



Mental Health Services

# Information Security

---

15 May 2009

Geoff Dembo

Mental Health Information  
Systems Analyst

---

# Why worry ?



**“The boss is worried about information security,  
so he sends his messages one alphabet letter  
at a time in random sequence.”**

# Why worry ?

- Lost information
- Inappropriately changed information
- Information accessible by the wrong people

# Why worry ?

- Lost information
  - Inappropriately changed information
  - Information accessible by the wrong people
- ... can lead to ...

# Why worry ?

- compromised care
- distress or other harm to client by information in wrong hands
- loss of confidence in agency by client
- bad publicity for agency, eg newspaper stories
- failing audit
- possible referral to the Privacy Commission

# Privacy Commissioner



“The Privacy Commissioner's Office works to develop and promote a culture in which personal information is protected and respected.”

# Privacy Commissioner

- Privacy Act 1993
- Health Information Privacy Code 1993 (HIPC)
  - Rule 5: Storage and security of health information

# Privacy Commissioner

## Rule 5: Storage and security of health information

- (1) A health agency that holds health information must ensure that -
  - (a) the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:
    - (i) loss; or
    - (ii) access, use, modification, or disclosure, except with the authority of the agency; or
    - (iii) other misuse; and
  - (b) if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and
  - (c) where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.
- (2) This rule applies to health information obtained before or after commencement of this code.

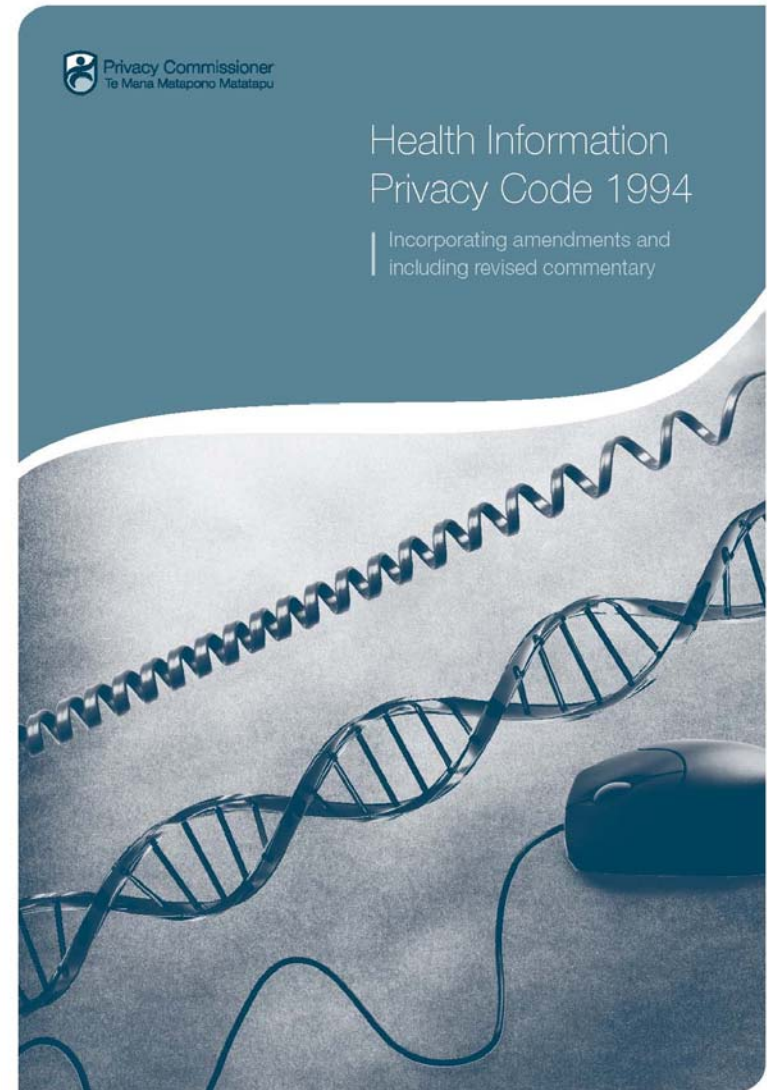
# What are our responsibilities?

- Not looking for military or SIS-level security



# What are our responsibilities?

- Not looking for military or SIS-level security
- Have a look through the commentary on Rule 5 in the Health Information Privacy Code 1994 (available from [www.privacy.org.nz](http://www.privacy.org.nz))



# What are our responsibilities?

- Not looking for military or SIS-level security
- Have a look through the commentary on Rule 5 in the Health Information Privacy Code 1994 (available from [www.privacy.org.nz](http://www.privacy.org.nz))
- Put together a plan, and discuss it with your staff

# Risks and practical steps

- Computer / electronic
- Paper and other

# Risks and practical steps

## Lost information:

- Loss of equipment - eg theft/mislaying of computer or portable storage device
- Hardware failure - eg hard disk crash
- Software fault - program does something unexpected
- Malware - computer virus/worm etc
- Operator mistake - accidental deletion/overwriting
- Business process problem - eg information not kept long enough

# Risks and practical steps

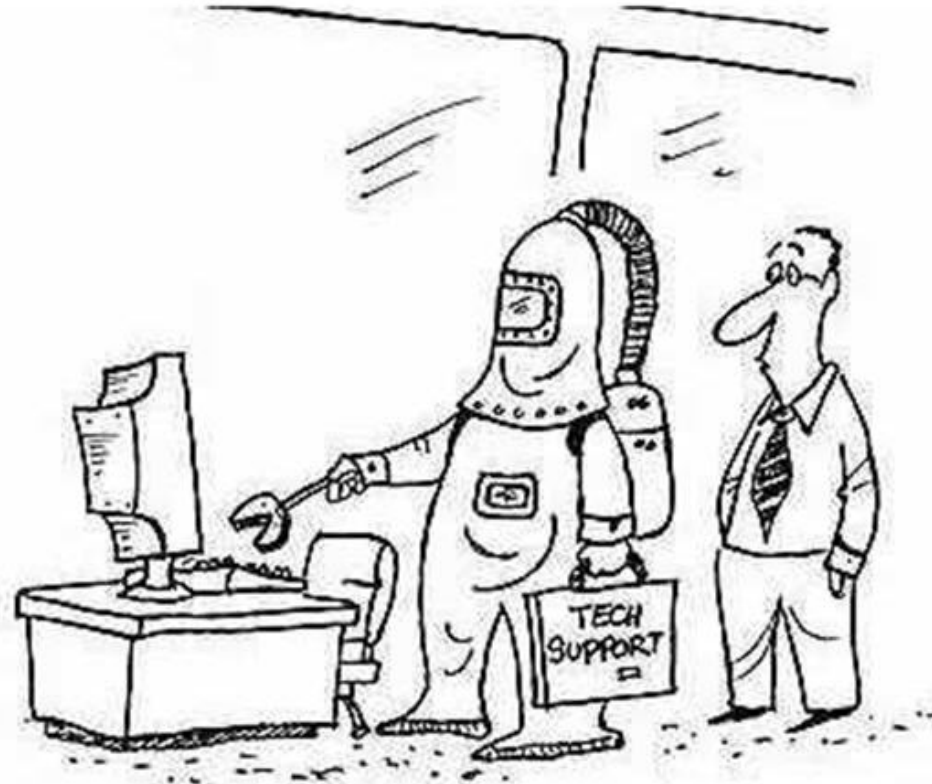
## Do backups



**“We back up our data on sticky notes because sticky notes never crash.”**

# Risks and practical steps

Keep malware out



"THE VIRUS IS THAT BAD, HUH?"

# Risks and practical steps

## **Inappropriate access/use/modification/disclosure:**

- Information accessed by staff member who has no right to be involved
- Information accessible by members of the public, eg unattended computer displaying client information or computer screen visible from street
- Information on lost/stolen/discarded equipment, eg lost USB flash drive or dumped computer
- Information sent by insecure means, eg ordinary email, or stored in inappropriate place, eg on home family computer
- Information shared with other agencies inappropriately

# Risks and practical steps

## Control access



"What do you mean Rumpelstiltskin is too long for a password?!"

# Risks and practical steps

Keep an eye on portable storage devices



# Risks and practical steps

Erase information from discarded equipment



# Risks and practical steps

## **Educate staff:**

- Make sure staff understand the importance of keeping information secure
- Train on doing backups

# Risks and practical steps

## **Educate staff:**

- Make sure staff understand the importance of keeping information secure
- Train on doing backups

## **Plan:**

- Audit what information you hold, and where.
- Have a plan for promoting information security and responding to breaches