

Physician's Office Security

Sadly year after year the crime rate remains high and the bulk of crimes are committed against property.

Physicians offices have become a prime theft target. Many modern offices now contain highly attractive contents such as PCs, laser printers, faxes, prescription pads and drugs.

Furthermore, there is an ever increasing public awareness with the introduction of Privacy Legislation over the security of personal and confidential records. Physicians have a responsibility to ensure an adequate level of security of such records whether they be on paper or computer.

The following summary of guidelines and good practice should help to secure your office against unauthorized entry both during and out of business hours.

Risk Assessment

As a first step a Risk Assessment should be carried out to:

- i) Assess the impact and effect on the business in the event of the loss of a computer, drugs, medical equipment or records.
- ii) Carry out a survey of the premises including the surroundings in order to identify potential risks and vulnerable areas.
- iii) Develop an integrated plan taking account of potential risks and costs and establish a security system design criteria.

Layered Security Plan

The design criteria should be used to provide a basis for a layered security plan of security barriers forming a gradual filter for authorized access during business hours and a physical barrier 'buying time' for unauthorized access out of business hours.

(i) Building Security

The office should be located in buildings of standard construction such as brick or reinforced concrete offering substantial resistance against physical attack. If space permits a perimeter security fence and gates has proved to be a most effective first level of defence in urban areas.

All exit doors should be of substantial construction and adequately secured with panic hardware or single cylinder deadlock.

All accessible glazing should be protected against unauthorized entry (e.g., grills or roller shutters and the provision of blinds to prevent visibility of attractive contents from outside).

(ii) Intruder Alarm

Consideration should be given to the fitting of an intruder alarm. The emphasis should be on providing early detection, preferably on the building perimeter such as doors and glazing before access to the target/sensitive contents is gained. Having an effective method of remote signalling to an alarm receiving centre who will contact key holders and the police is also advisable.

(iii) Access Control

A security system should be adopted which will allow access to vulnerable areas only to those persons having appropriate authorization. The method used can vary from a simple lock and key or combination lock through to a high security electronic access control system.

(iv) Security of Target/Sensitive Contents

Although the above measures should deter unauthorized persons from entering, the more attractive sensitive contents need a further degree of protection.

Computers

- Up to date inventory.
- Prominently marked.
- Located in well observed and preferably access controlled areas.
- Fitted with security enclosures to help prevent removal including the memory chip.

Drugs

- Up to date records of stocks and dispensing.
- Doctors bags kept with the person or in a locked secure room.
- All habit forming and addictive drugs (not just controlled drugs) should be;
 - secured in locked cabinets
 - cabinets should be fixed to the building structure
 - kept in a locked room with controlled access
- Ensure fridges which contain such drugs are lockable and located in an access controlled area.

Records

- Paper to be kept in a well observed area with controlled access. Out of business hours, this should have some degree of physical security and fire protection, (e.g., in a lockable fire proof cabinet providing at least one hour's fire resistance).
- All computer terminals and PC's with access to data with any degree of confidentiality should incorporate either or both a mechanical lock and password before access is allowed.
- Institute a clear desk policy.

Data back up procedures should include:

- Systematic and regular backing up of data.
- Regular testing/verification of backed up data.
- Remote off-site storage of back up copies.

Contingency Planning

- A written pre-planned contingency and action plan should be prepared detailing the procedures to be taken in the event of an incident.
- The plan should be periodically reviewed and tested.

Key Action Steps

- Carry out risk assessment and develop an integrated plan of potential risks and costs.
- Produce and implement a layered security plan considering the following:
 - Physical perimeter security
 - Fitting of an intruder alarm
 - Access control
 - Protection of target/sensitive contents
- Prepare a pre-planned contingency and action plan.
- Review, test and update procedures as required.

Useful Contacts

Canadian Alarm and Security Association
National Office
610 Alden Road Suite 100
Markham ON L3R 9Z1
(905) 513-0622
Toll Free 1-800-538-9919

References

Personal Information Protection and Electronic Documents Act
The Privacy Act
Additional detail on these acts may be obtained at:
Info@privcom.gc.ca