Policy & Procedure # 9

COPP PROVINCIAL ADVISORY COMMITTEE

Policies and Procedures
Subject: Information Security
Date: November 22, 2013
Amendment: February 25, 2017

According to the Personal Information Protection and Electronic Documentations Act (PIPEDA) personal information is information about an identifiable individual. Examples include:

- the individual's name,
- the individual's home address, or home telephone, facsimile or e-mail number,
- information about the individual's age, sex, sexual orientation, marital or family status,
- information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,
- information about the individual's religion or creed, or religious belief, association or activity,
- personal health information about the individual,
- the individual's blood type, fingerprints or other hereditary characteristics,
- information about the individual's political belief, association or activity,
- information about the individual's education, employment or occupation, or educational, employment or occupational history,
- information about the individual's source of income or financial circumstances, activities or history,
- information about the individual's criminal history, including regulatory offences,
- the individual's own personal views or opinions, except if they are about another person,
- the views or opinions expressed about the individual by another person, and

- an identifying number, symbol or other particular assigned to the individual.

Manitoba Public Insurance's (MPI) Information Security Directive provides direction for the protection of information from accidental or intentional disclosure, destruction, or modification, as well as protecting individuals from inadvertently placing themselves in positions of potential conflict or risk.

The Directive applies to information stored or transmitted in electronic and all other forms, including verbally and representation of the information on paper, film, or other types of media including email and Internet content.

COPP members must ensure that information, including personal information defined by PIPEDA, related to their COPP group, the group's activities, and its members is properly handled.

COPP members, as Persons Associated with Manitoba Public Insurance assume the following responsibilities:

1. COPP groups issued electronic devices by MPI should know the whereabouts of them at all times and are responsible for securing them against misuse, loss, or theft. In the event that a loss or theft occurs; it is to be reported to the COPP Provincial Coordinator as soon as possible.

2. COPP members shall exercise care and caution when printing, copying, sharing, storing or disposing of personal or sensitive information related to their members/group, COPP activities or partner organizations/agencies.

COPP members are expected to follow these best practices for collecting, storage and destruction of personal information:

- Collect only personal information that is the absolute minimum necessary to conduct the business of your group and only use it for COPP purposes.
- Personal information gathered while conducting COPP business such as patrolling, meeting, etc must only be shared with authorized individuals for the purposes of conducting COPP business. In addition, personal

information of COPP members must only be shared with authorized individuals with that person's permission.

- Passwords are not to be shared with unauthorized persons.
- Sensitive and personal information must not be discussed in public places or when on the telephone which could be overheard by an unauthorized person.
- Sensitive and personal information must not be left on answering machines, facsimiles, or voicemail systems that may be accessed by unauthorized persons
- Store documentation containing personal information, including shift notes, meeting minutes, group membership lists, videos, photos etc in a locked physical location and/or password protected electronic file that is only accessible by authorized COPP members or law enforcement partners.
- Personal information must be destroyed securely, by means such as shredding or file deletion. Secure disposal of information can be facilitated by a local police agency, municipal office, MPI Service Centre or the COPP Provincial Coordinator.
- Patrol notes of past members are to be collected and provided to the local law enforcement agency or the Provincial Coordinator.

If a complaint is received related to improper collection, use, disclosure, storage or disposal of sensitive or personal information the following procedure will be followed:

1. The group will immediately notify their Regional Representative or the Provincial Coordinator.
2. The MB COPP Chairperson will appoint a person to gather the information (the Investigator).
3. The Investigator will consult the MB COPP lawyer for guidance and will gather information from the complainant, defendant and other sources.
4. The Investigator will assess whether there has been a breach of:
    a. The Volunteer Letter of Agreement
    b. This policy
5. The Investigator will provide a recommendation to the board for a final decision.