ACC

Security Policy for Electronic Business

Version 1.4

Table of Contents

1. Your Responsibilities

Your obligation as a registered user of ACC's electronic services is to treat the access you have been given wisely. In many ways, this is similar to the prudent use of a credit card. Among the principles that you should observe are detailed below:

1.1. Digital Certificates and Digital Certificate Passwords

Your digital keys are delivered on CD and stored on your computer and its backup media. You must protect all copies of these keys and maintain the confidentiality of their passwords. Your password must be difficult to guess and must never be disclosed to anyone. (See ***Password Standards.***)

There are two variants of Digital Certificate available for use in conducting electronic business with ACC:

HealthSecure: This can be used for the electronic lodgement of ACC45 Injury Claim Forms, and ACC40 and ACC47 Billing Schedules. It can also be used to query the status of an ACC claim, schedule or invoice online.

SecureCert: This is used to access ACC's Accredited Employers website.

Note: If you believe your Digital Certificate or its password may have been compromised please advise, as soon as practicable, the New Zealand Health & Disability Sector Registration Authority (NZHSRA) on 0800 117 590 or registrar@nzhsra.co.nz.

1.2. Access User Ids and Passwords

You may be given additional user ids and passwords to access other facilities. Prudent technical controls have been implemented to support the integrity of this access. Your role is to maintain the confidentiality of your access passwords and to follow basic security requirements, such as changing your password when asked.

1.3. System Security

Effective system security relies as much on people as on technology. Use of common sense combined with security standards and practices to protect information assets, is the best assurance your patients can get of their privacy.

1.4. Overall Responsibility for Security of Information Systems

You are responsible for ensuring the physical protection of your systems, including PCs, laptops and other communications devices that may be connected to ACC. This includes the physical security of premises and physical access to hardware. Mobile systems and USB portable storage devices containing patient data are particularly vulnerable to loss or theft and steps should be taken (eg device encryption) to ensure any such loss or theft does not give access to this information.

1.5. Responsibility for use of your access codes, passwords and keys

Remember that you are responsible for any access to the ACC system obtained using your access codes, passwords and keys that belong to you and that are kept on your system(s).

1.6. Responsibility for Security of Information downloaded from ACC

Under the NZ Privacy Act (1993) you are responsible for the security of any personal information downloaded from ACC and stored on your local system. It is recommended that the only sensitive information to be stored on local systems should be that which is necessary for individual patients well being.

1.7. Nominated Security Officer

Your Practice should appoint a 'Nominated Security Officer', who is responsible for security awareness and reviews, and is the contact point for security related issues. All security related issues should be passed to your Nominated Security Officer. The Nominated Security Officer should advise ACC of any security issues, concerning ACC provided data that you may have, which they cannot resolve.

1.8. Information Security Agreement

As part of overall Information Security your Practice staff should sign a non-disclosure information and security agreement that highlights their obligations. This responsibility extends to all staff including any temporary and part time staff.

1.9. Malicious Software (Malware)

Like people, computers are susceptible to catching malicious software (including viruses, worms, and spyware) from external sources. To ensure that malware is not transferred to ACC, it is vital that malware prevention software is installed and active on your computer, and that it is regularly updated. Anti-malware software should identify and isolate any potential viruses, worms, spyware and other harmful software, thus protecting us all. Note, if you've been infected by malware and believe you may have passed it to ACC please phone 0800 222 994.

2. Password Standards (recommended)

Passwords must be:

- Kept confidential to the authorised user and not shared.
- Never written down in a place where others can access the password.
- Routinely changed to maintain their confidentiality eg monthly, quarterly.

Passwords Must NOT be:

- Months of the year, days of the week, date of birth or any other aspect of the date.
- Publicly known family names, initials or car registration numbers.
- Company names, identifiers or references.
- User Identification, user name, group identification or other system identifier.
- Telephone numbers or similar all-number groups.
- More than two consecutive identical characters.
- All-numeric or all-alphabetic groups.
- Any word contained within any dictionary; English or any other language.

For further information see the 'NZ Password Standard' at: http://www.e.govt.nz/standards/e-gif/authentication/password/ for further information.

3. Further Information

While new security risks continue to emerge, ACC will continue to monitor and promptly address these issues to maintain a secure transmission environment consistent with the sensitivity of the data.

For those providers seeking further information regarding information security please refer to the NZ Health Information Security Framework (HISF). The HISF has been designed to support organisations and practitioners holding personally identifiable health information to improve the security of that information, so it can be produced, stored, disposed of and shared in a way that ensures confidentiality, integrity and availability. The HISF specifies the minimum policy standards and technical requirements to best enable organisations to achieve this.

See http://www.nzhis.govt.nz/moh.nsf/indexcm/hisac2-standards-approved-hisf.

Should any conflicting statements between the HISF and this document be found, please advise the ACC eBusiness team.

Other Reference material is as follows:

- NZ Privacy Act (1993), NZ Health Information Privacy Code (1994) and their amendments,
- New Zealand Copyright Act (1994),
- Official Information Act (1982),
- New Zealand Information Security Management Standards (ISO/IEC 27001:2006; 27002:2007 and 27005:2008),
- New Zealand Information Security Manual (NZISM) – See: http://www.gcsb.govt.nz/newsroom/nzism.html
- www.acc.co.nz

ACC eBusiness team - email: eBusinessinfo@acc.co.nz or Phone: 0800 222 994

4. Information Non Disclosure Agreement (example only)

Employees or Contractors of [your organisation's name] have obligations under law to keep information confidential, including the following:

> Every employee or contractor must comply with statutes and regulations that relate to health information. In particular employees and contractors must comply with the following statutes and regulations:
>
> (a) the Privacy Act 1993;
>
> (b) the Health Information Privacy Code (1994);
>
> (c) the Health Act 1956;
>
> (d) the Hospitals Act 1957;
>
> (e) the Official Information Act 1982.

Relevant extracts of these statutes and the Code of Practice are available from your Manager. Management of [your organisation's name] encourages you to be familiar with them.

An employee or contractor must not disclose any personal information or information concerning the health, disabilities, or medical history of any patient, unless the employee or contractor is disclosing the information in a manner authorised by the Code of Practice.

The above rule is contained in the Privacy Act. Any person who breaches the Privacy Act may be subject to investigation by the Privacy Commission, who may refer the matter for proceedings before the Complaints Review Tribunal under the Privacy Act. The Tribunal has the power to award damages of up to $200,000, as well as make relevant declarations and orders, in respect of any successful complaint. The Tribunal may also refer a complaint to the High Court in appropriate circumstances.

As part of his or her employment contract with [your organisation's name], an employee or contractor shall not, at any time (except as may be necessary for the proper performance of the employee's or contractor's duties and responsibilities, or as may be required by law):

- Breach any of the legal requirements described above;
- Disclose to any person, other than to an employee of [your organisation's name] authorised to receive the same, any knowledge or information concerning the business, affairs, property or other activities of [your organisation's name] which has come to the employee's or contractor's knowledge in the course of the their employment;
- Disclose to any person other than authorised employees of [your organisation's name] personal information concerning current, potential or past employees of [your organisation's name]; or
- Use or attempt to use any of the information specified above for the employee's or contractor's own personal benefit, or for the benefit of any other person or organisation, or in any manner whatsoever, other than in accordance with the employee's or contractor's duties and consistent with the obligation of confidentiality expected for a person in the employee's position;

Breaches of any of the above obligations will be considered to be serious misconduct. Please note however, that the above obligations are not intended to prevent free speech or speaking out on matters of professional or ethical concern.

If you have any enquiries about the above requirements, please contact your Manager.

I, ... (Full Name) have read and agree to comply with the above.

....

(Signature) (Date)