Privacy Commissioner
Te Mana Matapono Matatapu

HEALTH

ON THE ROAD

How to keep health information safe while working in the community

May 2017

Protecting health information off-site

The healthcare sector is increasingly providing community-based health services. This guide aims to help you keep health information secure while you are off-site or on the road.

What is your responsibility?

Rule 5 of the Health Information Privacy Code requires health agencies to keep health information safe. The focus of rule 5 is whether a health agency has taken reasonable steps to keep information safe.

When deciding what steps are *reasonable*, you should consider:

- the sensitivity of the health information
- how a security measure will impact on your ability to carry out your functions, and
- the likely consequences if the health information is lost or stolen.

Health agencies are responsible for developing a security policy and making sure their employees know about it.

Agencies should do everything they reasonably can to protect the health information they have and make it difficult for someone to misuse it. This means designing security systems and policies in anticipation that theft or break-ins may occur.

Key Tips

Before you go

When you travel off-site, only take the information you need to complete your work. Whenever you take any health information off-site, you're exposing it to more risk than if you'd left it in the office, hospital or clinic.

On the go

We often hear of bags or laptops stolen from cars. Check:

- Is this health information something you should be leaving in your car?
- If you have to leave health information in your car, can you put it out of sight, for instance, in a locked glovebox or in the boot?

To ensure information is not lost or left behind in transit, eg in taxis, public transport or other vehicles, consider:

- Have you taken steps to remind yourself to take the health information with you when you stop on your journey?

Once you get there

How will you secure the health information once you've reached your destination? If you're taking the information to another health agency or facility, that may be relatively easy to do.

Community care workers sometimes need to take health information home with them. For instance, you may store information on a USB flash drive, or you may have clinical images stored on a personal mobile device. Devices like these are easy to transport and are also easy to accidentally misplace.

If your agency or employer allows you to take health information home, you should discuss with your agency or employer what additional security measures can be put in place to help you.

- Some workers may have access to a password-protected lockable mobile device, or even a lockable file box.
- Health information might be made available to you in a different way, for instance, by setting up remote access to your work computer.

If your agency or employer doesn't have a security policy for health information stored offsite, you should raise that with them so they can develop one.

Security for electronic information

You may have a choice between taking physical documents off-site or operating off-site with an electronic device such as a laptop, smartphone, notepad or external hard drive.

Unless your agency or employer has a policy that specifically permits the use of personal devices, you should not use a personal device to access health information.[1] The security you use on your device needs to be at least as good as the security you use at work:

Secure the device - set a strong password, passcode or pattern lock on the device. Is the security software up to date? Are there firewalls and current antivirus software in place and up to date?

Secure health information on the device - find out if you can use password protection on certain documents or if you can encrypt the information.

Why does this matter?

Keeping information secure is an essential step in maintaining the trust of patients and clients. There can be direct consequences for the person or people whose information is lost, and for your agency or employer.

Further, if you fail to take appropriate steps to keep health information secure while you're off-site, you could face disciplinary action, by your employer and/or

[1] See: HISO 10029:2015 17.2

through a professional standards body. There may be consequences for your professional registration. Your agency or employer could face reputational damage, or someone could make a complaint to the Privacy Commissioner.

What if something does go wrong?

It's important to be upfront if something goes wrong. Most agencies and employers accept that mistakes can happen and would prefer that staff let them know so that shortcomings can be addressed appropriately. Similarly, most patients will be more likely to be understanding and willing to listen if you've made efforts to address the problem quickly and transparently.

If you find yourself dealing with a situation where health information has been stolen or lost, there are four key steps to take:

1. **Containment** - prevent the situation from worsening
2. **Evaluation** - evaluate the potential harm that may be caused
3. **Notification** - decide whether the seriousness of the situation requires you to notify people who may be affected, and
4. **Prevention** - learn the lessons and reduce the chances of a repeat.

For more information, see our **Data Safety Toolkit.**

Checklist

- Do I need everything I'm planning to take? (If not, leave it behind!)
- What are my safest choices in accessing the health information on a job?
- What can I do to make sure the health information I take off-site is safe and secure (to prevent accidental loss or theft)?
- Is there anything else I can do to make sure the health information remains safe while I am off-site?
- When I get to my destination, how will I store the health information safely?
- Do I know what to do if something goes wrong?

Contact us

ENQUIRIES	privacy.org.nz/enquiries
WEBSITE	privacy.org.nz
FACEBOOK	PrivacyNZ
TWITTER	@nzprivacy
FAQs	privacy.org.nz/ask

Other resources

New Zealand Medical Association (NZMA), *Clinical images and the use of personal mobile devices,* 2016. See: Clinical images guide from NZMA