



# Health Intranet Connection Procedure

Procedure Number

CHC-PG-0045

Version Nos:

3

## 1. Purpose

This Procedure outlines a process to ensure that the West Coast District Health Board (WCDHB) complies with the security requirements communicated by the NZHIS Health Intranet Security Officer.

## 2. Application

This Procedure is to be followed by all staff members throughout the WCDHB.

## 3. Definitions

For the purposes of this Procedure:

**Authorised Signatory** is taken to mean a WCDHB staff member indicated on the BaycorpID "Organisation Digital Certificate Registration Form" under the heading "List of Organisation Authorised Signatories"

**Health Information Network** is taken to mean the Health Information Network which is a Virtual Private Network (VPN) established by the New Zealand Health Information Service to allow health sector subscribers share information securely.

**VPN** is taken to mean a private network, communicating over public media achieved using encryption technology. A cost-effective method of implementing a private network.

**IPSec** is taken to mean a collection of security protocols, including digital certificates used to transport information over a TCP/IP network securely, addressing the issues of authentication, confidentiality, non-repudiation and integrity.

**Digital Certificates** are taken to mean an electronic "passport" that establishes a user's credentials when interacting on the Health Intranet. A Certificate Authority (CA) issues it. It contains a user's name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signature), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. All digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

**Certificate Authority** is taken to mean a body that allocates certificates to authorised users. The Health Intranet uses BaycorpID Services Ltd to issue certificates.

## 4. Responsibilities

For the purposes of this Procedure:

**All WCDHB staff members** are required to ensure they abide by the requirements of this Procedure.

## 5. Resources Required

This Procedure requires no specific resources.

## 6. Process

1.00 Access to the New Zealand Health Information Service's (NZHIS) Health Intranet is an important part of WCDHB's communications facilities and if properly used can provide an efficient and effective means of communicating externally.



## Health Intranet Connection Procedure

Procedure Number

CHC-PG-0045

Version Nos:

3

- 1.01 It is critical that WCDHB protects information resources and information processed, stored, or transmitted via the Health Intranet.
- 1.02 Sensitive information accessed via the Health Intranet must be safeguarded against unauthorised disclosure, modification, access, use, destruction, or delay in service.
- 1.03 An Authorised Signatory is to authorise the requestor's use of the Health Intranet using the appropriate BaycorpID HealthCert forms.
- 1.04 Users of the WCDHB Information System shall be held responsible for all messages or communications generated from their account and will be responsible for all transactions carried out using their account.
- 1.05 The WCDHB Information Technology Department shall:
  - i) be responsible for the establishment and maintenance of the Health Intranet connection in accordance with this policy and any requirements mandated by the Health Intranet Security Officer. Information Technology will maintain the firewall and IPSec router to ensure security is not compromised;
  - ii) ensure any email that is intended for a subscriber to the Health Intranet be routed via the Health Intranet connection;
  - iii) ensure that any connections made through the Health Intranet to another subscriber must only be established using IPSec, to ensure that data is encrypted using 128bit keys and participants are authenticated;
  - iv) use all implemented automated checking processes to ensure that information transferred to the Health Intranet is virus free, and that information received is also checked.
- 1.06 Telecom will be responsible for establishing and maintaining the connection between the local router and the Health Intranet in accordance with the Health Intranet of New Zealand General Security Policy.

## 7. Precautions And Considerations

- ➔ Users of the WCDHB Information System shall be held responsible for all messages or communications generated
- ➔ The WCDHB Information Technology Department is responsible for the establishment and maintenance of the Health Intranet connection

## 8. References

There are no references associated with this Procedure.

## 9. Related Documents

The Health Intranet of New Zealand General Security Policy



## Health Intranet Connection Procedure

**Procedure Number**  
*CHC-PG-0045*

**Version Nos:**  
**3**

<b>Revision History</b>	<b>Version:</b>	3
	<b>Developed By:</b>	Information Technology Manager
	<b>Authorised By:</b>	Chief Executive Officer
	<b>Date Authorised:</b>	April 2001
	<b>Date Last Reviewed:</b>	January 2007
	<b>Date Of Next Review:</b>	January 2009



**Health Intranet Connection  
Procedure**

**Procedure Number**

*CHC-PG-0045*

**Version Nos:**

**3**

**This Page Is Deliberately Blank**