requested. Exemption requests must be sponsored by the respective Leader and include the specific policy item for which an exception is being requested, along with a rationale and plan for achieving future compliance.

Requests can be created using the IT service desk.

Non-compliance

A User who has been found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.