AR0100 – ACCEPTABLE USE OF DIGITAL INFORMATION SYSTEMS

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

To set standards for the use and management of Interior Health's Digital Information Systems and electronic information.

2.0 DEFINITIONS

TERM	DEFINITION
Confidential Information	*In this policy, Confidential Information refers to:* *a) Any electronic information that identifies an individual or that can be combined with other information to identify an individual. This definition applies to anyone, living or dead, and includes information like patient/client address, telephone number and health card number personal health number (PHN).* *b) Any electronic corporate information which has not been authorized for disclosure.*
Digital Information System	*The software, hardware and telecommunications networks used to enable communication and collaborative work; to collect, send or store data. Includes all computers or electronic devices used by Interior Health to collect, store or send information. This includes, but is not limited to, workstations and laptops, tablets, smart phones, cellular telephones, fax machines and printers.*

This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.

User	*Includes all staff, physicians, independent contractors, students, volunteers, and any other persons acting on behalf of Interior Health.*

3.0 POLICY

3.1 Use of Digital Information Systems

Interior Health Digital Information Systems are provided exclusively for conducting Interior Health business.

All Users have a legal and ethical duty to protect the confidentiality, integrity and availability of all electronic information.

Digital information systems usage must be able to survive public scrutiny and/or disclosure.

Personal use of Interior Health provided mobile devices, such as cellular phones, is acceptable when used in accordance with AR0150 Mobile Device Personal Use policy.

Users must:

- Follow all applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.
- Take reasonable steps to ensure that they do not cause offence to others.
- Ensure that they do not use excessive amounts of Digital Health resources.

Users must not:

- Use Digital Information Systems for any activity that could expose Interior Health, themselves, or colleagues to potential criminal or other legal proceedings. Examples of inappropriate uses are found in Appendix A.
- Use Digital Information Systems in any way that could adversely affect the reputation of Interior Health.
- Attempt to access Digital Information Systems and/or data to which they are not authorized.

- Change the system or data configuration of any Digital Information Systems in a way that could affect system integrity, unless authorized by the proper Director of Digital Health.

3.2 Personal Use

Although the Digital Information Systems are provided to the User for the purpose of business functions, a limited amount of personal use is allowed, on the following understanding:

- Any device included in the definition of Digital Information Systems, and everything it contains including but not limited to data files and email, are the property of Interior Health and subject to compliance audits and Freedom of Information – Access to Information Requests.
- Personal use of Interior Health provided mobile devices, such as cellular phones, is acceptable when used in accordance with AR0150 Mobile Device Personal Use policy.
- Personal use will not:
  - interfere with work productivity
  - disrupt the system and/or harm the reputation of Interior Health
  - violate this or any other Interior Health agreement / policy
  - involve any personal business activities

3.3 Compliance

Failure to follow acceptable use standards may lead to termination of access, employment and/or contract, withdrawal of privileges per Medical Staff Bylaws, and/or professional sanctions.

4.0 PROCEDURES

4.1 All Users will:

- Read and accept the proper data access and confidentiality acknowledgement before being granted access to the Interior Health information system.

4.2 Manager/ Chief of Staff will:

- Agree to this policy on an annual basis
- Decide the levels of access required by their staff and review existing levels of access periodically.

- For physicians, ensure proper access and confidentiality form has been completed by physicians and kept by the respective Medical Administration office.
- Follow-up on compliance audits in consultation with Human Resources and/or Executive Medical Directors and act when needed.

4.3 Digital Health will:

- Conduct regular audits to ensure compliance.

5.0 REFERENCES

1. AR0400 Privacy & Management of Confidential Information
2. AR0500 E-mail
3. AR0600 Internet Access
4. AR1000 Photography, Videotaping, Audio-Recording
5. AR0150 Mobile Device Personal Use
6. AC0500 Social Media
7. Social Media Guidelines
8. AU0100 Standards of Conduct
9. Medical Staff Bylaws

APPENDIX A – Examples of Inappropriate Use of Digital Information Systems

1. Examples of how Users might expose Interior Health, themselves or colleagues to potential criminal or other legal proceedings include:
   - Downloading, installing, copying, or using unlicensed software.
   - Sending defamatory messages to another person.
   - Disclosure of patient or Confidential Information to an online third-party document storage web site ("in-the-Cloud").
   - Accessing, processing, or distributing material of a pornographic nature.

2. Examples of unauthorized access to data include:
   - Accessing the records of patients who are not under the User's direct care. Accessing the User's own medical record

3. Examples of how offence may be caused using computing facilities are:
   - Sending email messages that are not of a professional nature.
   - Receiving, storing or distributing inappropriate material.

4. Examples of how the integrity of the system could be affected are by:
    - Connecting a personal networking device, such as a wireless router, to the IH network.
    - Installing non-Interior Health approved software or screensavers with the exception of applications being installed on corporate issued mobile phones as per the Mobile Device Personal Use policy.
    - Exposing the system or data to viruses by using non-IHA approved media (i.e., personal or unencrypted USB or portable hard drives) or opening unknown email attachments.
    - Entering your IH network credentials (User-ID and password) in non-IH approved websites (i.e., phishing websites).
    - Changing the configuration of any system unless specifically authorized.
    - Storing data in systems that are not backed up.

5. Examples of inappropriate use of system resources are:
    - Storing duplicate or unnecessary amounts of personal data (photo images, movies, music files) on Interior Health Authority information systems, with the exception of data being stored on corporate issued mobile phones as per the Mobile Device Personal Use Policy
    - Using bandwidth intensive applications such as Internet radio, continuous video streaming (e.g. sporting events, world events, Netflix), and peer to peer (P2P) file sharing on the corporate network.

6. Examples of how Interior Health's Digital Information Systems may be put at risk are by:
    - Compromising the integrity of the data.
    - Not applying proper access control to the data, such as using a weak password and not following the IH Password Policy.
    - Not taking reasonable care to secure assets whilst in transit. For example,
        - when using a portable device, i.e., laptop or handheld
        - when sending e-mail
        - when using the internet.
    - Not ensuring that the proper media handling procedures are in place.
    - Sharing passwords.