

**Access, Use and
Disclosure Policy for B4
School Check Information
System Users**

Ministry of Health. 2010. *Access, Use and Disclosure Policy for B4 School Check Information System Users*. Wellington: Ministry of Health.

Published in October 2010 by the
Ministry of Health
PO Box 5013, Wellington 6145, New Zealand

ISBN 978-0-478-36693-8 (online)
HP 5249

This document is available on the Ministry of Health's website:
<http://www.moh.govt.nz>



MANATŪ HAUORA

Contents

Introduction	1
Purpose of the System	2
National level information requirements	2
District Health Boards	2
District system to manage the programme	3
Provider level information requirements	3
Management of Health Information	4
Rule 1 – Purpose of collecting the information	4
Rules 2–4 – Source of information, collection of information from individuals and manner of collection	4
Rule 5 – Storage and security	5
Rule 6 – Access to information	6
Rule 7 – Correction of information	7
Rule 8 – Ensure accuracy of information before use	7
Rule 9 – Retention of information	7
Rules 10 and 11 – Limits on use and disclosure of information	8
Rule 12 – Unique identifiers	8
Complaints and Breaches of Privacy	9
Basic principles of security	9
Security control responsibilities	10
Complaints and Breaches of Security	11
Access to the System	12
Authorised user agreement	12
Access control responsibilities	13
Access Rights by Role	15

Introduction

This is the policy for the management and use of the health information collected as part of the B4 School Check and held on the national B4 School Check information system (the system).

The B4 School Check replaces the School New Entrant check as the eighth core Well Child contact and involves checks of height, weight, hearing, vision, oral health and development and behaviour assessments. Its purpose is to identify and address any health, behavioural, social, or developmental concerns which could affect a child's ability to get the most benefit from school, such as a hearing problem or communication difficulty.

Further information on the B4 School Check can be found on the Ministry of Health's website (<http://www.moh.govt.nz/b4schoolcheck>).

This document must be read and adhered to by all users of the system including but not limited to:

- contracted B4 School Check providers
- vision and hearing technicians
- District Health Board (DHB) staff
- the Ministry of Health national co-ordinator, IT technical staff, and online helpdesk staff.

Purpose of the System

The basic purpose of the system is four-fold.

1. **Allocation and coverage:** to ensure that each eligible child is invited to participate in a B4 School Check and to ensure a focus on those populations in highest need.
2. **Referral and follow-up:** to ensure all services beyond the basic check are requested and monitored. In addition to referral to specialist services, these include enrolment in dental services, repeat testing for hearing and vision, request for, and receipt of, the Strengths and Difficulties Questionnaire for Teacher (SDQ-T), and immunisation reminder and catch-up.
3. **To track the health status of four-year-olds:** to create a nationally available, unit-level database of non-identifiable information for research, service development and planning purposes.
4. **Performance monitoring:** to administer the programme, including creating progress reports, and for planning, funding and auditing.

National level information requirements

It is essential to be able to track and evaluate over time the collective efforts of the many planners and providers to improve the health and wellbeing of children in New Zealand. Therefore, national level access to non-identifiable clinical data will be retained.

The type of access required is for:

- non-identifiable, unit-level data for research, service development and planning purposes
- identifiable non-clinical data by the national co-ordinator in order to maintain the system.

District Health Boards

DHBs are responsible (and have contractual obligations to the Ministry of Health) for the health and wellbeing of the population of their respective districts. They are required to conduct regular health needs assessments and to plan to ensure adequate service provision. Further, they must take account of population movement between districts.

The type of access required is for:

- non-identifiable, unit-level data to plan for services and to provide reports on B4 School Checks service delivery to the Ministry of Health.

See the 'Access rights by role' table at the end of this document for more detailed information.

District system to manage the programme

Each DHB is required to engage a B4 School Check co-ordinator to ensure the success of the programme and its sustainability as part of standard health and disability services. It must be possible to monitor the completion of checks, to action and track referrals, and to ensure a quality service is provided.

The type of access required is for:

- identifiable non-clinical data to track completion of checks
- identifiable clinical data to track referrals, including scoring and decision-making related to SDQ-Ts arriving back from early childhood centres.

See the 'Access rights by role' table at the end of this document for more detailed information.

Provider level information requirements

Nurses delivering the checks and those only entering the check results will have different levels of access, but both will see identifiable clinical data. Nurses delivering the checks will be able to both enter information and use the system to 'score' questionnaires.

The type of access required is for:

- identifiable clinical data of their allocated four-year-olds by frontline providers, including free text commentary and provision of minimum data requirements to the national information system
- identifiable clinical data of individual four-year-olds by vision and hearing technicians (this access would only be to the individual vision and hearing data being entered)
- provider information to allow the local administrator to manage local provider access.

See the 'Access rights by role' table at the end of this document for more detailed information.

Management of Health Information

The collection, exchange and management of health information about identifiable individuals held on the system falls within the provisions of the Public Records Act 2005, the Health Act 1956, the Privacy Act 1993 (<http://www.privacy.org.nz>), the Health Information Privacy Code 1994 (HIPC) (<http://www.privacy.org.nz>), and the Health (Retention of Health Information) Regulations 1996 (<http://www.moh.govt.nz>).

The Health Information Privacy Code (HIPC) is briefly summarised here to clarify the information privacy obligations when delivering the B4 School Check. Because the rules have been abbreviated, the Health Information Privacy Code 1994 should be consulted for the complete wording of each rule.

Rule 1 – Purpose of collecting the information

Rule 1 states that health information can only be collected by a health agency if it is collected for a lawful purpose connected with a function or activity of the agency and the collection of the information is necessary for that purpose.

The purposes of collecting B4 School Check information are listed below.

Identifiable information is for:

- **allocation and coverage** – to ensure that each eligible child is invited to participate in a B4 School Check and to ensure a focus on those populations in highest need
- **referral and follow-up** – to ensure all services beyond the basic check are requested and monitored. In addition to referral to specialist services, these include enrolment in dental services; repeat testing for hearing and vision; request for, and receipt of, the SDQ-T; and immunisation reminder and catch-up.

Non-identifiable information is for:

- **tracking the health status of four-year-olds** – to create a nationally available, anonymous, unit-level database for research purposes
- **performance monitoring** – to administer the programme, including creating progress reports, and for planning, funding and auditing.

Rules 2–4 – Source of information, collection of information from individuals and manner of collection

Rule 2 requires that health information must be collected directly from the individual or their representative (parent/guardian) unless compliance is not reasonably practicable (eg, from an infant or young child).

Rule 3 requires that where information is collected directly from the individual or their representative the individual or their representative is made aware of certain matters.

Rule 4 states that health information must not be collected by unlawful means or by means that in the circumstances of the case are unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

For Rules 2, 3 and 4, the B4 School Check providers must ensure that individuals (children and their parents/guardians) are told the following:

- that the child's name, date of birth, ethnicity, National Health Index (NHI) number and the results of the checks will be recorded by the B4 School Check provider and stored in the national B4 School Check information system
- the purpose of collecting the information and how this information is to be used, which is outlined under 'Purpose of the system' on page 2 of this policy
- that the results of their child's B4 School Check will be given to their family doctor and the vision and hearing test results will be given to the child's early education centre, kohanga reo, and/or school. Any information stored can only be accessed by properly authorised people who are working with their child, co-ordinating the B4 School Check, or managing the information system (except in exceptional circumstances)
- that they have a right of access to their information (see Rule 6) collected during the check
- that they have a right to request correction of information (see Rule 7)
- who to advise of changes in their contact information at the DHB or provider
- what consequences there will be if the information is not provided to the provider.

Collecting the information must be done in a professional, considerate and respectful manner which is sensitive to cultural differences.

If an individual opts off the B4 School Check, the only information retained in the system will be the NHI number, demographics, the date of birth of their child, the date of opting off, and any events recorded before they opted-off. This data is retained to prevent inappropriate recall and referral services.

Rule 5 – Storage and security

Rule 5 requires that the information is protected against loss, unauthorised access, use, modification or disclosure, and other misuse.

The system has been implemented by DHBs and contracted providers in accordance with the health sector and Ministry of Health's security framework and can only be used by someone who has signed an Authorised User Agreement (AUA), which defines their access rights and obligations concerning use and disclosure of information.

Internal or external staff other than approved users with the organisation may gain access to the information on the system when the computer equipment is being repaired or serviced. This must be covered by an appropriate confidentiality clause in the employment or contract agreements. Appropriate actions must be taken by the health organisation, their staff, and the service organisation to protect unauthorised access to the information in the system.

Where information is destroyed, the information should be disposed of in a manner which ensures that the privacy and confidentiality of the individual concerned remains intact. Hard-copy health information should be destroyed using shredding or a secure disposal bin. For soft copies a suitable destruction method should be used. Discuss this with your security officer or IT manager for appropriate options.

Responsibilities

Access responsibilities are as follows.

The DHB/provider manager will:

- determine and support the DHB/provider access control strategy
- ensure the satisfactory resolution of issues relating to user access, where the security officer or relevant personnel identifies significant changes are necessary.

Rule 6 – Access to information

Rule 6 says that when an agency holds health information in such a way that it can be readily retrieved, the individual concerned is entitled to obtain confirmation from the agency as to whether or not it holds such information and (with very few exceptions) to have access to that information. Where access is given, the individual must be advised that, under Rule 7, they may request correction of that information.

A child has right of access to their own information. However, in many cases, an adult may request information on the child's behalf.

Under section 22F of the Health Act 1956, a parent or guardian of a child under 16 has a right of access, on request, to health information about his or her child. The agency receiving the request must give the parent or guardian access to the information unless the child does not, or would not want, the information disclosed or the disclosure would not be in the child's interests. (There are other grounds for withholding the information, such as the person has a legal excuse for withholding the information, a prohibition in a statute for example, or if there are good grounds for doing so under the Privacy Act, but both of these are unlikely to be relevant.)

Requests must be responded to within 20 working days, and the parent or guardian may complain to the privacy commissioner if he or she does not receive a satisfactory response.

Rule 7 – Correction of information

Rule 7 states that an individual may request correction of their health information.

A parent or guardian, acting as the agent of his or her child has the right to request the correction of any information held on their child's record. As follows, there are three possible outcomes of such a request, and the action taken is dependent on the circumstances of the perceived inaccuracy.

- The record is corrected. This is most likely to occur where there is agreement between the B4 School Check provider and the parent that a genuine error has been made (for example, a typographical error, change of address or misspelling of the child's name).
- Unless there is good evidence that something entered was inaccurate, a statement should be placed on the record in a position where it will be read alongside the original information. This is the usual course of action when a patient (or parent) believes that there has been a misdiagnosis or disagrees with information placed on the record by a health provider.
- The request for correction is refused and the parent is advised that they have the right to complain to the privacy commissioner.

Rule 8 – Ensure accuracy of information before use

Rule 8 requires that any agency that holds health information must not use that information without taking reasonable steps to ensure that, having regard to the purposes for which the information is proposed to be used, the information is accurate, up to date, complete, relevant and not misleading.

Many different providers will be contributing information that will be entered onto the system and it is very important that the accuracy of the information is checked with the child and parent/guardian prior to recording the information. B4 School Check co-ordinators or those with a data entry role have the responsibility to enter data accurately.

Rule 9 – Retention of information

Rule 9 states that a health agency that holds health information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

All information in the B4SC information system will be subject to the Privacy Act 1993, the Public Records Act 2005, the Health Information Privacy Code 1994 and the Health (Retention of Health Information) Regulations 1996, which state that providers are required to retain identifiable information for a minimum of 10 years, beginning the day after the date on which the service was provided.

Rules 10 and 11 – Limits on use and disclosure of information

Rules 10 and 11 require that information is not used or disclosed other than for the purposes it was obtained for. The Ministry of Health will not use or disclose any information from the system unless expressly authorised under law.

Levels of access to information will depend on the role of a user (as described later) who is authorised to use and disclose information in accordance with their function. In addition, it may be appropriate for some of the information held on the system to be used in a non-identifiable form by others (eg, researchers) and this will require specific approval by the system's national governance body. If information is required for statistical analysis or planning purposes there will be no need to make information available which identifies the individual.

Use of the system by authorised users is dependent on them having a legitimate need for the information about a specific individual or population. They will enter and retrieve data for individuals during the course of their duties as a Well Child provider, public health nurse, practice nurse, general practitioner, public health provider, medical officer of health, B4 School check co-ordinator, or support staff.

Requests for non-anticipated disclosure of information

Requests for information that do not fit neatly into one of the purposes for originally collecting the information held on the system may be received. These requests must be passed to the national co-ordinator and they will be managed via the system national governance body.

Penalties for unauthorised disclosures

Existing Ministry of Health and DHB or provider penalties for the unauthorised use or disclosure of health information will cover information held on the system and will be enforced. Penalties could include the revocation of authorised user privileges, professional sanctions and disciplinary action. For the employee specifically this could include termination of employment and reporting to their relevant registration body. For the organisation it could include referral to the Health and Disability Commissioner.

Rule 12 – Unique identifiers

Rule 12 establishes that a health agency must not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out one or more of its functions effectively.

An individual child will only be able to be registered on the system if they have an allocated NHI number. The system will use the existing NHI number assigned to each individual as an identifier, but does not assign an NHI number to individuals.

Who can allocate new NHI numbers?

Co-ordinators and providers should contact the patient management system administrator of their local hospital to obtain a new NHI number for a child.

Complaints and Breaches of Privacy

In accordance with section 23 of the Privacy Act, the Ministry of Health and DHBs will at all times have an employee(s) who:

- ensures authorised users of the system comply with the HIPC
- deals with requests made under the HIPC or Privacy Act 1993
- assists the privacy commissioner with any investigations that might take place
- is responsible for dealing with any complaints relating to the system, an alleged breach of the HIPC, or breaches of privacy or security.

Basic principles of security

This information is a guide, it is important for you to follow your organisation's policies for the acceptable use of information.

The Do's

- Ensure that your computer equipment and premises are kept physically secure.
 - The office environment of B4 School Check users needs to be secure to ensure that data and hardware is accessible only to authorised personnel.
 - When there is a need for copies of personally identifiable B4 School Check data to be removed from the operational environment every precaution must be taken to ensure that the data is kept secure at all times.
- Ensure passwords/passphrases are selected carefully and kept secure at all times.
 - Protect your passwords to ensure these are not seen or used by unauthorised people.
 - You are accountable for any actions that take place under your user-ID and password/passphrase.
- Be sure that anti-virus software has been installed and activated on the computer that you use and ensure it is regularly updated.
- Ensure that your agency has a policy for the secure use of portable storage devices and that this policy is being adhered to.
- Be aware when using the system and accessing data, that:
 - you access the system in an appropriate manner
 - only authorised people can see the data
 - when using the computer system for other functions, you are not putting the information system at risk.
- Report any security-related incidents to your security officer or the person who holds this role.

The Don't's

- Don't write your passwords down and leave them around your desk or computer.
- Don't introduce new software to your computer without first having this approved by an appropriate person to ensure it does not introduce any risks to the B4 School Check system.
- Don't assume that new software comes from a trusted source – prevention is the key to better security.
- Don't download any games or other unauthorised applications from the internet.
- Don't use your administrative systems password for web access or email purposes. This is so that inadvertent disclosure of one password will not compromise the security of other systems.
- Don't browse other information throughout the network – access to information is allowed on a need-to-know basis only.

Security control responsibilities

The DHB/provider security officer will:

- ensure policies and standards address all DHB/provider requirements
- ensure that log-on and system access procedures meet DHB- or provider-defined requirements
- ensure that data and applications are safe in project development environments
- assist users in their day-to-day use of DHB/provider computer systems by performing basic account administration functions, including the unlocking of locked accounts, resetting passwords and providing user instruction.

Complaints and Breaches of Security

Any security-related incidents, violations, or suspected security weakness or threats to the system must be reported to the national co-ordinator via your security officer at the earliest opportunity but no later than the following business day.

Access to the System

The issue of access is focused on the system rather than the information which it contains and also on the individuals who can use the system, and the provider organisations connected to the system.

(Please note that this section of the document will go through a series of revisions over time because, after the initial release of the system via the Health Network, alternative access methods will be implemented.)

B4 School Checks are being delivered according to a number of different business models. In some cases the DHB itself is administering it; in others, the DHB has contracted their responsibilities and accountabilities to primary health organisations, Plunket, or other Well Child providers.

Organisations (eg, the DHB or provider) authorised to use the system will be responsible for ensuring that only authorised health professionals or employees working at their premises have direct access to the system.

Organisations are required to ensure reasonable policies and procedures are in place to safeguard identifiable information in the system.

Authorised user agreement

B4 School Check information system AUAs must be signed by users before they can access the information system. Under the AUA, users agree to protect the security and privacy of the child and their parent/guardian.

AUAs must be completed and signed by the person requesting access to the system. Each form should also be sighted and initialled by appropriately delegated staff (before granting access). The following table shows the staff responsible for sighting and initialling each form.

AUA type	User type	Forms to be sighted and initialled by:
Individual	DHB contact	DHB general manager
	Co-ordinator	DHB contact
	Lead provider/provider	Co-ordinator
	Local administrator	Co-ordinator
Organisation/practice	Organisation/practice	Co-ordinator

Co-ordinators and local administrators are responsible for:

- the ongoing administration of all users in their region
- sighting and storing all AUA forms (ensuring they are completed correctly, sighted and initialled as set out above)
- adding new users for their organisation or region

- ensuring users only have appropriate access and controls on the system
- deleting users as they leave the programme.

See the 'Access Rights by Role' table at the end of this guide for detailed information on system administration.

Access control responsibilities

Access control responsibilities for roles within organisations (DHBs or providers) are as follows.

Manager

- Supports user access.
- Ensures the satisfactory resolution of problems relating to the provision of user access when, in response to the concerns expressed by the Security Officer, significant changes are deemed necessary.

Security officer and/or system administrators

- Ensures information and IT protection requirements are in line with good security practice.
- Ensures that log-on and system access procedures meet DHB- or provider-defined requirements.
- Ensures that data and applications are safe in project development environments.
- Assists users in their day-to-day use of DHB/provider computer systems by performing basic account administration functions, including the unlocking of locked accounts, resetting passwords and providing user instruction.

Privacy officer

- Ensures that all access, use and disclosure of B4 School Check information by the DHB/provider complies with the rules of the HIPC and other legal requirements.
- Deals with privacy complaints to the DHB/provider relating to the B4 School Check and works with the privacy commissioner in relation to any investigations.
- Handles requests to the DHB/provider for personally identifiable information relating to the B4 School Check system.

Access control responsibilities for users of the system are as follows.

The minimum requirements for the control of system access, which the system does automatically, are:

- valid individual user identifications and passwords for all system access
- successful and unsuccessful system accesses are to be recorded
- the last time a user was logged on is to be recorded or displayed

- user account details are to be issued
- new user accounts are to be initially configured so as to force a change of the password upon first logging on.

The minimum requirements for external network connections and controls are:

- connections to other networks, including the world wide web, are to be protected through a firewall
- firewalls must be properly configured so as to ensure the required level of security is achieved
- default settings in network servers are to be changed so as to minimise the possibility of unauthorised access
- no software, or other material, is to be downloaded from the world wide web without the prior knowledge of the security officer.

Organisations must ensure that users of the system comply with the Health Information Security Framework (HISF), which can be found at <http://ithealthboard.health.nz/hisf>.

Access Rights by Role

Function	Description	National co-ordinator	B4 School Check co-ordinator	Lead provider	Provider	Vision and hearing technician
System administration		Central administrator access	Local administrator access	Local administrator access	No system administration access	No system administration access
Add DHB and regional organisations		✓ nationally	x	x	x	x
Maintain DHB and regional organisations		✓ nationally	✓	x	x	x
Add provider organisations		✓ nationally	x	x	x	x
Maintain provider organisations		✓ nationally	✓ for DHB	✓ for organisation	x	x
Add employees for organisations		✓ nationally	✓ for DHB	✓ for organisation	x	x
Maintain employees for organisations		✓ nationally	✓ for DHB	✓ for organisation	x	x
Allocate roles and access rights for users		✓ nationally	✓ for DHB	✓ for organisation	x	x
View list of all users and their relationship with other organisations		✓ nationally	✓ for DHB	✓ for organisation	x	x
Set passwords		✓ nationally	✓ for DHB	✓ for organisation	x	x
Use of system						
Log on	Log on to system using user ID and password	✓	✓	✓	✓	✓

Function	Description	National co-ordinator	B4 School Check co-ordinator	Lead provider	Provider	Vision and hearing technician
View group of children	Children who are eligible for the B4 School Check can be viewed as a group. Filters such as location, age, ethnicity, deprivation, status of the check, can be applied to this group. Children leave this group when the check has been performed and closed off, or the campaign year is over and the child is no longer eligible.	✓ nationally	Can view the details of all children within this group located in their region.	View the details of all children within this group that have been allocated to them or search and view details of all children that are allocated to their organisation.	View the details of all children within this group that have been allocated to them.	View the details of all children within this group that have been allocated to them.
Search for children eligible children nationwide	Search on a nationwide basis for children aged over 4 years of age. The search requirement is the child's NHI number or first name, or surname, or date of birth.	✓	✓	✓	✓	
Allocate children to provider organisations	Children in the eligible group need to be allocated to a provider for the B4 School Check results to be entered into the system.	x	Allocate children in their region to the provider organisations.	Allocate the children (allocated to their organisation) to providers within that organisation.	x	x
View the status of B4 School Checks	The system enables the status of each B4 School Check to be tracked. A completed check may have outstanding referrals and the allocated provider has not closed the check.	x	View the status of all in-progress, completed and closed B4 School Checks within their region.	View the status of all in-progress, completed (but not closed) B4 School Checks allocated to them, and search then view status of checks allocated to their organisation.	View the status of all in-progress and completed B4 School Checks allocated to them.	View the status of B4 School Checks allocated to them.

Function	Description	National co-ordinator	B4 School Check co-ordinator	Lead provider	Provider	Vision and hearing technician
View an individual child's demographic information	The system enables the information for each eligible child to be viewed.	Search for and view the details of children allocated to each DHB for the campaign year for B4 School Checks in each region.	View the details of all children allocated to the DHB for the campaign year for the B4 School Checks within their region.	View the details of children allocated to them with not started, in-progress or completed B4 School Checks. Search for and view details of children allocated to their organisation.	View the details of all children allocated to them with not started, in-progress or completed B4 School Checks allocated to them.	View the details of all children allocated to them.
Enter the caregiver's consent into the system	The system requires an indication that consent has been obtained prior to entering the B4 School Check data.	x	Enter the consent details.	Enter the consent details for children that have been allocated within the provider organisation.	Enter the consent details for children allocated to them.	Enter the consent details for children allocated to them.
Enter B4 School Check results into the system	The results from each of the B4 School Check tests are entered into the system for each child. The prerequisite for this stage is the entry of the consent confirmation. Any referral resulting from the B4 School Check will be entered. A child's B4 School Check record can be closed off at this stage (indicating that the B4 School Check process has been completed) if no referrals have been generated.	x	Enter B4 School Check test results in their region.	Enter B4 School Check test results for children within the provider organisation.	Enter B4 School Check test results for children allocated to them.	Enter vision and hearing checks for children allocated to them.
Enter referral confirmations into the system	The system captures the generation of any referrals resulting from the B4 School Check. Each referral must be closed off by following up and completing the referral record in the system prior to closing the B4 School Check record for each child.	x	Enter referral confirmations in their region.	Enter referral confirmations for children within the provider organisation.	Enter referral confirmations for children allocated to them.	Enter vision and hearing referral confirmations for children allocated to them.

Function	Description	National co-ordinator	B4 School Check co-ordinator	Lead provider	Provider	Vision and hearing technician
Return to the co-ordinator those records that are not part of their organisation/ cohort	Children wrongly allocated to an organisation (eg, reside in a different region) need to be returned to the co-ordinator for reallocation.	✓	Return children to other co-ordinators.	Return to the co-ordinator children allocated to their organisation.	Return to the co-ordinator children allocated to them.	Return to the co-ordinator children allocated to them.