Central Patient Attachment Registry (CPAR) Quick Reference:

Summary of the Key Privacy and Security Information

CPAR

CPAR is a provincial database that captures the attachment of General Practitioners (GP) and Nurse Practitioners (NP) to their paneled patients. The information collected, used and disclosed in CPAR includes patients' health information and providers' and other users' personal information. CPAR is a joint initiative between the Alberta Medical Association (AMA), Alberta Health (AH) and Alberta Health Services (AHS).

The following summarizes the safeguards and protections, as well as the access requirements for CPAR as described in the Alberta Health CPAR Privacy Impact assessment (PIA).

Health Information Act (HIA)

CPAR is governed by the HIA for the collection, use, and disclosure of health information. Policies and security protections that follow best practices and industry standards have been developed to ensure safety and confidentiality of the information contained within CPAR. Fines are in place where an individual knowingly collects, uses, discloses or creates health information in contravention of the HIA. Under HIA, a GP and NP are considered custodians.

PIA

Under the HIA, custodians must submit a PIA to the Office of the Information and Privacy Commissioner (OIPC) prior to implementing or making changes to administrative practices and information systems relating to the collection, use or disclosure of individually identifying health information. AH has submitted a PIA to the OIPC for CPAR.

As a custodian, a GP or NP would only need to submit a PIA if they are implementing a new practice or system, or making a change to that practice or information system. If the GP or NP are simply uploading existing panels to CPAR there is no PIA obligation with the implementation of CPAR.

Security Risk Assessment

A Security Threat Risk Assessment (STRA) has been completed on CPAR to ensure appropriate information security protections are in place. For example: all file transfers across networks are encrypted; CPAR is housed and maintained in a secure environment; business continuity plans are in place and are continually updated; and there is a risk assessment framework in place to identify security threats and vulnerabilities and assess potential impacts.

Incident Response

The primary care provider and their affiliates are required to report to AH, any incidents that affect the security, confidentiality or availability of information in CPAR or CPAR infrastructure. The process that must be followed when reporting a CPAR incident is the Provincial Reportable Incident Response Process (PRIRP).

Responsibilities for Health Information

AH is responsible for CPAR. As a custodian under the HIA, and as public body under the *Freedom of Information and Protection of Privacy Act* (FOIP Act), AH exercises custody and control over the health and personal information in the registry.

As custodians, GPs or NPs are responsible to collect, use, disclose and protect health information within their custody and control in accordance with provisions set out in the HIA. GPs and NPs have a duty to identify their affiliates (e.g. employees, Information Managers, and individuals who provide services for them) and take steps to ensure they comply with the HIA and the custodian's policies and procedures.

An affiliate's collection, use or disclosure of health information is considered the same as collection, use or disclosure by the custodian. The custodians' policies and procedures must reflect their College's Standards of practice, and HIA requirements regarding health information management and protection. Custodians must ensure that the organizational management within their practice addresses overall management of privacy functions.

Access and Correction Requests

AH exercises custody and control over the health and personal information in CPAR and will respond to access and correction requests for the registry.

Primary care providers do not exercise custody and control over the health and personal information in CPAR. If providers have printed or saved reports from CPAR and stored them in their own clinical records, they need to consider these records as potentially responsive in any individual health information access, or correction request and process according to their own organizational policies.

Providers participating in CPAR will be made aware of Alberta Health's responsibility for responding to access and correction requests and their own responsibility with regards to any records they print or store from CPAR.

Training

AH provides training and awareness materials to primary care providers regarding access to CPAR. Pursuant to section 8(6) of the *Health Information Regulation*, GPs and NPs, in their role as custodians, are expected to implement HIA training to ensure their affiliates are aware of and adhere to all administrative, technical and physical safeguards in respect to health information. This includes ensuring that their affiliates comply with HIA and regulations, as well as with their policies and procedures for their practice.

Notice, Consent and Expressed Wishes

CPAR does not collect health information directly from patients, and does not rely on patients' consent as an authority to collect, use or disclose health information.

Primary providers collect health information from their patients as part of regular treatment and care. The primary providers are responsible for providing appropriate collection notice pursuant to HIA section 22(3) at that time.

Providers may opt-out of CPAR. If they opt-in providers must consider and respond to an expressed wish from a patient, under section 58(2) of the HIA to limit disclosure of their health information. Providers should consider and respond to expressed wishes according to their own HIA policies. Providers who receive an expressed wish from a patient can opt-the-patient out of CPAR.

Panel Conflicts

A panel conflict occurs when a patient is attached to more than one primary provider. Primary providers and their staff should communicate with patients to resolve panel conflicts.

Access

CPAR access is role based. Users are permitted to access functionality and administer panels and rosters based on their assigned role. Access permissions and other security credentials are set up so that users have information on a "need-to-know" basis. Permission levels are established at the time of user account creation, and are verified periodically to ensure that the access is still appropriate for the user's role. Providers and panel/program administrators can only access their own panels and program rosters.

Access to CPAR is provided through secure networks or securely over the internet using two-factor authentication. Two-factor authentication involves a password and ID to be used in conjunction with an authentication device (SecureID remote access fob). Both must be present for the individual to gain access.

All users must agree to terms and conditions before accessing CPAR. The user must acknowledge that they have read, understood and agree to be legally bound by and comply with these Terms of Use and any terms, conditions, legal notices and disclaimers in the footers, content, other pages of the registry.

GP and NP offices must establish a CPAR Access Administrator. A CPAR Access Administrator could be a provider at the site, or an affiliate of that provider. Once a site's CPAR Access Administrator is set up, that person may provision other CPAR users. While the user provisioning process is delegated to a CPAR Access Administrators, this process is supervised by providers, who are ultimately accountable for their affiliates' use of CPAR.

Audit

CPAR auditing adheres to the Provincial Logging and Auditing Standard (PLAS) and section 6 of the Alberta Electronic Health Record Regulation. CPAR logs allow for user reporting and auditing. Audit logs are reviewed on a regular basis and any inappropriate activity will be reported to AH Privacy and Security.