

10 Fair Information Privacy Principles

(for Enhance Ontario in its role as a Health Information Network Provider)

1. Accountability

EO is responsible for ensuring PHI entrusted to its systems is protected.

EO designates a **Chief Privacy Officer (CPO)** and a **Information Security Officer (CISO)** to oversee privacy and security compliance, training, and safeguards.

2. Identifying Purposes

EO identifies and communicates the purposes for which PHI is handled—specifically, to enable secure electronic sharing of PHI on behalf of Health Information Custodians (HICs). EO does **not** collect PHI for its own operational purposes.

3. Consent

EO supports HICs' consent practices by ensuring that its systems enable PHI handling strictly in accordance with the HICs' legal authority and patient consent rules under PHIPA.

4. Limiting Collection

EO limits any access to PHI to what is necessary to operate and support network services (e.g., troubleshooting, security monitoring). No unnecessary collection occurs.

5. Limiting Use, Disclosure, and Retention

EO uses or discloses PHI only for providing its network services and retains information only for as long as necessary for those purposes.

As required by HINP regulations, EO supports controlled access, audit logs, and transparency requirements.

6. Accuracy

EO ensures systems maintain PHI in a manner that supports accuracy, completeness, and reliability for the HICs that rely on the network.

7. Safeguards

EO implements administrative, technical, and physical safeguards including:

- Mandatory training
- Access controls and monitoring
- Confidentiality agreements
- Secure system design and audit log availability

8. Openness / Transparency

EO maintains public-facing HINP notices and plain-language descriptions of services, safeguards, and policies, as required under PHIPA O.Reg 329/04.

This includes making policies available where doing so does not reveal confidential or proprietary information.

9. Individual Access

While HICs are responsible for providing individuals access to their PHI, EO supports this by ensuring transparent logging, secure system design, and audit trails that can be made available to HICs upon request.

10. Challenging Compliance

EO ensures individuals or HICs can challenge EO's compliance through a formal process managed by the **CPO** and provides contact mechanisms for complaints.

Escalation routes include the **Information and Privacy Commissioner of Ontario (IPC)**.