ISO TC 215/N601

Date: 2007-12-18

ISO/DTS 27527

ISO TC 215/SC /WG 1

Secretariat: ANSI

Health informatics — Provider identification

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: Technical Specification
Document subtype:
Document stage: (30) Committee
Document language: E

Document type: Technical Specification
Document subtype:
Document stage: (30) Committee
Document language: E

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TS 27527 was prepared by Technical Committee ISO/TC 215, *Health informatics*, WG1, *Data structure*.

0 Introduction

The ability to positively identify providers and locate their relevant details is an important support to the provision of speedy, safe, high quality, comprehensive and efficient health care.

This Technical Specification is the result of health industry needs for a common, best practice approach to the way data are used captured, stored and managed for the purpose of identifying providers. The objective is to provide the health industry with a Technical Specification for healthcare provider identification for clinical and administrative data management purposes (data structure and specification) which promotes uniformly good practice in identifying individual providers and providers as organisations and recording identifying data. This will assist significantly in ensuring that records relating to each provider will be associated with that individual or organisation and no other.

Without such a document, the unique identification of providers will be jeopardized and there is a risk that different parties may develop inconsistent methods.

This Technical Specification has important uses in common with ISO/DTS 22220 *Health informatics – Identification of subjects of health care*. For example, when patient health information is shared between various providers for purposes of clinical management, ISO/DTS 22220 should be used to ensure the unique identification of the patient associated with a particular provider and organisation.

In this initial publication, the scope of the Technical Specification has been limited to provider identification and though it identifies the relationships required between providers, provider organisations, sites of services and the services themselves, these are not discussed in detail.

This Technical Specification does not supersede any other International Standard or Technical Specification but rather acts as a consolidation of best practice principles and guidelines for collection and storage of provider identification data.

The term ‘informative’ has been used in this Technical Specification to define the application of the annexes applied to it. An informative annex is only for information and guidance. Safe and efficient patient care requires that all organizations implementing shared access to electronic health records ensure that providers of services are correctly and unambiguously identified, even if the records with which they are associated come from sources outside conventional juridicational or organisational boundaries. This is critically important to countries, provinces and/or states with significant cross border flow of patients. This identification is further complicated when one entity is certified by more than one professional organization or discipline, or works in more than one organizational context. The provision of directories or lists of providers and their service locations for consumer information and to support electronic communication between providers is beyond the scope of this document.

The ability to positively identify providers (both face-to-face and electronically) and to locate their relevant details, is an important support to the provision of speedy, safe, high quality, comprehensive and efficient.

Unambiguous identification of providers (individuals or organizations) is necessary for a wide range of purposes including:

i) registration of providers;

ii) requesting and/or reporting of orders, tests and results (e.g. pathology, diagnostic imaging);

iii) other communications and referrals between providers regarding ongoing care of patients (e.g. a referral from a general practitioner to a specialist, a hospital discharge plan);

iv) reporting on health services provision to statutory authorities (e.g. reporting of hospital patient administration systems data to state/territory government health agencies);

v) payments to providers; and

vi) directories or lists of providers and their service locations for consumer information.

Benefits of positive identification include:

i) the ability to verify information about individual providers with other data to identify or confirm their capabilities and qualifications (e.g. their speciality, registration with accredited bodies);

ii) the ability to confidently communicate with other providers for ongoing client care;

iii) the ability to compile reliable information about services provided by individual providers to individual clients;

iv) efficient and appropriate payments of fees, rebates, etc. to providers;

v) reduction of the time wasted and inconvenience generated in searching for and/or re-gathering information;

vi) provide a source of reliable information to access, authorization and security systems and enhances provider and consumer confidence in electronic health records;

vii) improve care quality by supporting professional practice reviews, research on care delivery patterns and outcomes, etc.;

viii) auditing who has added, changed or accessed electronic records for quality, access and privacy audits;

ix) secondary use of provider data for purposes such as manpower planning and resource allocation.

Standards for the communication of identifying information are beyond the scope of this document, and are specified within standards of the Health Level 7 (HL7) organisation.

The development and use of provider identification in health care supports collection and maintenance of information identifying the qualifications and accreditation of providers as well as electronic signature information. This document defines qualification data requirements but not those required for electronic signatures as these are defined elsewhere.

The effective and efficient identification of providers translates to more efficient and high quality care.

The delivery of health care services is undergoing paradigm change, brought about by changing consumer expectations, technological advances, economic pressures, socio-demographic change and changes in the patterns of health and ill health in communities.

These changes include:

a) a shift from institution-centred care to client-centred care, together with greater empowerment of consumers;

b) greater emphasis on continuity of services in supporting quality and safety, health promotion and maintenance;

c) more integrated services, in which organizational and administrative barriers are invisible to clients;

d) migration from paper based to electronic media for transactions including orders, tests and results, sharing of patient health information between various providers, and payments to providers.

These changes underline the need for more careful attention to the provision of unambiguous identification of providers across all disciplines and settings, especially where multiple records or information systems are involved.

This Technical Specification provides a framework for improving confidence in the data being associated with any given provider, and upon which clinical communication and data aggregation are based, are appropriate and accurate.

Health informatics — Provider identification

1 Scope

This Technical Specification provides a framework for improving the positive identification of providers. Identification of ‘providers’ encompasses individuals and organizations. The Technical Specification includes data elements needed for identification of individual providers (i.e. individuals), data elements needed for the identification of organization providers (i.e. organizations). Identification in this document refers both to the process of being able to identify individuals and organisations and the data elements required to support that identification manually and from a computer processing perspective.

This Technical Specification can be applied to all providers of services, individuals and organisations. It details both data and processes for collection and application of identifying information for providers. It defines demographic and other identifying data elements suited to capture and use for the identification of providers in health care settings and provides guidance on their application. The services provided, and the locations at which these services are provided by organisations and individuals, are not included, but are a logical later extension of this document.

This Technical Specification provides:

- definitions of data elements to support the identification of individual providers and organisational providers for purposes such as electronic health record authentication and authorization, communications, role definitions, delegation of authority, and the management of certification of individuals where more than one discipline is concerned;

- guidance on the development, population, governance and ongoing management of provider identifiers from multiple potential sources. This includes identification of processes to support national, multinational and provincial/state or local level identification. Unique identifier structures may differ for different purposes, or with different originating organisations. For this reason a generic approach to the structure of these identifiers is given in this document to support multiple unique identifiers and the ability to link these to the relevant provider.

This Technical Specification is primarily concerned with provider identification data for clinical and administrative purposes. The Technical Specification should be used by health and health related establishments that create, use or maintain records on providers. Establishments should use this Technical Specification, where appropriate, for collecting data when registering providers.

The scope of identification in the environment of national registers includes the elements in Figure 1.

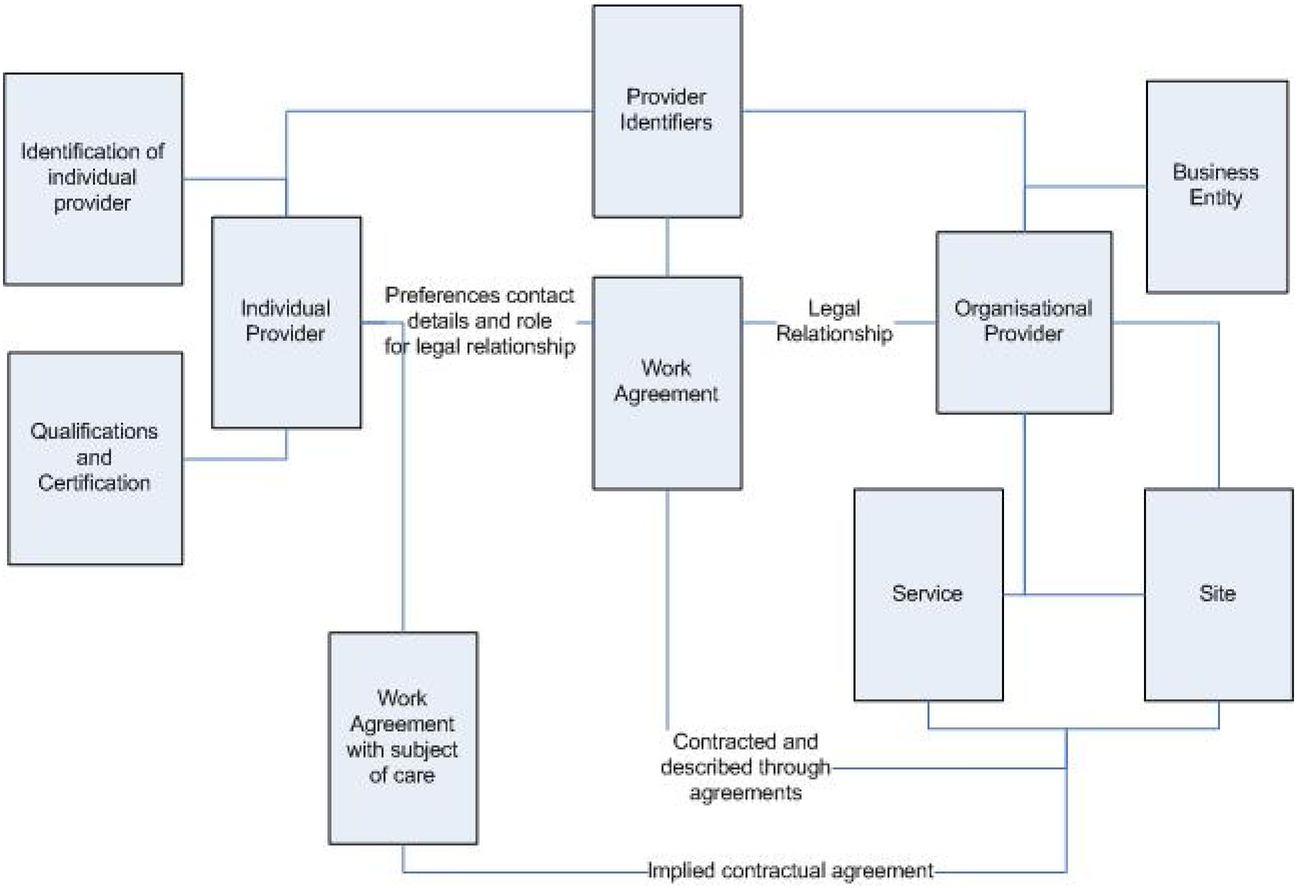
Provider Identifiers
Identification of individual provider
Business Entity
Individual Provider
Preferences contact details and role for legal relationship
Work Agreement
Legal Relationship
Organisational Provider
Qualifications and Certification
Service
Site
Work Agreement with subject of care
Contracted and described through agreements
Implied contractual agreement

Figure 1 — Typical components of provider registers

The scope of this work is limited to the areas included in more detail in Figure 2, individual and organisational provider identification, excluding work agreements, site and service relationships.

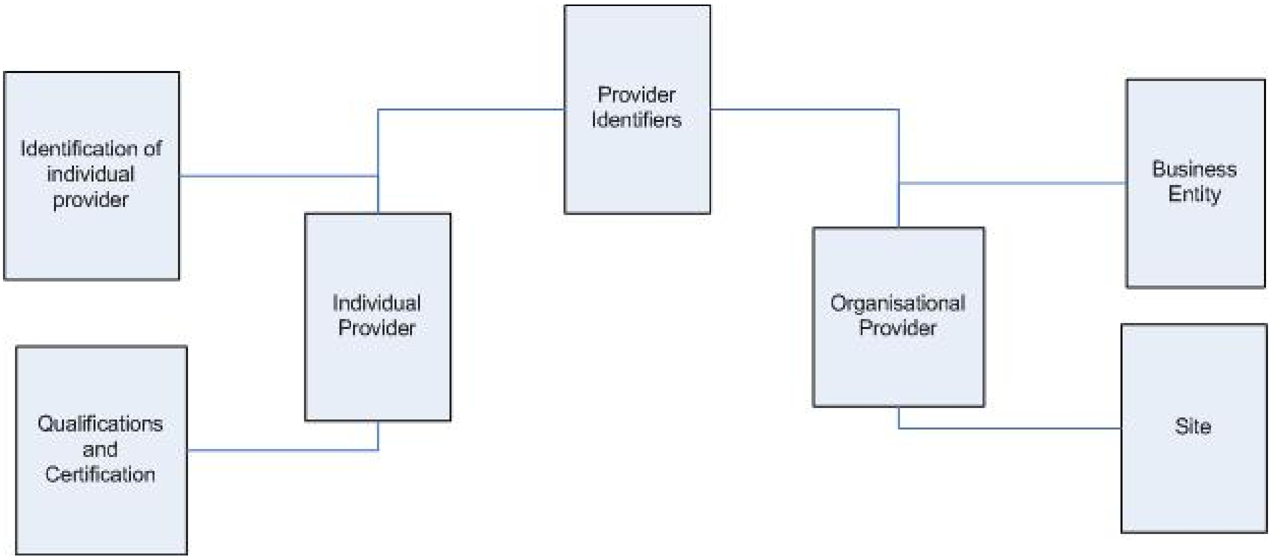

Figure 2 —Individual and organisational provider identification relationships

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10646:2003, *Information technology -- Universal Multiple-Octet Coded Character Set (UCS)*

ISO/IEC 11179:2005, *Information technology—Metadata registries (MDR)*

ISO/IEC 11179-3-2005, *Information technology -- Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes*

ISO/IEC 19785-1:2006, *Information technology -- Common Biometric Exchange Formats Framework -- Part 1: Data element specification*

ISO/IEC 19785-2:2006, *Information technology -- Common Biometric Exchange Formats Framework -- Part 2: Procedures for the operation of the Biometric Registration Authority*

ISO/IEC 2022:1994, *Information technology – Character code structure and extension techniques*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
business entity
recognised formal business entity, such as a corporation or company. This entity holds details of the formal 'owner' entity of the organisation

3.2
capture
deliberate action, which results in the registration of a record into a provider record keeping system

3.3
individual provider
any person who provides or is a potential provider of a health care service. An individual provider is an individual person and is not considered to be a group of providers

3.4
information system
organized collection of hardware, software, supplies, policies, procedures and people that stores, processes and provides access to information

3.5
organization
any organization of interest to, or involved in, the business of service provision

3.6
provider
any person or organization that is involved in or associated with the delivery of health services to a client, or caring for client well-being

3.7
provider identifier
unique number or code issued for the purpose of uniquely identifying a provider

3.8
records
recorded information, in any form, including data in computer systems, created or received and maintained by an organization or person in the transaction of business or the conduct of affairs and kept as evidence of such activity

3.10
registration
act of giving a record a unique identity in a record keeping system

3.11
service entity
services provided by an organisation or which an organisation is able, or licensed, to provide

3.12
storage
function of storing records for future retrieval and use

4 Components

This Technical Specification includes recommendations concerning the data elements most likely to affect the quality and ability to achieve accurate identification of providers, particularly when identifying individuals face-to-face or when communicating electronically. This document also identifies the data elements suited to identification in the broad delivery environment.

It is good practice to always use name, sex and date of birth to identify individuals, and name and address to identify organizations when manually confirming the identity of either an individual or an organisation. When communicating between systems electronically, the existence of a unique identifier may be used with some of these elements confirming (where required) the unique identity of the individual. This document does not endeavour to identify the required elements for transmission between systems, as these can be highly dependant upon local, cultural and policy factors.

Figure 3 indicates the data elements defined in this Technical Specification and indicates their general relationships to each other.

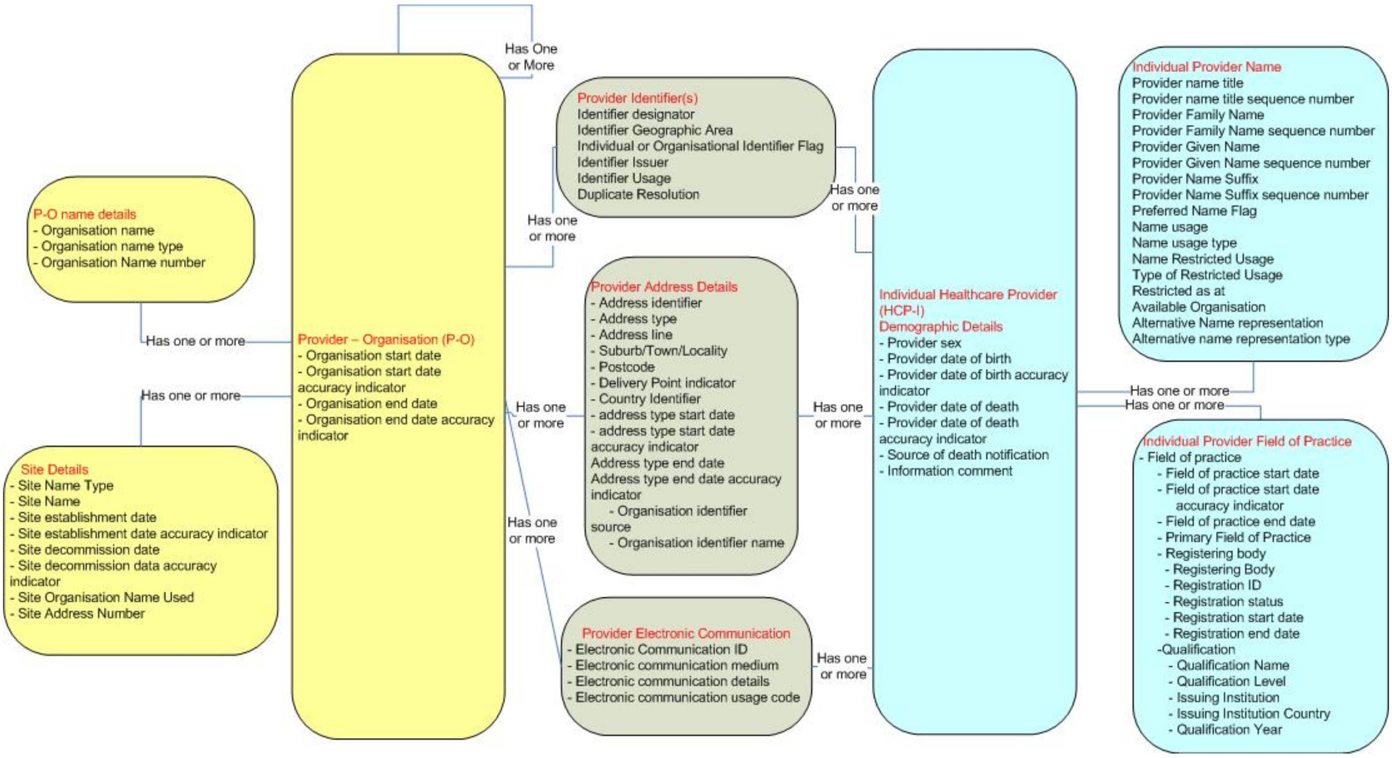
Has One or More
P-O name details
- Organisation name
- Organisation name type
- Organisation Name number
Has one or more
Provider – Organisation (P-O)
- Organisation start date
- Organisation start date accuracy indicator
- Organisation end date
- Organisation end date accuracy indicator
Has one or more
Site Details
- Site Name Type
- Site Name
- Site establishment date
- Site establishment date accuracy indicator
- Site decommission date
- Site decommission data accuracy indicator
- Site Organisation Name Used
- Site Address Number
Has one or more
Provider Identifier(s)
Identifier designator
Identifier Geographic Area
Individual or Organisational Identifier Flag
Identifier Issuer
Identifier Usage
Duplicate Resolution
Has one or more
Has one or more
Provider Address Details
- Address identifier
- Address type
- Address line
- Suburb/Town/Locality
- Postcode
- Delivery Point indicator
- Country Identifier
- address type start date
- address type start date accuracy indicator
Address type end date
Address type end date accuracy indicator
- Organisation identifier source
- Organisation identifier name
Has one or more
Has one or more
Provider Electronic Communication
- Electronic Communication ID
- Electronic communication medium
- Electronic communication details
- Electronic communication usage code
Has one or more
Individual Healthcare Provider (HCP-I)
Demographic Details
- Provider sex
- Provider date of birth
- Provider date of birth accuracy indicator
- Provider date of death
- Provider date of death accuracy indicator
- Source of death notification
- Information comment
Individual Provider Name
Provider name title
Provider name title sequence number
Provider Family Name
Provider Family Name sequence number
Provider Given Name
Provider Given Name sequence number
Provider Name Suffix
Provider Name Suffix sequence number
Preferred Name Flag
Name usage
Name usage type
Name Restricted Usage
Type of Restricted Usage
Restricted as at
Available Organisation
Alternative Name representation
Alternative name representation type
Has one or more
Has one or more
Individual Provider Field of Practice
- Field of practice
- Field of practice start date
- Field of practice start date accuracy indicator
- Field of practice end date
- Primary Field of Practice
- Registering body
- Registering Body
- Registration ID
- Registration status
- Registration start date
- Registration end date
-Qualification
- Qualification Name
- Qualification Level
- Issuing Institution
- Issuing Institution Country
- Qualification Year

Figure 3 — Detailed elements in provider identification

4.1 Data element structure

Each data element has been defined according to a set of metadata components that are based on ISO 11179-3. The data set to be determined consistent with country requirements and standards. Most components (viz. definition, data type, representational class, data domain, etc.) describe essential features of the structure of a data element. Some components such as collection methods and comments describe additional, non-essential features and may be left blank where appropriate.

The metadata components of each data element are described in sections 4.1.1 to 4.1.9.

4.1.1 Synonym

Alternative name(s) for this data element.

4.1.2 Definition

A statement that expresses the essential nature of the data element and its differentiation from all other data elements.

4.1.3 Source standards

Details of established data definitions or guidelines for data elements that have been cited in this Technical Specification are listed in Clause 2 and the Bibliography.

4.1.4 Data type

It is recognised that different representations of the values shown in this Technical Specification may be required. Where possible the data types are described in a manner consistent with HL7 data types.

- Boolean-literal (true/false);
- Number (ISO 11404) (only used in this Technical Specification where arithmetic operations are performed)
- Character string;
- Text or unconstrained text;
- Coded text (from an agreed vocabulary or value domain);
- Constrained text (where the text is associated with a formal terminology). The difference between the coded and constrained text is the relationship to a formal, structured terminology, as opposed to a code set, or list of values;
- Unique identifier;
- Dates/times.

Though there are other data types, they are not required within this Technical Specification so have not been included here.

4.1.5 Data domain

The values or codes acceptable for representation of the data element. The data elements contained in this Technical Specification are either free text or coded free text. For each data element that is coded, a code value is provided as well as a description of the code value and in some cases an alternative code (generally an alphabetic representation). The code should be used for communication of this data value, the descriptor is the title of the code value, and the alternative code is provided for collection of the data, where the use of alphabetic code values is preferred at the point of data collection or for screen viewing. For example, the data domain for the data element Sex is shown in Table 1 below:

Table 1 —Example of data domain representation

Code	Descriptor	Alternative code
1	Male	M
2	Female	F
3	Indeterminate	I
9	Not stated/inadequately described	N

4.1.6 Guide for use

Additional guidance to inform the use of the data element.

4.1.7 Verification rules

Quality control mechanisms that restrict the collection, storage or transferral of non-valid data.

4.1.8 Collection methods

Comments and advice concerning the actual capture of data for the particular data elements to achieve uniformly high quality data.

4.1.9 Comments (optional)

Any further information relevant to data element collection or storage.

4.2 Summary of provider identifiers

This section of the Technical Specification identifies and describes the components and attributes and the relationships between them for basic provider identification. Table 2 represents the concepts required to meet the needs of provider identification that are included and described more fully in this Technical Specification.

Table 2 — Summary of data element structure

Section of document	Data elements	Opt.	Data type	Repeat data element
5	Provider identifier	R	Identifier	Y
6	Individual provider (P – I)	0	Text	Y
6.1	Individual provider name	R	Text	Y
6.2	Individual provider demographic details	R	Text	N
6.3	Individual provider field of practice	R	Text	Y
7	Individual provider biometric identifier	R	Text	Y
8	Provider organisation (HCP-O)	O	Text	Y
8.1.1	Organisation start date	R	Date	N
8.1.2	Organisation start date accuracy Indicator	R	Coded text	N
8.1.3	Organisation end date	O	Date	N
8.1.4	Organization owner provider identifier	R	Identifier	Y
8.1.5	Organisation name details	R	Text	Y
8.1.6	Organisation site	R	Text	Y
9	Provider address	O	Text	Y
10	Provider electronic communication	O	Text	Y

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required
O = Optional

Identification of ‘providers’ includes the need to uniquely identify both *individuals* and the *organizations* who provide health services. This Technical Specification includes the:

- data elements needed for identification of individual providers (i.e. *individuals*) and their authority to provide specific services within the system at any given point in time;

- data elements needed for the identification of organizations acting as providers (i.e. *organizations*) and to identify the business within which the organisation works and the services provided by that organisation and the location of those services;

- data elements needed for the identification of both individuals and organisations.

Unambiguous identification of an individual provider in data systems is only assured through the use of an officially assigned identifier (e.g. a professional registration number, an identifier issued by a recognized accreditation body or regulatory authority (e.g. a state medical registration board). Other personal characteristics such as name, address, date of birth, sex, qualifications and/or electronic communication details (e.g. phone, fax or email address) are an important adjunct to the process of unambiguous identification by humans interacting with a system to identify a provider, as are the services which the person is authorised to provide and the place at which those services are offered. These contact details are also required to support electronic communication and access in an electronic health record environment.

Unambiguous identification of an individual provider within an organization (i.e. the combination of *organization* and *individual* often through a specific role to provide a service at a location*)* requires identification of the individual using the individual provider data elements, in addition to an organization identifier and the identification of the specific role in which the relationship between the provider and the organisation is being invoked. This Technical Specification does not identify provider roles or the relationships between an individual and the organisation.

5 Provider identifier

Whether considering an individual or an organisation, a unique identifier is required. This section includes data elements that are used as a unique identifier. The provider identifier is composed of five elements. These elements together represent a unique identifier. A provider may have one or more of these identifiers, each of which may be used for different purposes and by different health care organisations. This approach has been adopted to allow for the identification of providers in legacy systems and through historical legal health care documentation and processes, as these alternative identifiers are likely to continue to exist throughout health care systems.

Table 3 — Summary of data elements for provider identifier

Section of document	Data elements	Opt.	Data type	Repeat data element
5	Provider identifier	R	Identifier	Y
5.1	Provider identifier designation	R	Identifier	N
5.2	Provider identifier geographic area	O	Coded text	N
5.3	Individual or organisational identifier flag	R	Coded text	N
5.4	Provider identifier issuer	R	Identifier	Y
5.5	Provider identifier usage	R	Coded text	Y
5.6	Duplicate resolution	O		Y
5.6.1	Not a duplicate of	O	Identifier	N
5.6.2	Duplicate of	O	Identifier	N
5.6.3	Confirmed by organisation	R	Identifier	Y
5.6.4	Date confirmed	R	Date	Y
5.6.5	Retired identifier	R	Boolean	N

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required
O = Optional

5.1 Provider identifier designation

Synonym Healthcare provider identifier number

Individual provider identifier number

Provider number

Individual provider identifier (IPI)

Health provider identifier – individual provider (HPI-P)

Healthcare provider organisation number

Healthcare provider number

Healthcare provider organisation identifier (HPI-O)

Registration number

Definition

A number or code assigned to an individual or organisation, agency, establishment or domain in order to uniquely identify that provider within the system.

Source Technical Specifications

ASTM E1714-00, *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*

Data type

Unique identifier

Data domain

Identifier code

Guide for use

Individual agencies, establishments or collection authorities may use their own alphabetic, numeric or string coding systems for identification of individuals within their own systems. However regional, national or international approaches are required for the identification of organisations and for identification of individuals across and between organisations.

The combination of the provider identifier designation, provider identifier usage, provider identifier issuer, individual or organisational identifier flag and provider identifier name, uniquely identify the provider.

ASTM E1714-00 should be used as a guide to the properties of provider identifiers.

It shall be noted that though this is a unique identifier, the identifier is only unique within the purpose for which it was issued and for the organisation responsible for issuing the number. In other words, a single identifier may exist more than once in a system, but when combined with the other data components of the provider identifier the total, aggregate provider identifier is unique.

Validation rules

Field may not be blank.

Collection method

The following criteria and characteristics of the provider identifier are adapted from the ASTM E1714-95 *Guide for Properties of a Universal Identifier (UHID).*

Atomic - the provider identifier should be a single data item. It should not contain sub-elements that have meaning outside the context of the entire identifier. Nor should the identifier designation consist of multiple items that shall be taken together to constitute an identifier.

Content free - the provider identifier should not depend on possibly changing or possibly unknown information pertaining to the provider. Including such content in the identifier will make it impossible to assign the 'correct' identifier if that information is not known. It also leads to invalid situations if the information changes: for example, what happens to an identifier based on sex if the subject has a sex change procedure.

Longevity – the provider identification system should be designed to function for the foreseeable future. It should not contain known limitations that will force the system to be restructured or revised radically.

Permanent - once assigned, a provider identifier should remain with the individual provider. It should never be reassigned to another subject, even after the subject's death.

Unambiguous - whether represented in automated or handwritten form, a provider identifier should minimize the risk of misinterpretation. Where using string identifiers, be aware of possible confusion with the number '0' with the letter 'O' and the number '1' with the letter 'l'.

Unique – a valid provider identifier designation should identify one and only one provider.

5.2 Provider identifier geographic area

Definition A code representing the geographic area within which this identifier is used.

Source Technical Specifications

Data type Coded text

Data domain

Code	Description	Alternative code
1	Local identifier	L
2	Area, region or district identifier	A
3	State/province/territory identifier	S
4	National identifier	N

Verification rules

Collection method

5.3 Individual or organisational provider flag

Synonym Individual or organisational provider indicator

Definition Indicates whether this is an identifier for an individual healthcare provider or for a healthcare organization.

Source Technical Specifications

Data type Coded text.

Data domain

Code	Description	Alternative representation
1	Individual provider	I
2	Organisational provider	O

Guide for use This is a required field.

Verification rules Field may not be blank.

Collection method

5.4 Provider identifier issuer

Synonym Provider identifier assigning authority (HL7 PID 3.4)

Definition The organisation, agency or provider that allocates a provider identifier designation.

Source Technical Specifications HL7 (STF-2 ID code <assigning authority>)

HL7 V3 Authority Name

Data type Unique identifier

Data domain Unique identifier of the issuer of this provider identifier.

Guide for use It is desirable that this field be represented using established, formal identifiers to assist in communication between organisations. As such, an identifier does not always exist. Implementation may require that the field be free text. Where an established identifier exists for a service provider who issues the identifier, the unique identifier of that organisation should be used in this field.

Verification rules

Collection method

5.5 Provider identifier usage

Synonym	Provider identifier type code.
Definition	The specific context of use for which this identifier is used within the organisation (e.g. billing identifier, national identifier).
Source Technical Specifications	HL7 PID-3.5 - Identifier Type Code
Data type	Coded text.
Data domain	The purpose or intended use of this unique identifier.
Guide for use	Each identifier issuer shall identify the usage for each type of identifier they issue: Examples of individual provider identifier usage types could include: 01 – Unique national identifier (to be used where only one number is used for identification by this issuer) 02 – Billing identifier 03 – Business or individual taxation or social security identifier 08 – obsolete identifier – used in the past but no longer used by the issuer
Verification rules	
Collection method	

5.6 Duplicate resolution

Provider registries may have duplicates (multiple registrations for a single individual or organisation). Computer systems and manual searching of registries will identify potential duplicates. This group of data allow users to identify where they have determined that two identifiers which appear to be duplicates are not duplicated, or to indicate that where they are discovered to be duplicates – which number is retired and no longer used, and which is retained. This process is often called 'merging' of identifiers. This group of data allow the user to establish the relationship between potential or actual duplicate entries.

5.6.1 Not a duplicate of

Definition	The identifier which has been determined to not be a duplicate of this identifier.
Source Technical Specifications	
Data type	Identifier
Data domain	A valid provider identifier in the register with the same geographic area, organisation identifier, provider identifier issuer and provider identifier usage as this identifier.
Guide for use	The identifier entered into this field is not a duplicate entry of this identifier. The objective of this field is to support potential duplicate reporting by being able to identify that the set indicated by this link do not represent a duplication, even if each provider's information is very similar.
Verification rules	If entered the 'confirmed by' and 'date confirmed' shall be entered. If entered the 'duplicate of' field shall not be entered.

5.6.2 Duplicate of

Definition	The identifier which has been determined to be a duplicate of this identifier.
Source Technical Specifications	
Data type	Identifier

Data domain A valid provider identifier in the register with the same geographic area, organisation identifier, provider identifier issuer and provider identifier usage as this identifier.

Guide for use The identifier entered into this field is a duplicate entry of this identifier. The objective of this field is to support potential duplicate reporting by being able to identify that the set indicated by this link do not represent a duplication, even if each provider’s information is very similar.

Verification rules If entered the 'confirmed by' and 'date confirmed' shall be entered.

If entered the ‘Not a duplicate of’ field shall not be entered.

5.6.3 Confirmed by organisation

Definition The organisation that has confirmed the duplicate or not duplicate status of this identifier.

Source Technical Specifications

Data type Identifier

Data domain A valid provider organisation identifier.

Guide for use The identifier of the organisation that has confirmed the duplicate status of this identifier.

Verification rules Where a duplicate or not, this field shall be entered.

5.6.4 Date confirmed

Definition The date upon which this identifier was determined as a duplicate or not a duplicate.

Source Technical Specifications

Data type Date.

Data domain A valid date.

Guide for use This dates indicates the date upon which this identifier was either:

- determined not to be a duplicate of the 'not a duplicate’ identifier; or
- determined to be a duplicate of the ’duplicate of’ identifier.

Verification rules A current or past date.

5.6.5 Retired identifier

Definition For a duplicate identifier set this field indicates if this number is the one retired (not for further use) or not.

Source Technical Specifications

Data type Boolean

Data domain Y = this identifier is retired

N = this identifier is not retired

Guide for use When two identifiers are found to be duplicated for a given individual the ’duplicate of’ field will be completed. In this case it is necessary to indicate which of the two identifiers is to be retained and which retired. This field indicates the number that is not for ongoing use. The identifier is retained in systems, but not actively used.

Verification rules Required when the ’duplicate of’ field is not blank.

6 Individual provider

The person who has, is, or could, provide services is an individual provider. Many of the data elements required to support the unique identification of a provider are the same as those used to identify an individual subject of care. Where the elements are the same, the subject of care Technical Specification has been referenced.

To support provider verification and directory services a provider identification system shall have details of the individual and of their qualifications and certification. This document identifies qualifications and certifications for individual providers, but does not address the relationships between the individual and the organisation.

Individual providers can be identified uniquely using a unique identifier. They may be found using directory services by searching using specific data elements. This search process results in the detection of the provider's unique identifier. Identifiers may be linked to electronic signature information, which is not described here. Clear communication with individual providers can occur directly through the individual, e.g. for confirmation or update of registration information, or through the identification of the relationship of the provider to the organisation/location/service. This section deals with identification of the individual provider.

Table 4 indicates the component elements required for identification of the individual as a provider. The identification of the individual person requires the maintenance of at least these data elements.

Table 4 —Data element components for individual providers

Section of document	Data elements	Opt.	Data type	Repeat data element
5	Provider identifier	R	Identifier	Y
6	Individual provider	R	Text	Y
6.1	Individual provider name	R	Text	Y
6.2	Individual provider demographic details	R	Text	N
6.3	Individual provider field of practice	R	Text	Y
7	Individual provider biometric identification	O	Text	Y
9	Provider address	R	Text	Y
10	Provider electronic communication	O	Text	Y

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required
O = Optional				

Those data elements that are generic to all providers (whether individual or organisations have been specified once, and though referenced in this section, are not included in detail). Table 4 indicates the section of the document in which each element is presented and described in detail.

6.1 Individual provider name

6.1.1 General

Individual provider name is a composite data element that is captured through the combination of name title group, given name group, name usage group and name suffix group

There may be more than one name recorded for each individual provider. At least one name shall be captured. There may be multiple titles, given names, suffixes and name usage for any name (referred to as the complete set of attributes). Only one name may be the person's preferred name at any given point in time. A specific name may be necessary to be used for reporting to given agencies. This concept is managed through the name usage concept. Where different languages and cultures require names to be represented using alternative character sets, this is done through the alternative name representation concept, of which any name may have multiples.

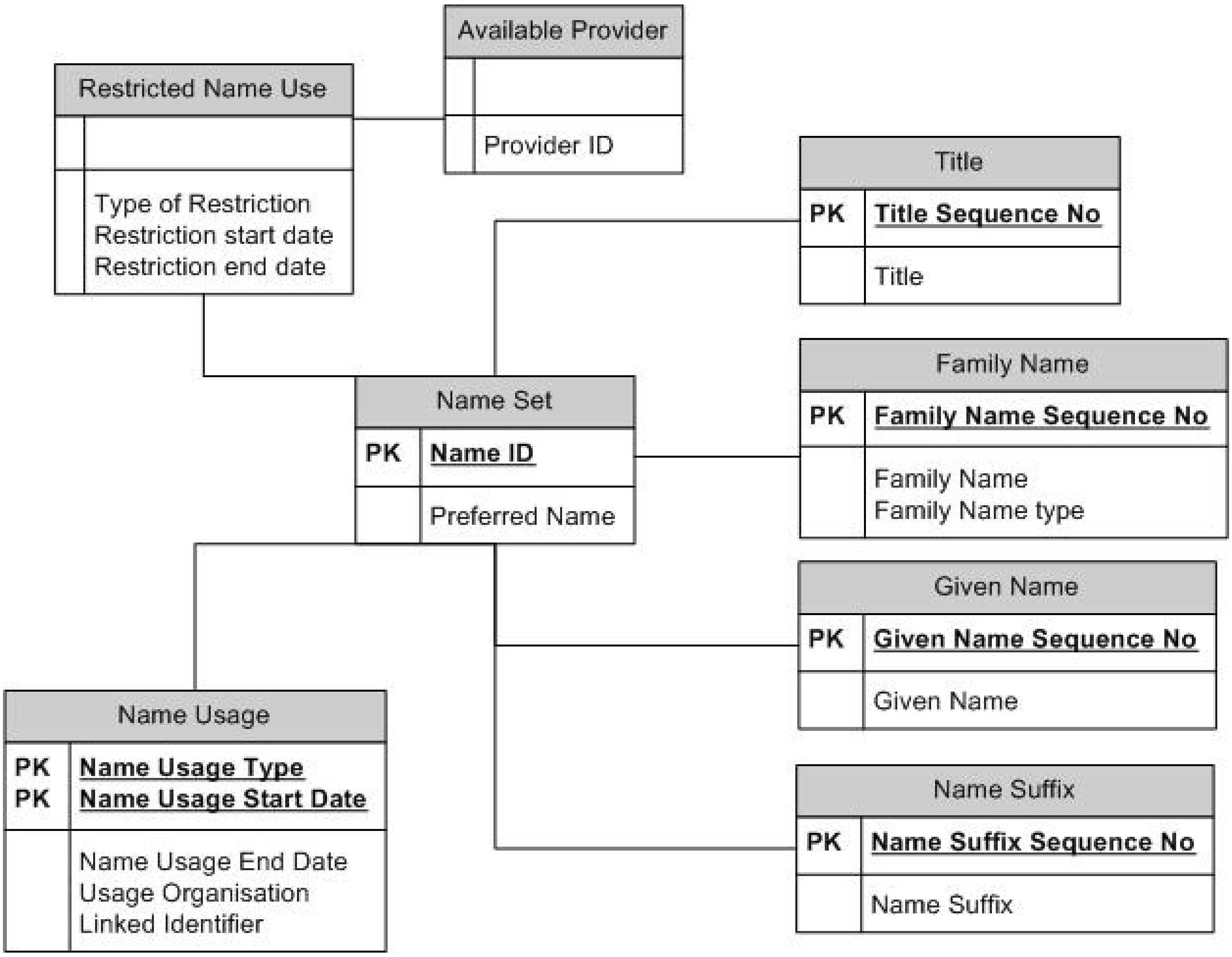

Figure 4 — Relationships of name data elements

Figure 4 indicates the data elements available for the combination data element of name. Table 5 shows a summarised example outline of each of these elements.

Each of these data elements is consistent with those described in ISO TS 22220 *Heather informatics - Identification of subjects of health care,* Section 6. For that reason they are only described in summary here.

Table 5 — Individual provider name data elements

Section	Data element name	Opt.	Data type	Repeat data element	Example
6.1	Individual provider name	R		Y	
6.1.2	**Family name group**	**R**	**Text**	**Y**	
6.1.2.1	Family name	R	Text	N	Brown
6.1.2.2	Family name sequence number	R	Number	N	1
6.1.3	**Preferred name**	**R**	**Boolean**	**N**	**N**
6.1.4	**IP name title group**	**O**		**Y**	
6.1.4.1	IP name title	R	Text	N	Dr
6.1.4.2	IP name title sequence	R	Number	N	1

	number				
6.1.5	**Given name group**	**O**		**Y**	
6.1.5.1	Given name	R	Text	N	Mary
6.1.5.2	Given name sequence number	R	Number	N	1
6.1.6	**Name suffix group**	**O**		**Y**	
6.1.7	Name suffix	R	Text	N	
6.1.7.1	Name suffix sequence number	R	Number	N	
6.1.8	**Name usage group**	**O**		**Y**	
6.1.8.1	Name usage	R	Coded text	N	1 Reporting
6.1.8.2	Name usage start date	R	Date	N	
6.1.8.3	Name usage end date	O	Date	N	
6.1.8.4	Usage identifier	O	Unique identifier	N	113456 Insurance company unique ID for this person
6.1.9	**Alternative name representation**	**O**		**Y**	
6.1.9.1	Representation usage	R	Coded text	N	
6.1.9.2	Alternative representation	R	Text	N	
6.1.9	**Restricted name usage**	**O**		Y	
6.1.9.1	Type of restriction	R		N	
6.1.9.2	Restriction start date	R		N	
6.1.9.3	Restriction end date	O		N	
6.1.9.4	Available provider	O		Y	

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required (the group may be required, or where the group is optional the individual data elements within the group may be marked as required. In this case, where the group exists the required elements shall be present.
O = Optional (the group or individual data element are optional)

6.1.2 Family name group

This group includes each family name element of a specific family name set and indicates the sequence within which the names should be used. The group includes family name and a family name sequence number. Individual provider name is the combination of name title (and sequence number/s), family name/s (and sequence number/s), given name/s (and sequence number/s), name suffix/s (and sequence number/s) and usage information such as preferred name, name usage and name conditional use.

6.1.2.1 Family name

Synonyms Surname

Last name

Definition The part of a name a person usually has in common with some other members of his/her family, as distinguished from his/her given names.

6.1.2.2 Family name sequence number

Definition An indicator of the order of use for family name/s.

6.1.3 Preferred name

Definition Indicates the name by which the subject chooses to be identified.

6.1.4 Name title group

This group holds details of each title relevant to a specific family name for this individual provider. The group indicates the actual title and the sequence in which that title should appear before the person's name.

EXAMPLE 'DR, Rev Brown' would have DR as the 1st sequenced name title and Rev as the 2nd sequence name title.

6.1.4.1 Name title

Synonym Title

Honourific

Name prefix (HL7)

Definition An honorific form of address commencing a name, used when addressing an individual provider by name, whether by mail, by phone, or depending upon cultural situation in person.

6.1.4.2 Name title sequence number

Definition An indicator of the order of use for name titles.

Collection method

6.1.5 Given name group

The given name group is associated with a specific family name and set of titles, suffixes and name usage rules. There may be many given name groups, within each there is a given name and a given name sequence number.

6.1.5.1 Given name

Synonym First name

Middle name

Forename

Second name

Other given name

Other given name/s

Definition The subject's identifying name(s) within the family group or by which the subject is uniquely identified.

6.1.5.2 Given name sequence number

Definition An indicator of the order of use for given names.

6.1.6 Name suffix group

This group indicates a specific name suffix used with a defined name group. The sequence number indicates the sequence in which the suffixes are to be used for display, printing, etc.

6.1.7 Name suffix

Definition Additional term used following a person’s name to identify an individual provider.

6.1.7.1 Name suffix sequence number

Definition An indicator of the order of use for name suffix.

6.1.8 Name usage group

This is a value set that enables differentiation between recorded names for an individual provider. A name may be associated with a specific unique identifier, in which case the usage type should indicate the identifier type and identifier issuer and identifier name in the specific identifier field. For example, the name to be used for billing purposes.

A name may have many name usage groups, but each group shall have a name usage indicated, and may have associated dates and unique identifier for reporting.

6.1.8.1 Name usage

Definition A classification that enables differentiation between the usage of names for an individual provider. An individual name may have many name uses.

Source Technical Specifications HL7 (PID-5 *Patient* name, Table 0200 *Person Name Usage code*)
AS 4590 (Clause 3.6 *Person Name Usage code*)

Data type Coded text

Data domain

Code	Description	Alternative code
1	Reporting	R
3	Professional or business name	B
4	Maiden name (name at birth) (original name)	M
5	Registered name (legal name) (formal name)	L
8	Other name (alias)	O

Guide for use

More than one name can be recorded for an individual provider and each of these names may have more than one usage at any given point in time. Each name shall have one or more name usages associated with it. Record as many as required.

Where there is only one name recorded that name is assumed to be the name for all other purposes, including unique identification, and financial reporting. However, where the subject offers more than one name, clarification should be obtained from the subject to ensure accurate recording of the various names. All currently used names, as well as names by which the subject has previously been known, should be recorded if these are known. These names should never be deleted from the system as there may be existing paper work with the old names, or reference from other agencies to the name used in the past or in error.

Reporting name (R) is the subject's name as it is to be used for reporting, when used with a specific identifier. There should only be one reporting name for any given specific identifier at a time, therefore the combination of usage type, identifier and obsolete as it should clearly identify the name to be used for reporting.

Professional or business name (B) is the name used by the individual provider for business or professional purposes.

Maiden name (M) is the name used by the individual provider prior to marriage

Other name (O) is any other name that a subject is also known by, or has been known by in the past; that is, all other names. This includes misspelled names or name variations that are to be retained as they have been used to identify this subject. More than one other name may be recorded for a subject.

Validation rule

Collection method

6.1.8.2 Name usage start date

Definition The date at which this name usage for the name to which the usage is associated starts.

6.1.8.3 Name usage end date

Definition The date at which this name usage for the name to which the usage is associated ceased to be used.

6.1.8.4 Usage identifier

Definition The combination of identifier type, identifier issuer and identifier name that specify the link between this name and reporting, or other unique identifier usage.

Source Technical Specifications

Data type Unique identifier.

Data domain Provider identifier.

Guide for use This field is used to provide a link between the name and a unique identifier and identification issuer for a purpose, usually reporting.

Validation rule A unique identifier shall exist for the provider for whom this set of identifier information is to be used

Collection method It is suggested that a system would provide a set of existing identifiers from which the user can select, rather than expect manual entry of this information.

6.1.9 Alternative name representation

This group of data elements indicate the representation of a name when the alphabetic representation is not the one used within a community. This is sometimes called the domestic name, local representation or local name. Any alternative font or character-based representation of a name set should be included here.

A name may have multiple alternative name representations

6.1.9.1 Representation usage

Synonym Domestic name type

Type of local representation of name

Alternative character set handling scheme (HL7)

Definition Name of the representational form used.

Source Technical Specifications ISO/IEC 2022

Data type Coded text.

Data domain Valid language representations

Guide for use This field is used to indicate domestic representations,

e.g. domestic Russian name, Chinese character representation.

Verification rules

Collection method

6.1.9.2 Alternative representation

Synonym Domestic name

Character representation

Local name representation

Domestic name representation

Definition Alternative representation of this individual provider name using alternative styles of representation such as characters or language character set variations for local display.

Source Technical Specifications

Data type Text.

Data domain

Guide for use Name represented using an alternative font / character system.

This field is linked to the representation usage element.

Verification rules

Collection method

6.1.9 Restricted name usage

A name may be used for a limited period of time or special purpose within an organisation (such as tribal names). This set of data elements apply to a specific name set and are used within computer systems to restrict the way a name is used or displayed in that system.

6.1.9.1 Type of restriction

Synonym Conditional name usage type.

Definition An indicator of special conditions or rules that shall be applied to an individual provider name.

Source Technical Specifications

Data type Coded text

Data domain

Code	Description	Alternative code
1	Unreliable information	U
2	Name not for continued use	N
3	Special privacy /security requirement	P

Codes 1-3 are recommended for *storage*, and the alternative codes are recommended for *collection* of data where the full descriptor cannot be displayed.

Guide for use **Unreliable information** -should be used where it is known that the name recorded is a fictitious or partial name. These names should not be used for automatic matching provider data.

Name not for continued use -certain tribal names may become ‘not for continued use’.

Special privacy/security requirements -may apply to names for which episodes are attached that should only be accessible to specified authorized persons. There shall be a specific need to implement this additional security level. Local policy should provide guidance on the use of this code.

Verification rules Valid codes or blank.

Collection method

6.1.9.2 Restriction start date

Definition The date at which this restricted name usage starts.

6.1.9.3 Restriction end date

Definition The date at which this restricted name usage ceased to apply.

6.1.9.4 Available provider

Synonym Viewing provider

Definition The provider identifier where this name is unrestricted.

Source Technical Specifications	
Data type	Identifier
Data domain	A valid provider identifier (individual or organisational)
Guide for use	This field indicates those providers who should be able to see this name and the details associated with it.
Verification rules	Valid provider identifier.
Collection method	

6.2 Individual provider demographic details

6.2.1 General

This section describes additional demographic data elements that should be used, where relevant, to maximize the likelihood of positive identification of an individual provider. Figure 5 shows the structure of this data group. The elements included in this group are consistent with those used for identification of subjects of care. For full details refer to ISO DTS 222200 *Health informatics – Identification of subject of health care.*

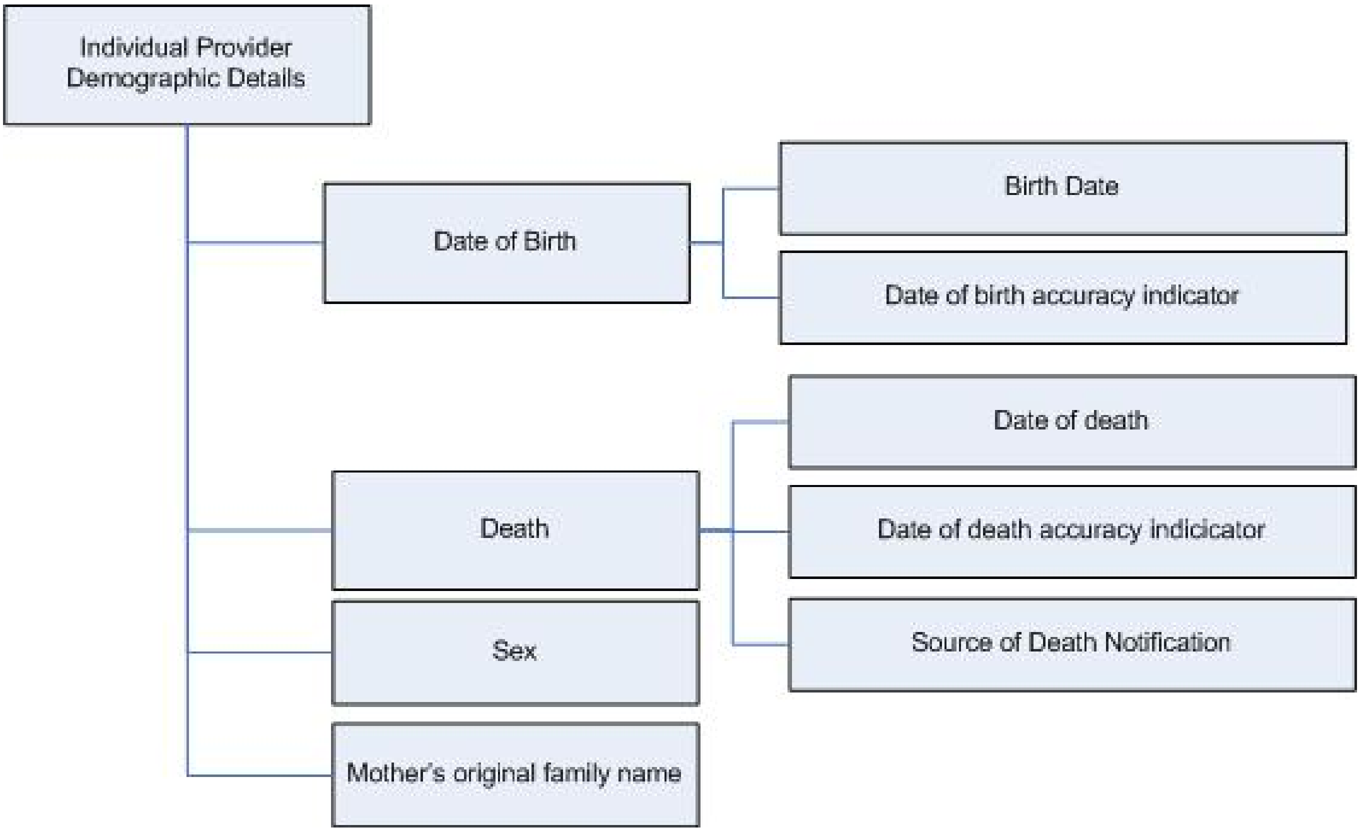
Individual Provider Demographic Details
Date of Birth
Birth Date
Date of birth accuracy indicator
Date of death
Death
Date of death accuracy indicator
Sex
Source of Death Notification
Mother's original family name

Figure 5 — Structure of individual provider demographic details

Table 6 indicates the data elements that describe specific demographic components of a person's demography of particular importance when identifying an individual.

Table 6 — Summary of demographic components

Section	Data element name	Opt.	Data type	Repeat data element	Example
6.2.2	**Date of birth data**	**R**		**N**	

	group				
6.2.2.1	Date of birth	R	Date	N	19601209
6.2.2.2	Date of birth accuracy indicator	O	Coded text	N	AAE
6.2.3	**Death**	**O**		**N**	
6.2.3.1	Date of death	R	Date	N	19991208
6.2.3.2	Date of death accuracy indicator	O	Coded text	N	AAE
6.2.3.3	Source of death notification	O	Coded text	N	2
6.2.4	**Sex**	**R**	**Coded text**	**N**	**1 (Male)**
6.2.5	**Mother's original family name**	**O**	**Text**	**N**	**N**
NOTE: Opt. = Indicates whether the data element is optional or required R = Required (the group may be required, or where the group is optional the individual data elements within the group may be marked as required. In this case, where the group exists the required elements shall be present. O = Optional (the group or individual data element are optional)					

6.2.2 Date of birth data group

This concept of date of birth comprises the elements date of birth, date of birth accuracy indicator.

6.2.2.1 Date of birth

Synonym Birthdate

Definition The date of birth of the individual provider

Comment May be used in conjunction with date of birth accuracy indicator.

6.2.2.2 Date of birth accuracy indicator

Definition An indication of the accuracy of a reported date at the date component level for dates represented in YYYYMMDD format.

6.2.3 Death

This concept of death comprises the elements death date, date of death presentation style, estimated date (of death) flag.

6.2.3.1 Date of death

Synonym Death date.

Definition The date of death of the individual provider.

6.2.3.2 Date of death accuracy indicator

Synonym Estimated date (of death) flag.

Definition An indication of whether any component of a reported date was estimated.

6.2.3.3 Source of death notification

Definition Indicates the most reliable source for information about an individual provider’s death. This field provides an indication of the certainty of the information.

Source Technical Specifications

Data type Coded text

Data domain

Code	Description
1	Registry
2	Healthcare provider
3	Relative
4	Other
9	Unknown

Guide for use **Registry –** notification received from an official registry such as births, deaths or coroner, death certificate. This source is considered to be the information source of the greatest certainty.

Healthcare provider – death is notified directly from a provider, other than the person responsible for certification of death. This source is considered to be of very good certainty.

Relative – death is highly likely to be certain, but cases of inaccurate reporting of death by relatives has been known and should not be considered equal in certainty to health provider or official register as a source of death information.

Other – death is identified through newspapers and other sources. These should be considered a less reliable source of death notification.

Unknown - The source of information about the subject’s death is not known. This is the least reliable source of death notification.

Validation rule Valid codes or blank. Death notification may not be recorded by the provider to whom this record pertains.

Collection method This data element should always be used in conjunction with a date of death

Comment Where an official registry is not the originating source, every attempt should be made to subsequently validate the reported death against the registry, and the code for the source updated accordingly.

6.2.4 Sex

Definition The sex of the provider individual.

Sex is the biological distinction between male and female. Where there is an inconsistency between anatomical and chromosomal characteristics, sex is based on anatomical characteristics.

6.2.5 Mother’s original family name

Synonym Mother’s maiden name

Mother’s gamily name

Mother’s surname

Definition The original family name of the individual provider’s mother.

6.3 Field of practice

6.3.1 General

This section contains data elements that describe the provider's field of practice, including their qualifications and registration/certification to provide services within that field of practice. Figure 6 indicates the components of field of practice.

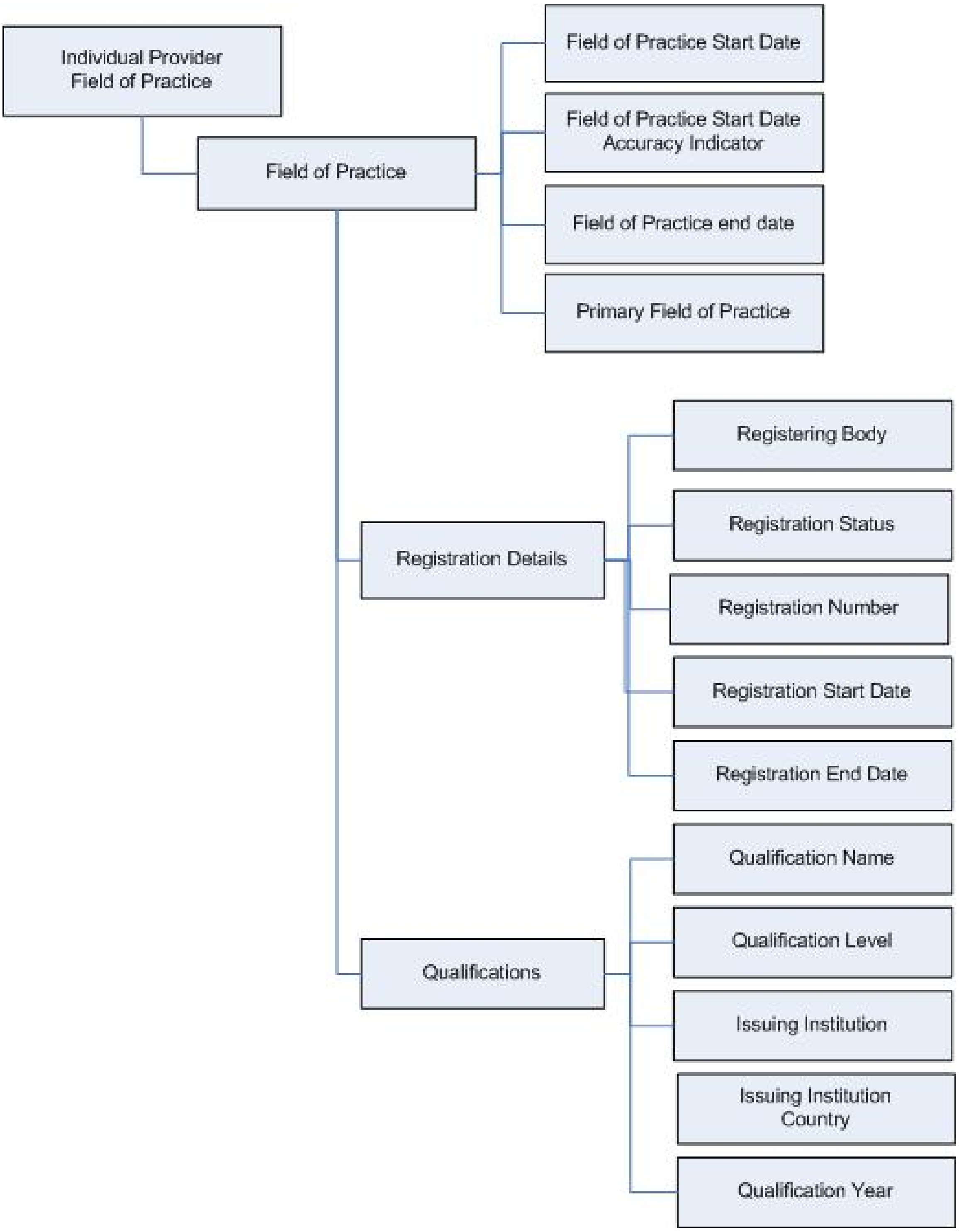

Figure 6 — Structure and components of individual field of practice

These elements are required to identify a provider's legal capacity to provide a service within a field of practice.

Table 7 — Summary of field of practice components

Section	Data element name	Opt.	Data type	Repeat data element
6.3	**Field of practice**	**R**	**Coded text**	**Y**
6.3.1.1	Field of practice start date	R	Date	N
6.3.1.2	Field of practice start date accuracy indicator	R	Coded text	N
6.3.1.3	Field of practice end date	O	Date	N
6.3.1.4	Primary field of practice	R	Boolean	N
6.3.1.5	Registration details	R		Y
6.3.1.5.1	Registering body	R	Coded text	N
6.3.1.5.2	Registration status	R	Coded text	N
6.3.1.5.3	Registration number (unique identifier)	R	Identifier	N
6.3.1.5.4	Registration start date	R	Date	N
6.3.1.5.5	Registration end date	O	Date	N
6.3.1.6	Qualifications	O		Y
6.3.1.6.1	Qualification name	R	Coded text	N
6.3.1.6.2	Qualification level	O	Coded text	N
6.3.1.6.3	Issuing institution	R	Coded text	N
6.3.1.6.5	Issuing institution country	R	Coded text	N
6.3.1.6.4	Qualification year	O	Coded text	N

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required (the group may be required, or where the group is optional the individual data elements within the group may be marked as required. In this case, where the group exists the required elements shall be present.
O = Optional (the group or individual data element are optional)

6.3.2 Field of practice

Field of practice indicates the specialty in which this provider is qualified by a recognized accreditation body or regulatory authority to provide services. A provider may be entitled to practice in more than one field. Field of practice is used in conjunction with field of practice start date, field of practice start date accuracy indicator and field of practice end date.

Definition: The field that an individual provider identifies as being their field of practice and has the required qualifications and registration to support that claim.

Source standards: HL7 (PRA-3 *Practitioner category*)

Data type: Coded text.

Data domain: Determine codes used within the identifier domain.

Guide for use: The following is an example of a list of common provider occupations. The Abbreviation NEC represents a code to be used when the concept is ‘Not Elsewhere Classifiable’:

Occupations	**ASCO code**
General medical practitioner	2311-11
Medical practitioner in training	2311-81
Anaesthetist	2312-11
Dermatologist	2312-13
Ophthalmologist	2312-19
Paediatrician	2312-21
Pathologist	2312-23
Specialist physician	2312-25
Psychiatrist	2312-27
Radiologist	2312-29
Surgeon	2312-31
Specialist medical practitioner *NEC*	2312-79
Nurse manager	2321-11
Nurse educator	2322-11
Nurse researcher	2322-13
Registered nurse	2323-11
Registered midwife	2324-11
Registered mental health nurse	2325-11
Registered development disability nurse	2326-11
Dentist	2381-11
Dental specialist	2381-13
Hospital pharmacist	2382-11
Industrial pharmacist	2382-13
Retail pharmacist	2382-15
Occupational therapist	2383-11
Optometrist	2384-11
Physiotherapist	2385-11
Speech pathologist	2386-11
Chiropractor	2387-11
Osteopath	2387-13
Podiatrist	2388-11
Medical diagnostic radiographer	2391-11
Radiation therapist	2391-13
Nuclear medicine technologist	2391-15
Sonographer	2391-17
Dietician	2393-11
Naturopath	2394-11
Acupuncturist	2394-13

Natural therapies professional **NEC*	2394-79
Audiologist	2399-11
Orthoptist	2399-13
Orthotist	2399-15
Health professionals **NEC*	2399-79
Social worker	2511-11
Rehabilitation counsellor	2513-11
Drug and alcohol counsellor	2513-13
Clinical psychologist	2514-11
Psychologist **NEC*	2514-79
Office manager	3291-11
Enrolled nurse	3411-11
Ambulance officer	3491-11
Intensive care ambulance paramedic	3491-13
Dental therapist	3492-11
Dental hygienist	3492-13
Dental technician	3492-15
Aboriginal and Torres Strait Islander health worker	3493-11
Massage therapist	3494-11
Secretary	5111-11
Personal assistant	5111-13
Receptionist	6131-11
Admissions clerk	6191-13
Hostel parent	6313-11
Child or youth residential care assistant	6313-13
Refuge worker	6313-15
Aged or disabled person carer	6313-17
Therapy aide	6313-19
Personal care assistant	6314-11
Nursing assistant	6314-13
Dental assistant	6391-11
Security officer	8311-11

Verification rules:

Collection methods: Collect also the provider field of practice start date, field of practice start date accuracy indicator and provider field of practice end date as well as information on the registering authority and/or issuing body. The registering body or issuing body is the preferred source of this information, and if not, then should be used to validate the information wherever possible.

Comments: Field of practice is collected for the purpose of unambiguous identification and is not intended to be an exhaustive list of all fields of practice and/or specialty work areas or roles.

6.3.2.1 Field of practice start date

Definition: The date on which an individual provider commenced practising in a field of practice.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date.

Data domain: Valid dates.

Guide for use: Enter the date using day, month and year.

If the date is estimated is some way, it is recommended the data element, date accuracy indicator, also be recorded at the time of record creation to flag the accuracy of the data.

For data integrity, data exchange, future data analysis and/or manipulation of data from diverse sources the date accuracy indicator shall be used in conjunction with the provider field of practice start date in all instances to ensure accuracy.

Verification rules: This field shall:

- be less than or equal to the field of practice end date (if that date is not blank);
- be a valid date

Collection methods:

6.3.2.2 Field of practice start date accuracy indicator

Definition An indication of the accuracy of the start date recorded for this field of practice.

Source Technical Specifications Australian NHDD (Knowledgebase ID: 000431 estimated date flag)

Data type Coded text

Data domain Any combination of the values A, E, U representing the corresponding level of accuracy of each date component of the reported date including:

Code	**Description**
AAA	Accurate date
EEE	Estimated date
UUU	Unknown date
EAA	Accurate day and month, estimated year
AAU	Unknown day, accurate month and year
UUE	Unknown day and month, estimated year
UUA	Unknown day and month, accurate year

The domain values will be dependant upon the date of birth presentation style value. The examples below are for a presentation style DDMMYYYY.

Data domain	Date component (for format DDMMYYYY)		
	(D)ay	(M)onth	(Y)ear
Accurate	A	A	A
Estimated	E	E	E
Unknown	U	U	U

Guide for use Used to record the level of certainty or estimation used in recording the Individual Provider's address type start date.

Validation rules Any combination of the codes A, E and or U.

Collection method This data element should always be used in conjunction with a field of practice start date.

Comment Most computer systems require a valid date to be recorded in a date field i.e. the month part shall be an integer between 1 and 12, the day part shall be an integer between 1 and 31 with rules about the months with less than 31 days, and the year part should include the century. However, in actual practice, the date or date components are often not known. This means that a date shall be included and it shall follow the rules for a valid date. It therefore follows that, while such a date will contain valid values according to the rules for a date, the date is in fact an 'unknown' or 'estimated' date. For future users of the data it is essential they know that a date is accurate, unknown or estimated and which components of the date are accurate, unknown or estimated.

6.3.2.3 Field of practice end date

Definition: The date on which an individual provider ceased practising in a field of practice.

Source standards: HL7 (STF-13 *Institution inactivation date*)

Data type: Date.

Data domain: Valid dates or blank.

Guide for use: Enter the date using day, month and year.

Verification rules: This field shall:

- be greater than or equal to the field of practice start date;
- be a valid date

6.3.2.4 Primary field of practice

Synonym: Main area of practice

Main field of practice

Principal field of practice

Principal specialty

Definition: A flag that indicates the current primary specialty or field of practice of an individual provider.

Source standards:

Data type: Boolean

Data domain:

Code	Description
1	Main/primary field of practice
2	Other field of practice

Guide for use: Multiple values for ‘field of practice’ may be collected. Where an individual identifies with only one field more specifically than another currently active field of practice, this flag can be set. For example, a dentist who is also a medical practitioner may practise as both and want both recorded as his/her ‘field of practice’.

Verification rules: Only one field of practice may be designated the primary field of practice at any given point in time.

Collection methods: This data should be collected from the most reliable source that is available, e.g. the issuing body, and updated regularly to reflect any changes in the provider’s field of practice and associated qualifications.

Comments:

6.3.2.5 Registration details

In most cases providers are required to be registered or certified in order to practice legally. Where this is a requirement of a given field of practice these details shall be recorded. An individual field of practice may have multiple registration details over a period of time.

6.3.2.5.1 Registering body

Synonym Registration board

Certification body

Definition: The organisation with the legal and professional capacity to register or certify and uniquely designate an individual health care provider in this field of practice.

Source standards:

Data type: Coded text.

Data domain: Established by the governing body for provider registration within a jurisdiction, such as a state or nation.

Guide for use: The registering body shall be recorded along with the registration status and start date for registration to be considered valid. The information should be validated with the registering body on a regular basis to reflect changes in the provider’s registration status.

Verification rules: Shall be the registering body appropriate to the field of care applicable at the time within the jurisdiction.

Collection methods: Collect also registration status, registration number and registration start date.

Comments:

6.3.2.5.2 Registration status

Synonym Registration level

Certification level

Definition: The status of the individual provider's registration to practice in a given field of practice.

Source standards:

Data type: Coded text.

Data domain:

Code	Description
1	Active / full registration
2	Limited registration
3	Student registration
4	Suspended registration
5	Terminated registration
6	Nullified
7	Pending
9	Inactive registration

Guide for use: The registering body may indicate different levels of registration.

Full registration – the registrant is fully qualified to provide services within the scope of the field of practice.

Limited registration – the registrant is limited to provide services within a defined sub-set of the field of practice. These limitations need to be clearly defined for each field of practice.

Student registration – the registrant is able to provide supervised services only.

Inactive – the registrant is no longer active in the field.

This approach supports easier re-registration of registrants who may be practicing in a different jurisdiction for a period of time.

Verification rules: This information shall be provided in conjunction with registration information.

Collection methods: Collect also registering body, registration number and registration start date.

Comments:

6.3.2.5.3 Registration number

Synonym Unique provider identifier

Certification number

Definition: The unique identifier issued by the registering body to this provider that identifies them uniquely within the registration system. This item is not described here, as it is an example of a unique identifier, described earlier.

6.3.2.5.4 Registration start date

Definition: The date on which an individual provider's formal registration commenced.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date.

Data domain: Valid dates .

Guide for use: Enter the date using day, month and year.

Verification rules: This field shall be entered and:

- be less than or equal to the field of practice end date (if that date is not blank); and
- be a valid date.

Collection methods:

6.3.2.5.5 Registration end date

Definition: The date on which an individual provider's formal registration ceased/ceases.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date.

Data domain: Valid dates.

Guide for use: Enter the date using day, month and year. This date may be the end of one registration period and be followed by the addition of a whole set of new registration details. It would be expected that the common data scenario would be that the end date of the last registration period would be the day before the start date of the next registration period.

Verification rules: This field shall be entered and:

- be less than or equal to the field of practice end date (if that date is not blank); and
- be a valid date.

Collection methods:

6.3.2.6 Qualification

This group of data indicate the formal qualifications of an individual provider. Individuals may have multiple qualifications. For each qualification the following data items for a descriptive set.

6.3.2.6.1 Qualification name

Definition: The full and formal name given to the qualification.

Source standards:

Data type: Text.

Data domain:

Guide for use: Enter the full name of the qualification.

E.g. Bachelor of Medicine.

Verification rules: This field shall be entered.

Collection methods:

6.3.2.6.2 Qualification level

Definition: Classification indicating the level of qualification.

Source standards:

Data type: Coded text.

Data domain: Data set to be determined consistent with country requirements and standards.

Guide for use: Indicate the level of this qualification.

Verification rules: This field shall be entered.

Collection methods:

6.3.2.6.3 Issuing institution

Definition: The name of the educational organisation who issued the qualification.

Source standards:

Data type: Text.

Data domain: Data set to be determined consistent with country requirements and standards.

Guide for use: Enter the full name of the institution.

Verification rules: This field shall be entered.

Collection methods:

6.3.2.6.4 Issuing institution country

Definition: The international code for the country within which the education institution is registered.

Source standards: Data set to be determined consistent with country requirements and standards.

Data type: Coded text.

Data domain: Data set to be determined consistent with country requirements and standards.

Guide for use: Enter the code relevant to the country applicable at the time of qualification.

Verification rules: This field shall be entered and shall be a valid country code.

Collection methods:

6.3.2.6.5 Qualification year

Definition: The year in which the individual provider obtained this qualification.

Source standards:

Data type: Date.

Data domain: Year.

Guide for use: Enter the year. If the year is unable to be obtained with certainty, enter the earliest available registration year.

Verification rules:

Collection methods:

7 Biometric identifiers

Biometric identifiers may be used in addition to conventional identification methods, as they can be faster and more reliable. Traditional methods of identification centre around something one has, such as a token, or driver's license, something one knows, such as passwords, addresses, names, etc. Unlike these, biometric identifiers are part of the person themselves and therefore can’t be forgotten or stolen.[1].

“Biometric capture devices create electronic digital templates that are encrypted and stored and then compared to encrypted templates derived from “live” images in order to confirm the identity of a person. The templates are generated from complex and proprietary algorithms and are then encrypted using strong cryptographic algorithms to secure and protect them from disclosure. Thus standing alone, biometric templates cannot be reconstructed, decrypted, reverse-engineered, or otherwise manipulated to reveal a person’s identity.” [1]

This Technical Specification does not identify the method of recording, or the structure used within the different forms of biometric identification. It provides a structure into which these details could be put to support common usage across healthcare.

Common types of biometric identification include:

- **Fingerprint** records the unique skin pattern of a finger or fingers. These devices capture one or two fingers, creating a template for comparison. This process requires identification of the digit/s to which the image relates. There are two types of fingerprint images appropriate to individual provider identification:
  - **Fingerprint – rolled** are created by rolling each individual finger. “Rolled finger prints generally have sufficient ridge details to allow classification in almost all cases. Rolled fingerprints provide a great deal of information allowing for highly accurate searches. However, capturing a properly rolled fingerprint is a slow process that requires trained staff, and the operator’s manipulation of the subject’s fingers often makes the subjects feel ‘manhandled’” [2];
  - **Fingerprint – flat**, also called ‘plain’ fingerprints. These can be captured quickly using inexpensive scanners by individuals with minimal training. They are more difficult to classify than rolled fingerprints, and often provide a lower quality image than the rolled fingerprint.
- **Facial features** record the shape of the face, determined by distances between the eyes, ears and nose and other facial characteristics which are stored in a template.[3]. This method can identify an individual from many directions and even following changes such as plastic surgery;

- **Voice recognition** operates by recording a specific set of words and the method by which an individual says those words. It considers both pitch variations and timing;

- **Iris** scanning records 247 traits of a person's iris into a template for comparison. It functions with or without glasses, contact lenses;

- **Retinal** scanning records the structure of a person's retina into a template for comparisonn;

- **Hand geometry** records the size and shape of the hand and fingers. Hand geometry evaluates a three dimensional image of the four fingers and part of the hand for comparison. This process requires identification of the hand to which the image relates;

- **Signature dynamics** record not only the shape and style of a signature but the speed and pressure used in the creation of the image;

- **Keystroke dynamics** record the rhythmic elements of keystroke entry;

- **Lip movement** records the movement elements of different parts of the mouth and surrounding structures when specific words/sentences are said;

- **Thermal face image** records heat patterns in the face;

- **Thermal hand image** records heat patterns in the hand;

- **Gait** records a wide range of elements in the body movement when walking, or running;

- **Blood type** records both the blood type and rhesus factor of the blood. This is not a unique identifier but it serves as a suitable additional identifier in healthcare;

- **DNA** records the unique pattern of DNA for the individual.

For full details of biometric identifiers see ISO/IEC FCD 19785-1 *Information technology -- Common biometric exchange formats framework - Part 1: Data element specification* and ISO DTS 22220 *Identification of subject of health care*.

8 Provider organisation identification

8.1 General

Provider organizations can be identified through the combination of data elements shown in Figure 7.

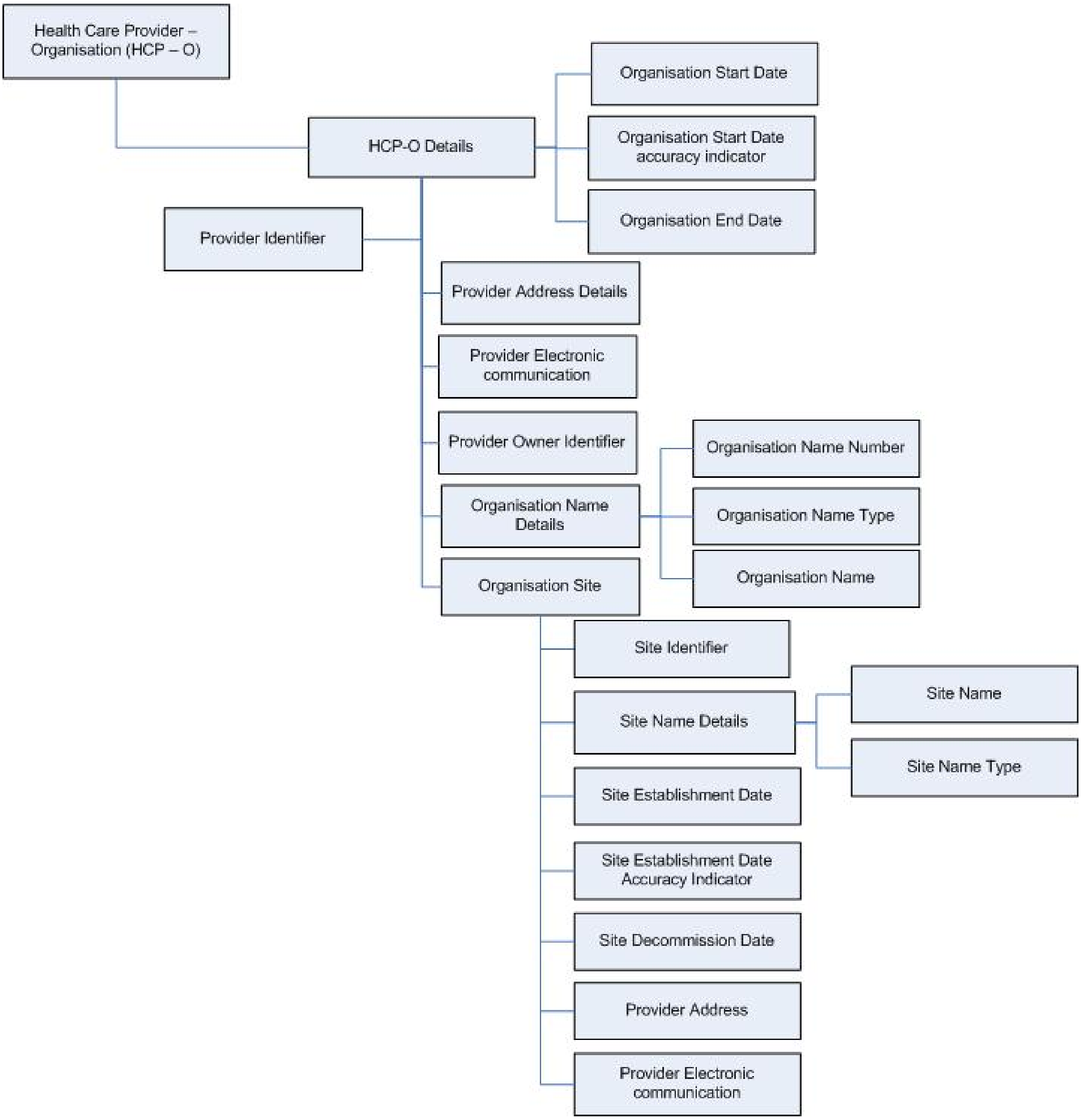

Figure 7 — Structure and components of provider organisation identification

Each provider organisation may exist as a business entity, and as a provider entity. Each organisation may also operate at a number of different physical sites. These concepts are incorporated into the description provided. Table 8 indicates the document sections in which each element is described.

Table 8 — Sections for organisational provider identification

Section	Data element name	Opt.	Data type	Repeat data element
8	**Healthcare provider – organisation**	**R**		**Y**
5	**Provider identifier**	**R**	**Identifier**	**Y**
8.1.1	**Organisation start date**	**R**	**Date**	**N**
8.1.2	**Organisation start date accuracy indicator**	**R**	**Coded text**	**N**
8.1.3	**Organisation end date**	**R**	**Date**	**N**
9	**Provider address**	**R**	**Text**	**Y**
10	**Provider electronic communication**	**O**	**Text**	**Y**
8.1.4	**Organisation owner provider identifier**	**O**	**Identifier**	**N**
8.1.5	**Organisation name details**	**R**	**Text**	**Y**
8.1.5.1	Organisation name number	R	Number	N
8.1.5.2	Organisation name type	R	Coded text	N
8.1.5.3	Organisation name	R	Text	N
8.1.6	**Organisation site**	**O**		**Y**
8.1.6.1	Site identifier	R	Identifier	N
8.1.6.2	Site name details	R	Text	Y
8.1.6.2.1	Site name	R	Text	N
8.1.6.2.2	Site name type	R	Coded text	N
8.1.6.3	Site establishment date	R	Date	N
8.1.6.4	Site establishment date accuracy indicator	R	Coded text	N
8.1.6.5	Site decommission date	O	Date	N
9	Site provider address (see provider address)	R	Text	N
10	Site provider electronic communication (see provider electronic communication)	O	Text	Y

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required (the group may be required, or where the group is optional the individual data elements within the group may be marked as required. In this case, where the group exists the required elements shall be present.
O = Optional (the group or individual data element are optional)

8.1.1 Organisation start date

Definition: The date on which a provider organisation was formally commissioned or created as a legal entity.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date

Data domain: Valid dates

Guide for use: Enter the date using day, month and year.

Verification rules: This field shall be entered and:

- be less than or equal to the field of practice end date (if that date is not blank); and

- be a valid date

Collection methods:

8.1.2 Organisation start date accuracy indicator

Definition An indication of the accuracy of the start date recorded for this organisation.

Source Technical Specifications Australian NHDD (Knowledgebase ID: 000431 Estimated date flag)

Data type Coded text.

Data domain Any combination of the values A, E, U representing the corresponding level of accuracy of each date component of the reported date including:

Code	Description
AAA	Accurate date
EEE	Estimated date
UUU	Unknown date
EAA	Accurate day and month, estimated year
AAU	Unknown day, accurate month and year
UUE	Unknown day and month, estimated year
UUA	Unknown day and month, accurate year

The examples below are for a presentation style DDMMYYYY

Data domain	Date component (for format DDMMYYYY)		
	(D)ay	(M)onth	(Y)ear
Accurate	A	A	A
Estimated	E	E	E
Unknown	U	U	U

Guide for use Used to record the level of certainty or estimation used in recording the individual provider’s address type start date.

Validation rules Any combination of the codes A, E and or U.

Collection method This data element should always be used in conjunction with a field of practice start date.

Comment Most computer systems require a valid date to be recorded in a date field i.e. the month part shall be an integer between 1 and 12, the day part shall be an integer between 1 and 31 with rules about the months with less than 31 days, and the year part should include the century. However, in actual practice, the date or date components are often not known. This means that a date shall be included and it shall follow the rules for a valid date. It therefore follows that, while such a date will contain valid values according to the rules for a date, the date is in fact an ‘unknown’ or ‘estimated’ date. For future users of the data it is essential they know that a date is accurate, unknown or estimated and which components of the date are accurate, unknown or estimated.

8.1.3 Organisation end date

Definition: The date on which a provider organisation is formally closed or ceases to operate.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date

Data domain: Valid dates

Guide for use: Enter the date using day, month and year.

Verification rules: If entered this field shall be:

- be less than or equal to the organisation start date;
- be equal to or greater than the date of decommissioning of all sites associated with this organisation; and
- be a valid date.

Collection methods:

8.1.4 Organisation owner provider identifier

Synonym: Owner identifier

Organisation owner provider ID

Definition: The unique provider identifier for the organisation that legally owns or is responsible for this organisation.

Source standards:

Data type: Identifier.

Data domain: Valid provider identifier with individual or organisational identifier flag of 2 – organisation.

Guide for use: As organisations may be owned by other organisations, this element provides a mechanism to indicate this linkage.

Verification rules:

- If entered this field shall be a valid, current provider identifier with an individual or organisation identifier flag of 2.

Collection methods:

8.1.5 Organisation name details

Organisations may have multiple names. Their formal name used for business purposes, abbreviated or shortened names for marketing.

8.1.5.1 Organisation name number

Definition: The unique identifier of this name for this organisational provider.

Source standards:

Data type: Identifier.

Data domain:

Guide for use: This number is used to reference a specific name as required for the organisation.

Verification rules: This field shall be entered.

Collection methods:

8.1.5.2 Organisation name type

Definition: A code that enables differentiation between an organisation or service location indicative of purpose for communication.

Source standards: HealthNet/BC Provider Data Standard
HL7 (STF-12 *Institution activation date <institution name – alternative identifier*>)

Data type: Coded text.

Data domain:

Code	Description
1	Organizational unit/section/division name
2	Service location name
3	Business name
4	Locally used name
5	Abbreviated name
6	Enterprise name
8	Other
9	Unknown

Guide for use: Code 1 – Used where a business unit, section or division within an organization may have its own separate identity.

Code 2 – Used where the service location name is an important part of the organization name and is used for identification purposes, e.g. Mobile Immunization Unit at Bankstown.

Code 3 – Business name used only for trading purposes.

Code 4 – Used where a local name is used, e.g. where a medical practice is known by a name that is different to the company registration name or business name

Code 5 – A short name or an abbreviated name by which the organization is known, e.g. HIC

Code 6 – Generally, the complete organization name should be used to avoid any ambiguity in identification. This should usually be the same as company registration name.

Code 8 – Used when the organization name does not fit into any one of the categories listed above.

Code 9 – Used when the organization name type is unknown.

Generally, the complete organization name should be used to avoid any ambiguity in identification. However, in certain circumstances (e.g. internal use), a short name (i.e. an abbreviated appellation by which the organization is known) may be used. Further, a business unit within an organization may have its own separate identity; this should be captured (as the unit name).

In cases where the organization is a sole provider, organization name may (or may not) be the same as the personal name.

Verification rules: This field shall be entered.

Collection methods: Multiple organizational names may be collected, each with an organization name type.

8.1.5.3 Organisation name

Definition: The name by which a provider organization is known or called.

Source standards: HealthNet/BC Provider Data Standard
HL7 (STF-12 *Institution activation date <institution name – alternative text>*)

Data type: Text.

Data domain:

Guide for use: Generally, the complete organization name should be used to avoid any ambiguity in identification. This should usually be the same as company registration name. However, in certain circumstances (e.g. internal use), a short name (i.e. an abbreviated name by which the organization is known) or a locally used name (e.g. where a medical practice is known by a name that is different to the company registration name) can be recorded as an additional name. Further, a business unit within an organization may have its own separate identity; this should be captured (as a separate organisation that shares an address or is owned by the 'parent' organisation – whichever represents the actual situation).

Verification rules:

Collection methods: Multiple organizational names may be collected, each with an organization name type.

8.1.6 Organisation site

An organisation site is a physical location at which health services are provided. These data are optional. If the organisation has only one site and that site is the same as the organisation's only address, then no additional information need be recorded.

8.1.6.1 Site identifier

Definition: A unique identifier (for this organisation) of each individual site of the organisation.

Source standards:

Data type: Identifier

Data domain:

Guide for use: The organisation shall establish a unique identifier for each of their sites. This identifier can then be used to uniquely identify the location of service provision.

Verification rules: This value shall be unique for each organizational provider.

Collection methods: A site may have several identifiers for varying purposes – e.g. as assigned by the organization, a funding agency, local government, etc.

8.1.6.2 Site name details

Each site has a name by which it is generally known. This could be a campus name or acronym. The site may have a specific link to a given name for billing or reporting.

8.1.6.2.1 Site name

Definition: A unique identifier (for this organisation) of each individual site, campus or location.

Source standards:

Data type: Text.

Data domain:

Guide for use: Service provision locations or sites often have local names indicating their purpose or location. This might be a campus name, or abbreviation.

Verification rules: This value shall be unique for each organizational provider.

Collection methods:

8.1.6.2.2 Site name type

Definition: A code that enables differentiation between a service location (site) indicative of purpose for communication.

Source standards: HealthNet/BC Provider Data Standard
HL7 (STF-12 *Institution activation date <institution name – alternative identifier*>)

Data type: Coded text.

Data domain:

Code	Description
2	Service location name
3	Business name
4	Locally used name

5	Short or abbreviated name for the site
8	Other
9	Unknown

Guide for use: Code 2 – Used where the service location name is an important part of the organization name and is used for identification purposes, e.g. Mobile Immunization Unit at Bankstown.

Code 3 – Business name used only for trading purposes.

Code 4 – Used where a local name is used, e.g. where a medical practice is known by a name that is different to the company registration name or business name.

Code 5 – A short name or an abbreviated name by which the organization is known, e.g. HIC.

Code 8 – Used when the organization name does not fit into any one of the categories listed above.

Code 9 – Used when the organization name type is unknown.

However, in certain circumstances (e.g. internal use), a short name (i.e. an abbreviated appellation by which the organization is known) may be used. Further, a business unit within an organization may have its own separate identity; this should be captured as an organisation rather than a site.

Verification rules: This field shall be entered.

Collection methods: Multiple site names may be collected, each with a site name type.

8.1.6.3 Site establishment date

Definition: The date on which a provider organisation established this site for service provision.

Source standards: HL7 (STF-12 *Institution activation date*)

Data type: Date

Data domain: Valid dates

Guide for use: Enter the date using day, month and year.

Verification rules: This field shall be entered and:

- be less than or equal to the site establishment end date (if that date is not blank); and
- be a valid date

Collection methods:

8.1.6.4 Site establishment date accuracy indicator

Definition An indication of the accuracy of the provider organisation site establishment date.

Source Technical Specifications Australian NHDD (Knowledgebase ID: 000431 Estimated date flag)

Data type Coded text.

Data domain Any combination of the values A, E, U representing the corresponding level of accuracy of each date component of the reported date including:

Code	Description
AAA	Accurate date
EEE	Estimated date
UUU	Unknown date
EAA	Accurate day and month, estimated year
AAU	Unknown day, accurate month and year
UUE	Unknown day and month, estimated year
UUA	Unknown day and month, accurate year

The examples below are for a presentation style DDMMYYYY

Data domain	Date component (for format DDMMYYYY)		
	(D)ay	(M)onth	(Y)ear
Accurate	A	A	A
Estimated	E	E	E
Unknown	U	U	U

Guide for use Used to record the level of certainty or estimation used in recording the establishment date accuracy. A site may have been established some time ago and it might not be possible to identify the start date with accuracy. In this circumstance this indicator allows the user to identify the accuracy of the date recorded.

Validation rules Any combination of the codes A, E and or U.

Collection method This data element should always be used in conjunction with a site establishment date.

Comment Most computer systems require a valid date to be recorded in a date field i.e. the month part shall be an integer between 1 and 12, the day part shall be an integer between 1 and 31 with rules about the months with less than 31 days, and the year part should include the century. However, in actual practice, the date or date components are often not known. This means that a date shall be included and it shall follow the rules for a valid date. It therefore follows that, while such a date will contain valid values according to the rules for a date, the date is in fact an ‘unknown’ or ‘estimated’ date. For future users of the data it is essential they know that a date is accurate, unknown or estimated and which components of the date are accurate, unknown or estimated.

8.1.6.5 Site decommission date

Definition: The date on which this site was decommissioned for service provision.

Source standards:

Data type: Date

Data domain: Valid dates.

Guide for use: Enter the date using day, month and year.

Verification rules: If entered this field shall be:

- be less than or equal to the site establishment date; and
- be a valid date

Collection methods:

9 Provider address

9.1 General

This section describes the data elements used to capture and store address details for providers of health services, both individual and organisational. The structure outlined in this Technical Specification attempts to simplify data collection whilst capturing the range of addresses and telephone numbers important to establishments. The format of data storage is not as important as the consistent method of recording this data.

Each individual provider address is defined as the combination of data elements set out in Table 9.

Table 9 — Individual provider address data elements

Section	Data element name	Opt.	Data type	Repeat data element	Examples
9	Provider address	R	Text	Y	
9.2	Address line	O	Text	Y	Level 7, room 5
9.2.1	Building/ complex sub-unit type – abbreviation	O	Coded text	N	APT
9.2.2	Building / complex sub-unit number	O	Text	N	6
9.2.3	Address site name	O	Text	N	Treasury building
9.2.4	Floor / level number	O	Text	N	L 3
9.2.5	Floor / level type	O	Coded text	N	B (basement)
9.2.6	Street number	O	Text	N	401A
9.2.7	Lot number	O	Text	N	Lot 52A
9.2.8	Street name	O	Text	N	Mortonville
9.2.9	Street type code	O	Coded text	N	Circuit
9.2.10	Street suffix code	O	Coded text	N	N (north)
9.3	Suburb / town / locality	O	Text	N	Upper Conductor West
9.4	State / territory / province	O	Coded text	N	NSW
9.5	Postal code (zip code)	O	Coded text	N	25300

9.6	Delivery point identifier	O	Coded text	N	
9.7	Country identifier	O	Coded text	N	
9.8	Address type	O	Coded text	N	
9.9	Address type start date	R	Date	Y	19951012
9.10	Address type start date accuracy indicator	O	Coded text	Y	AAE
9.11	Address type end date	O	Date	Y	19951012
9.12	Address end date accuracy indicator	O	Coded text	Y	EUU
9.13	Address security	O		Y	
9.14	Address available to provider	R	Identifier	Y	

NOTE:
Opt. = Indicates whether the data element is optional or required
R = Required (the group may be required, or where the group is optional the individual data elements within the group may be marked as required. In this case, where the group exists the required elements shall be present.
O = Optional (the group or individual data element are optional)

These data elements are listed briefly. For detailed description you should refer to ISO DTS 222200 *Health informatics -Identification of subjects of health care.*

9.2 Address line

Definition A composite of one or more Technical Specification address components that describe a low level of geographical / physical description of a location that, used in conjunction with the other high-level address components i.e. 'suburb / town / locality name', 'postal code', 'state / territory / province', and 'country', forms a complete geographical / physical address.

9.2.1 Building / complex sub-unit type – abbreviation

Definition The specification of the type of a separately identifiable portion within a building / complex, marina, etc. to clearly distinguish it from another.

9.2.2 Building / complex sub-unit number

Definition The specification of the number of identifier of a building/complex, marina etc. to clearly distinguish it from another.

9.2.3 Address site name

Definition The full name used to identify the physical building or property as part of its location.

9.2.4 Floor / level number

Definition Descriptor used to identify the floor or level of a multi-storey building / complex.

9.2.5 Floor / level type

Definition Descriptor used to classify the type of floor or level of a multi-storey building / complex.

9.2.6 Street number

Definition The numeric or string reference number of a house or property that is unique within a street name, suburb.

9.2.7 Lot number

Synonym Section, allotment number.

Definition The lot reference allocated to an address in the absence of street numbering.

9.2.8 Street name

Definition The name that identifies a public thoroughfare and differentiates it from others in the same suburb/town/locality.

9.2.9 Street type code

Definition A code that identifies the type of public thoroughfare.

9.2.10 Street suffix code

Definition Term used to qualify street name sued for directional references.

9.3 Suburb/town/locality

Definition The full name of the general locality containing the specific address of an individual provider.

9.4 State / territory / province identifier

Definition An identifier of the province, state or territory in which an individual provider resides.

9.5 Postal code

Synonym Zip code

Post code

Definition The code for a postal delivery area, aligned with locality, suburb or place for the address of an individual provider, as defined by the postal service.

9.6 Delivery point identifier

Definition A unique number assigned to a postal address as designated by the postal service.

9.7 Country identifier

Definition A code representing the country component of an individual provider’s address.

9.8 Address type

Definition A code representing a type of address.

9.9 Address type start date

Definition The date on which the address type is first applicable to the individual provider

9.10 Address type start date accuracy indicator

Definition An indication of the accuracy of the address type start date at the component level for the date.

9.11 Address type end date

Definition The date on which the address or address type is no longer applicable to the individual provider.

9.12 Address type end date accuracy indicator

Definition The date accuracy indicator for the address type end date.

9.13 Address security

Definition: When an address is not to be openly displayed, except to specific organisations, this flag will be set.

Source standards:

Data type: Boolean

Data domain: Y = this is a secure address not to be made openly available.

N = this is not a secure address and may be made openly available.

Guide for use: Where the flag is Y this is not an openly available address, such as the home address.

Verification rules: The value will be assumed to be N if not entered.

9.14 Address available to provider

Definition: When an address has security set to Y, then only those provider's identified in this field may access this address.

Source standards:

Data type: Identifier.

Data domain: A provider identifier (organisational or provider).

Guide for use: When the address security is set to Y there shall be at least one identifier indicated who may access the address.

Verification rules: May not be blank when address security = Y.

10 Provider electronic communications

10.1 General

This section describes data elements used to capture and store the electronic communication contact details of healthcare providers. Examples of the contact details that may be collected include telephone numbers, or email addresses. Each provider's electronic communication contact detail is defined as the combination of the data elements set out in Table 10. There may be multiple instances of provider electronic communication for any provider, individual or organisation or organisation site.

Table 10 — Individual provider electronic communication data elements

Section	Data element name	Opt.	Data type	Repeat data element	Examples
10	Provider electronic communication	R	Text	Y	
10.2	Electronic communication medium	R	Text	Y	Phone
10.3	Electronic communication usage code	O	Coded Test	Y	Business
10.4	Electronic communication details	R	Text	N	+61 39995555
10.5	Communication privacy	O	Boolean	N	
10.6	Communication available to provider	R	Identifier	Y	
NOTE: Opt. = Indicates whether the data element is optional or required R = Required O = Optional					

Details of each element are available in ISO DTS 22220 *Health Informatics – Identification of subjects of health care*, only the description is provided here.

10.2 Electronic communication medium

Definition A code representing a type of communication mechanism used by a provider.

10.3 Electronic communication usage code

Definition A code representing the manner of use that a person applies to an electronic communication medium.

10.4 Electronic communication details

Definition A unique combination of characters used as input to electronic telecommunication equipment for the purpose of contacting a provider.

10.5 Communication privacy

Definition: When a communication mechanism is not to be openly displayed, except to specific organisations, this flag will be set.

Source standards:

Data type: Boolean

Data domain: Y = this is a secure communication mechanism not to be made openly available

N = this is not a secure communication mechanism and may be made openly available.

Guide for use: This flag allows identification registers to maintain details of ‘silent’ phone numbers and other communication mechanisms that are not to be freely available within the register. Where the flag is Y this is not an openly available communication mechanism.

Verification rules: The value will be assumed to be N if not entered.

10.6 Communication available to provider

Definition: When an address has security set to Y, then only those providers identified in this field may access this communication mechanism data.

Source standards:

Data type: Identifier.

Data domain: A provider identifier (organisational or provider).

Guide for use: When the communication security is set to Y there shall be at least one identifier indicated who may access the communication mechanism.

Verification rules: May not be blank when communication security = Y.

Annex A
(informative)

Implementation

A.1 General

This section of the Technical Specification discusses general issues that may arise in implementation of the concepts within this document. Given the wide range of uses of this Technical Specification this appendix does not prescribe solutions for context-specific implementation issues, as these are more appropriately addressed and resolved within the particular application of the Technical Specification.

This section is designed to assist health information system developers and process managers in implementing ‘best practice’ in provider identification. Many computer systems used for identification in health care were designed according to manual identification processes or in situations where providers were limited to those within a specific organisation; these systems have not been built to meet the needs of the wider applications they now serve. This section:

a) identifies best practice in identification processes, taking advantage of the potential of computer technology;

b) acknowledges the importance of the staff that are part of this process; and

c) recognizes the various needs of different sizes and types of health care delivery systems.

It is recognized that many information systems and current work processes will not be using the systems/technology/processes described in this section at the time of publication, but this is intended to establish a benchmark to which our systems must aspire if they are to serve our needs into the future.

This section comprises sufficient detail and discussion to support the implementation of provider identification in health care.

A.2 Responsibilities

Responsibilities for the capture, storage and use of identifying data for health care providers, should be clearly and unambiguously assigned within the health care establishments, and documented in relevant policies, procedures and work instructions.

A.3 Objective of this section

This section provides guidance and support in the development of quality data collection systems and encourages consistency of procedural approaches to service provider identification. Specific benefits include:

— Assistance to software developers in creating and improving information systems that facilitate data searching, data associations and provider identification;

— Encouragement of standardized search processes, according to data collection size, that improve the health care facility’s ability to find existing provider information in its computer systems;

— Support of semantic interoperability between data collections in different areas of health care, thereby improving comparability of and ease of communication between data sets;

— Improvement of the quality and value of provider identifying data through improved data collection processes;

- Clarification of the issues of provider identification and thereby support staff education activities and procedure development to suit a computerized information system;

- Improved efficiency of the provider registration and identification process at all levels of health care and promote consistency of practice and support the development of provider directory services;

- Improved awareness of principles for the appropriate use of identifying health information and the mechanisms to protect provider privacy;

- Increased accuracy in identifying providers and linking their data across source systems for purposes such as use of professional quality assurance reviews, health system research and health workforce planning.

A.4 Purpose of identification

With the increased use of information technology, many more individual identifiers are being created to satisfy a range of purposes. In health care, unique identifiers are often assigned to facilitate communication of health care information and to directly support the delivery of health services. They may however, also be used for billing, funding, and program management purposes. A key principle for the use of identifiers is that they should only be used for purposes consistent with the context in which they were created. In the context of healthcare, the use of an existing identifier by multiple organisations is a useful technique to simplify communication thereby supporting the purpose for which the identifier is instituted.

The allocation of a unique identifier in itself does not constitute unique identification, unless it is supported by sound business processes to ensure uniqueness and accuracy in the identifier’s assignment. The aim of unique identification is to differentiate between individuals with some or all of the same identifying data. Unique identification can occur with or without a unique identifier. The continuity and effectiveness of patient care across care settings and organisations through electronic communications between care providers and the use of technologies such as electronic health records is greatly facilitated when health care providers can be consistently identified, even though information systems may use different identifiers for the same care provider.

A.5 Primary and multiple identifiers

This section describes how individual providers may have multiple identifiers of different types for a wide range of purposes. For example, a general practitioner may have one or more provider numbers, a prescriber number, one or more state/territory medical registration board numbers, other identifiers associated with the conduct of his/her business, and in some cases, identifiers related to a different field of practice issued by another professional regulatory body. Each of these identifiers clearly has a specific purpose, and some of these identifiers are for restricted purposes.

In general, a single primary identifier should be used in any given application, and this should be an appropriate identifier for the purpose for which it is being used (e.g. assigned by the organization for the purpose of identifying the particular provider). Where there are additional identifiers that are relevant to the provider, these should be collected as other provider identifiers and associated or linked to the primary identifier to facilitate its retrieval.

While this Technical Specification allows for multiple names, address and electronic communication details for individual providers, at least one name, address and set of electronic communication information should generally be recorded in any given application. These details should be those most commonly associated with (or primary to) the particular identifier being used in that application.

A.6 Business processes

Business processes associated with the capture, storage and use of provider identifying data should be designed and continuously improved so as to ensure accurate, consistent and complete data collection and storage practices are used. This section endeavours to indicate how processes can be implemented in a standard manner whilst others will need to be considered at a local level. All policies and procedures should be documented for ongoing reference and staff training purposes. Data should only be linked where there is a business need and supporting regulatory framework.

A.7 Training

All staff responsible for registering new health care providers, or updating existing registration details should receive training that highlights the nature, importance, and health care and business benefits of accurate identification. Training should include information regarding:

- The flow and uses of identifying information;

- The purpose and objectives of searching data;

- Principles and standardized procedures for searching for existing registrations;

- Principles and standardized procedures for registration, including local policies regarding identification and anonymity requirements;

- Quality control feedback and processes;

- Appropriate use of identifying information and the need to protect individual privacy (e.g. familiarization with national privacy requirements).

A.8 Resources

Resources are needed to support the implementation, application and ongoing maintenance of unique provider identifiers. These include human resources, computer systems and support, matching algorithms and accurate ancillary sources of provider data that can be used for verification purposes, and organizational recognition that accurate provider identification is vital to health records and patient care. Different levels and types of resources will be required, depending on the uses of providers identifiers; the degree to which data shall be integrated or communicated across multiple care settings, systems and organizations; and the size, business focus and nature of the organization implementing them.

A.9 Identification of individual provider (s) and/or organization(s)

Sections 1 and 6 explain that identification of ‘providers’ encompasses individuals and organizations. In many instances, identification only of the individual provider is required (for example, reporting of a pathology test result to a specific general practitioner). In other instances, identification only of the organization may be required (for example, identification of a corporate practice located in an area that is accessible by a client). As health care becomes increasingly integrated across care settings and organizations, with the development of electronic health records, telehealth and other technologies, however, identification of both the *individual* provider and the *organization* he/she works for may be required (for example, identification of a medical registrar in a particular public hospital).

The data elements set out in this document are for use as appropriate for the given purpose. It is not necessary to identify both the individual provider and the organization provider in all instances. Where identification only of the individual provider is required, the identification of the organization with which the individual provider is associated does not need to be recorded. Similarly, where identification only of the organization is required, the identification of an individual provider does not need to be recorded.

A.9.1 Identification of health care providers

The identification of health care providers is similar in concept to client identification in that both processes identify individuals. The main difference in identification of health care clients and providers is the relationships of individual health care providers to organizational health care providers. This can be a complex concept. In general, it is recommended that provider organizations be registered as unique entities. Similarly, individuals should then be registered as individual providers. Additional data attached to the individual provider record would include the identification of the organizations within which the individual practices. This could be via a linkage key or could include much more detailed information (such as employment contract details) if required for additional functions, such as a provider register.

A.9.2 Individual client/provider identification characteristics

A.9.2.1 General

An individual (client or provider) is usually identified via a combination of identification details such as sex, date of birth, name, address and/or identifier. It is optimal to collect this data once and reuse as often as possible in accordance with existing privacy or other relevant legislation. The specific information used for identification should be that which is most likely to differentiate this individual from all others registered on a database. The purpose of searching a database should always be to find if the individual is already registered.

NOTE While an individual health care provider may practice in multiple places, with multiple employers, in multiple time frames and in multiple health professions or fields of practices, they should only be registered once for identification purposes – they will simply have multiple associated attributes.

Ongoing processes should be implemented for identifying registrations already on the system that may relate to this individual, particularly if they are registered with some slightly different information (e.g. an old address or a name they no longer use). It is important to both prevent duplicates wherever possible, as well as to have documented procedures for merging duplicated records. If a person is registered again, information previously collected about them will not be associated with the new record, and this may affect the ability to communicate effectively with and identify services provide by the provider.

A.9.2.2 Provider identifiers

Some national, state, provincial or territory laws restrict the adoption or use of certain unique identifiers. As a general rule, health care identifiers should only be used for the purpose for which they are allocated. Where there are a number of identifiers, however it is possible to link each to the one individual.

Health care providers may be assigned one or more of the following identifiers for specific purposes, such as:

- Staff identification code or employee number;
- Health care provider number;
- Medical registration board number;
- Business or taxation number;
- Professional organization membership or license number.

Provider identifiers are uniquely comprised of the following combination of data elements:

- Identifier designation (or person identifier), the actual identifier;
- Identifier geographic area (for client and provider organizations);
- Identifier issuer (or person identifier issuer), assigning health care establishment identifier code or name;
- Identifier type (or person identifier type).

Key principles for assignment of provider identifiers include:

a) Identifiers are of fixed length, and that if they are numeric, the leading zeros are retained;

b) Identifiers incorporate a checking algorithm so as to protect against errors due to (at least) single-character transcription errors;

c) Identifiers are not re-used for different people or organizations, under any circumstance;

d) Organizations issuing identifier numbers should at all times retain a record of information allocated to previously-valid identifiers, and use some sort of (preferably date-based) validity code, rather than define a ‘current list’ by merely removing entries.

A.9.2.3 Name

Providers may use, or be known, by more than one name over time. At any single point in time, a person has:

— a name they are currently known by (referred to as the preferred name in this document);

— a name they are officially recognized by (formal name registered for government, reporting or other purposes; and

— may have one or more other names (names that the person may use colloquially or previously).

All known names should be collected and recorded. The provider’s formal name should always be recorded. Additionally, official reporting names should be captured if different to the formal name, as well as any other names (one or more) that they are, or were, known as. This includes capturing colloquial names (or the name generally used by the provider such as a shortened version of their name used to make communication with clients simpler. Providers may have a professional or business name by which they are known. All these names should be recorded to enable accurate identification of past, current and future information regarding the provider and to assist the use of the name to communicate with health consumers and patients.

The provider name is captured with the combination of the following data elements:

— Name set (each individual name used by a provider represents a name set that may be composed of the following components:

  - Name title (abbreviation): e.g. Rev, Prof.;
  - Name title sequence number: to indicate the first or subsequent name title;
  - Given name: client’s identifying name within the family group;
  - Given name sequence number: the first or subsequent given name;
  - Family name: name in common with other members of the client’s family;
  - Family name sequence number: the first or subsequent family name;
  - Family name type: the type of name (such as family name prefix – such as von, de);
  - Name suffix (abbreviation): e.g. Jnr, MP;
  - Name suffix sequence number: to indicate the first or subsequent name suffix.

— Name usage (which applies to a whole name set): i.e. registered, reporting, newborn, professional or business, maiden or other name;

— Preferred name indicator, indicating which name set is preferred for communication with the provider;

— Name usage start date;

— Name usage start date accuracy indicator;

— Name usage end date;

— Name usage end date accuracy indicator;

— Name conditional use flag: to indicate if the name is unreliable, not for continued use or subject to special privacy or security requirements (indicating conditional information that applies to a given name set).

NOTE Some data elements may have multiple occurrences, for example, name title and given name.

A.9.2.4 Contact details

Organizations collecting health care provider identification information would also always collect the relevant provider’s addresses and phone numbers. In addition, other electronic communication details may also be collected for communication purposes.

A.9.2.5 Address

All current and past (previously recorded) addresses for a provider should be recorded and retained for identification and communication purposes. The addresses that could be collected include:

- Business or office (service delivery) address: one or more would always be collected;
- Mailing or postal address: if different to the business address;
- Temporary accommodation: for providers who normally live overseas but are currently practising in the country to which this standard applies (or vice versa), or who for other reasons, are in temporary accommodation;
- Residential address: where appropriate.

All addresses should indicate the address purpose details (including address purpose start date and address purpose end date).

International address information is usually collected using the following combination of data elements:

- International address line;
- International state/province;
- International postcode;
- Country identifier;
- Address purpose details (including address purpose start date and address purpose end date).

A.9.2.6 Electronic communication details

Other identification contact details that may be recorded for clients or providers include fixed line and mobile telephone numbers, facsimile numbers, pager numbers, email or URL addresses. These are referred to as the ‘medium’ of communication.

Full electronic communication details are therefore collected via the following data elements:

- Electronic communication medium: e.g. phone, fax or pager number, email or URL address;
- Electronic communication usage code: business only, personal only or both;
- Electronic communication details: the actual number or electronic address to be used for communication.

More than one of any of these communication mechanisms may be recorded for any one provider.

A.9.2.7 Other identifying information

Providers may also be identified via a range of other identifying information, some of which may include:

- Sex: male, female, indeterminate/intersex, or not stated/inadequately described;

- Date of birth and date of birth date accuracy indicator: to indicate level of reliability of the date of birth;

- Date of death and date of death date accuracy indicator: to indicate the level or reliability of the date of death;

- Source of death notification;

- Mother's original family name;

- Country (or place) of birth;

- Birth plurality: indicating a multiple birth i.e. twins;

- Birth order: e.g. indicating second of a multiple birth;

- Health care provider field of practice: to indicate the fields of practice or occupation of the practicing provider;

- Field of practice start date, field of practice end date, field of practice start date accuracy indicator and field of practice end date accuracy indicator.

A.9.3 Organization provider identification characteristics

Health care provider organizations are identified using very similar identification data to that used for individuals. They are identified using a combination of:

- Organization identifier: comprising of the identifier designation, identifier geographic area, identifier issuer and identifier type;

- Organization name: comprising the health care provider organization name and name usage;

- Organization address: as per individual address;

- Electronic communication details: electronic communication medium, usage code and details;

- Other identification details: including organization start and end date, organization start date accuracy indicator and organization end date accuracy indicator.

A.9.4 Collection versus exchange

Codes used for data collection via information systems need not be the same codes used for exchange or extraction of data. That is, if users are familiar with certain codes (such as, 'M' as designated for male in the system) for data collection, more accurate data collection may result from using these more meaningful codes. Where alternative codes are used, these should be mapped by the information system to storage codes (such as, '1' as designated for male in the database) for data extraction and subsequent use.

A.9.5 Identification and registration process

The process of collecting individual identifying information and allocating a unique identifier is known as registration. The purpose of registration is to uniquely identify an individual and allocate an identifier in order to link information to that individual according to business needs. The identifier unique to an organization should be used consistently across that organization as the individual's identifier.

Registration is a distinct process, separate from provision of services or employment contracts, though these processes are intimately related. In some instances, identification confirmation may also occur via an identification check using pre-existing documentation to support confirmation of the authenticity of the individual as the person they claim to be.

For providers registering as health care practitioners, the following steps of registration are applied:

Step 1: Identification of the individual provider or organization;
Step 2: Collection of registration details into an information system;
Step 3: Determination of whether the individual, or organization, has been previously registered, by searching the database and reviewing possible matches;
Step 4: Allocation of a (or retrieving a previously allocated) unique identifier;
Step 5: Confirmation of details for previously registered clients, and update of details as required;
Step 6: Quality control review.

A.9.6 Provider registration

Provider registration may be performed to identify health care practitioners that are authorized to provide services and access client information within a health care establishment. Providers that are regulated are registered by regulatory bodies that have the jurisdictional authority to legally permit a health care provider to practice within their jurisdiction, may also be registered in a provider or professional society directory. A health care provider directory is an information system that contains a register of known health care providers. Such a register may be used as a directory to provide information to authorized individuals or organizations on the:

- Identification of one or more health care providers;
- Availability of qualified providers in a geographic area;
- Qualifications, credentials and/or experience of a health care provider;
- Role or scope of work of a health care provider;
- Work locations of a health care provider;
- Contact details of a health care provider.

The type of additional information that could be contained in a provider directory could include, but is not limited to:

- Qualifications;
- Specialties;
- Scope of practice;
- Employment status & location;
- Experience;
- Current practicing status;
- Conditions of practice;
- Registration type and details;
- Special authorizations (e.g. permissions to prescribe certain or restricted medications).

The scope of a provider directory or index can vary widely. Some databases may be limited to a particular type of provider (e.g. physiotherapist graduates) or may have a defined geographic scope (e.g. medical practitioners currently practicing in city Y). Similarly, some databases may include some or all of the non-regulated health care providers and/or complementary health care providers. Examples include naturopaths, homeopaths, and massage therapists.

A.9.7 Registration Issues

Key issues for registration and identification, especially when communicating between information systems include:

- Incomplete or out-of-date information (e.g. limitation of source systems which may only get annual updates);
- Incorrect data capture (e.g. due to communication difficulties or trauma);
- Difficulties experienced by staff collecting the information, especially information perceived by the client or staff to be sensitive;
- Incorrect information or fields marked ‘unknown’ that are provided by the health provider themselves;
- Incorrect recording and transcription errors;
- Failure to capture and/or track changes;
- Failure of the provider/organisation to provide correct, accurate and legible information (e.g. where there is lack of understanding of the information required);
- Inadequate search processes for matching against existing data;
- Differing data capture requirements and mechanisms;
- Provider registration conducted by a separate organization, where the information requirements are different from the needs of the health service;
- Time delays in documentation of provider details and recording into the provider database;
- Inadequate staff training;
- Inadequate staff resources;
- Varying methods of data matching.

Information perceived to be sensitive can be difficult to collect due to:

- Lack of understanding by staff or the provider regarding reasons why the information is collected and how it will be used;
- Reluctance by staff to ask for information perceived to be sensitive;
- Concerns regarding privacy and confidentiality;
- Inconsistent internal collection practices and/or lack of local guidelines.

A.9.8 How to improve registration processes

To improve the accuracy of identifying data, information systems should be able to flag data that is known to be of poor quality or unreliable. This data should be excluded from matching algorithms or protocols.

Organisations responsible for identification should have clearly documented policies, procedures and/or guidelines on their registration process. The process of developing these enables discussion of registration practices, agreement on local business rules, and establishment of consistent documented methods of registering clients. Identification search procedures should take into consideration the population and data sources being searched, as correct searching is the key to accurate registration and identification.

The scope of the policies and guidelines developed could include:

a) Registration procedures;

b) Guidelines to ensure staff understand the importance of valid registration, the rationale for data collection and how the information is used. This includes guidelines on collection, storage, use and disclosure of identifying information in line with relevant privacy legislation. In particular, it is a common requirement to ensure that those people being identified are reasonably aware of the purposes for which their information is being collected;

The use of ‘collection statements’ and other similar processes provide a good opportunity to explain to individuals why their information is required. Good communication can minimize the risks of subsequent concerns about information handling processes. It can also maximize the ability to obtain reliable information, as people will tend to have a better understanding about the importance of ensuring that they can be properly identified, and the fact that this can ensure that they receive communication intended for them, and that processes such as patient referrals occur in a timely manner.

c) Allocation of identifiers;

d) Where providers are registered and by whom;

e) Prepared answers for staff when handling difficult situations and people’s questions;

f) Specification of the tasks included in job descriptions;

g) Guidelines to assist collection of information including useful questions to ask when obtaining or clarifying information when searching an identification database.

Once policies, procedures and/or guidelines are documented, there should a program of staff training, which should include information on:

i) Why people are registered and the benefits to the individuals of the process and data availability;

ii) How the information is used;

iii) Why accurate registrations are important;

iv) What the local business rules are;

v) Where to obtain information;

vi) Tips for effective searching.

Other procedures that could be defined and used for staff training include:

— Registration system operation and troubleshooting;

— Follow up of incomplete data;

— Procedures for managing record merges and un-merges;

— Processes for verifying data with trusted sources (e.g. registration authorities);

— Data update and management including whom to contact if errors are identified and resolving duplicates registrations.

These should be an ongoing competency based training program to support accurate identification and registration of clients. The program should include system application training on non-production versions of the client database application, if available. And importantly, there should be an auditing program to ensure registration data quality and accuracy.

A.9.9 General principles of identification and registration of providers

When identifying a provider the following principles should be applied:

a) Providers should be uniquely identified and registered;

b) When face-to-face contact with an individual occurs, then some form of identity verification should be attempted. An acceptable method of verifying who a person is on the telephone needs to be determined, such as a question and answer session;

c) To protect confidentiality, the individual performing the registration process should not provide identification data to the provider for verification, rather non-leading questions should be asked for authentication purposes. For example, a provider should be asked probing questions, such as, where do you currently live, what was your previous address or on what day and month were you born, rather than asking ‘do you live at “xyz”?’ or ‘is your date of birth “full date of birth”?”;

d) ‘Identification confirmation questions’ and responses can be used to assist identification. These are additional data that are often used to confirm the identity of someone accessing their own data, such as, health data from an information system portal. The types of questions that are commonly offered as options for identity confirmation include ‘What is your mother’s maiden name?’, ‘What is the name of

the street where you grew up?’ or ‘What is your pet’s name?’ These are similar to a personal identification number and can assist in the identification of a provider;

e) A thorough database search shall be performed for all individuals regardless of whether they indicate that they have previously attended/provided a service or have been registered before or not;

f) Key identifying data elements shall match the provider’s current and past demographic details to confirm a previous registration, and be agreed to by the individual;

g) Unique identification numbers should never be re-allocated once assigned;

h) A record of any change to key identifying data elements should be maintained for information audit trail processes;

i) A person master index or provider register shall always be accessible to meet current and future information needs;

j) A planned systematic program of auditing should be undertaken to maintain data quality and assure privacy compliance.

A.9.10 Data collection

When a person’s identifying information changes, the changes should be made in registration systems as soon as the information becomes available. A history of changes should also be retained.

To ensure efficient and accurate individual registration, information shall be gathered using effective interviewing techniques that ask the right questions. Use of effective interviewing techniques is vital to eliciting useful information from clients and protecting their privacy. Such techniques include the appropriate use of closed and open questions, good listening skills, awareness of non-verbal cues (e.g. use of eye contact and appropriate body language), empathy and patience.

Open interrogative questions commence with who, what, where, why, when or how. These open questions are more helpful in obtaining good quality information than closed questions that require only a ‘yes’ or ‘no’ answer. Some probing may be required to clarify information, however, staff should be encouraged not to ask leading, presumptive or multiple (i.e. double-barrelled) questions.

In order to protect the privacy of individuals, the registration screen should be located where it cannot be seen other than by the staff member entering the information. If left unoccupied, no information should be left on the screen. Screen savers should also be used where possible to reduce the chance of casual observation. If required, the registration screen can be shown to the provider to confirm the information contained about them, only when the information on the screen relates to them and only them. The registration screen should not be shown during the searching process, nor should an individual be asked to identify which record on a search output list relates to them. Staff should also ensure that any search list cannot be seen in the background if the registration screen does not hide the search results, in the event that the screen is to be shown to an individual. Useful questions to ask to clarify information, when searching for a person on the database are:

a) What is your family name/surname/last name?

b) What is your given name/first name? A closed question would be ‘Are you Mary Smith?’

c) Are there other ways of spelling your name?

d) Are you commonly known by another name such as a shortening of your name or a nick name?

e) Have you ever been registered as a health care provider before?

f) Are there any alternative or previous names you may have been known by, for example, maiden name or have you changed your name?

g) What is your address? Do not ask ‘Do you live/work at 20 Smith Street,…’

h) What is your mother’s maiden name?

People should not be prompted with any identifying details that may have been found on a search, since doing so provides the individual with information that potentially identifies others who are registered on the identification database.

When attempting to identify an individual, search output may include multiple people with similar identifying information. Careful review of the details of each matching person needs to be undertaken to reduce the probability of creating duplicate records. It may be appropriate in this situation to use a leading question to determine if they have previously lived at a certain address. This can be asked indirectly or generally by asking: Have you ever lived in <suburb>? Then if the answer is ‘yes’, ask: What was your address there?

At the point of data collection, people should be informed about the information collected, how it will be used, where it is held, who has access to it and to whom it may be disclosed. This information may be provided through privacy brochures and handouts.

A.9.11 Searching an identification database

A.9.11.1 General

The purpose of searching a database for an individual is to find an existing registration rather than to confirm that the individual is not in the database. There is a need to find all possible existing registrations or potential matches to ensure that all the appropriate information is associated with the appropriate individual.

Information systems should be designed to accommodate alternative search processes relevant to the population included in the database. For example, searching may be greatly assisted by a search protocol that includes details of registration such as specialty, geographic area of practice (suburb, postcode, or postcode group).

The importance of finding the correct identifier for the provider when needed cannot be over emphasized. Systems shall be searched thoroughly for the provider. If a previous registration cannot be found then, and only then, should a new registration be made and an identifier allocated.

Information systems should not allow a new registration to be created without a prior search being conducted.

Search methodologies are dependent on the logic of the health information system. The following information should be used as a guide in developing policies appropriate for a health care establishment to maximize the likelihood of appropriately identifying providers.

A.9.11.2 Principles

The search criteria chosen should suit your organization and be based upon the following principles.

Principle 1: Include appropriate data for searching so as to not exclude the person for whom you are searching.

a) Search data items need to be highly reliable. If they are not reliable they need to be made more generic. It is more appropriate to restrict the search using highly reliable data elements such as sex or age than less reliable data components.

b) Caution should be used if using given name as an element of the search criteria for the following reasons:

   i) Given names have many different spellings (Catherine with a C or a K) and therefore should usually only be included when applying a ‘sound-alike’ matching protocol. Therefore where a data element is included in a search and that data element is not highly reliable computer algorithms should be used to support finding those individuals likely to be the same as the one for whom you are looking;

   ii) Given names have many variations of the one that might have been used in a system before (Bill or William). Record each alternative name including nick names;

   iii) Given names can be recorded in different sequences, or people can be known by a name other than the first name previously recorded. Search algorithms that match on all names in the string overcome this issue;

   iv) Consider special names, such as ‘baby of’. The search algorithm should match these special names to any given name entered. Any existing entry in the computer system that has a given name of this type should be treated as if the given name is blank for search procedures. The same concept applies to U ‘unknown’ in the sex field, which should match to either M ‘male’ or F ‘female’.

c) Inclusion of given name in the search without any algorithms increases the likelihood of excluding the person for whom you are searching. If the objective is to find the client, it may be more accurate to exclude the given name from the search, but include it in the information displayed for the user to review.

d) Dates of birth can easily be mistyped, and are often not known. To avoid missing the entry because of a numerical typographical error, use date of birth to determine an age range for searching and/or combination of the numbers in the date of birth (that is, 01/05/2004 or 05/01/2004; or 01/05/1980 or 01/05/1990).

e) Ensure that data items such as flags for date accuracy indicator are considered in the search algorithm.

f) If the system allows, ‘and’ plus ‘or’ search criteria should be used.

Principle 2: Consider the variability of the data over time in your population to identify which data items are likely to be assist in finding the entry you want.

a) Data items such as sex, when collected correctly, are highly reliable over time. They are unlikely to exclude the person for whom you are searching, and therefore, make excellent search criteria. Note that a sex-assisted search may be unreliable in circumstances where the sex has been determined from the individual’s name. For example, ‘Kim’ could denote male or female.

b) Elements of a person’s address may be useful in populations that are not highly mobile or where address is a major factor of service provision (for example, in district nursing services Mrs Smith of Bellarine is likely to be key to identifying the person concerned).

Principle 3: Search using accurate data.

a) Information likely to be known by the patient and able to be easily solicited accurately may be useful additions to the search criteria.

EXAMPLE ‘I work with Dr Wilks’, ‘My office is at...’.

Principle 4 Aim to build a search criteria approach that requires only one or two searches. It should be recognised that the health environment is not one where clerical processes are often stressful and given lower priority than direct patient care. In these environments the search process needs to be designed to return all highly likely matches in the first search. Frequently there is insufficient time or clerical resource to undertake multiple searches.

a) Staff are often busy and will rarely go through more than one search to try and find the individual’s registration.

b) When searching, people often assume that if the computer didn’t find it, it isn’t there.

c) Include search algorithms such as ‘sound-alike’ options and other names in a single search process. An exact match search as the first ‘default’ search process is not recommended as this is likely to exclude the individual for whom you are searching and has been shown to lead to duplicate registrations.

d) If too many entries are being returned, staff should know to review the search criteria to include additional reliable data items.

General search principles

The following key identifying data are commonly used when searching for an individual:

- Family name (with sound-alike options or partial matching algorithms);
- Date of birth or age;
- Sex.

In addition, the following identifying data may also be used:

- Other names;
- Health identification number;
- Mother’s original family (maiden) name;
- Residential address or suburb;
- Country of birth;
- Telephone number;
- Date of death.

The following example demonstrates the searching process when one or more of the following are available to the user: name, sex and age/year of birth.

a) Family name, given name, sex, age or date of birth (example: Scholtz, Susan, F, 24). Only exact matches will be displayed;

b) Family name, initial of given name, sex, age or date of birth (example: Scholtz, S, F, 24). All females, with the age five years either side of the age 24, with the family name of Scholtz, and initial of the given name beginning with 'S' will be displayed. This will include variations of spelling of the given name Susan, such as, Sue, Susan, Suzie, Suzanne and/or Susannah;

c) Family name only (example: Scholtz) All clients with the family name of Scholtz will be displayed. The display will include any other given name that Susan SCHOLTZ may have used (for example, middle name as given name) and will pickup any entry that may have been registered under the incorrect sex;

d) Family name—sound-alike assisted. All patients with a family name that sounds similar to Scholtz; such as Schultz or Scholts. Remember that the sound-alike search is not infallible. The sound-alike algorithms follow a defined set of rules to determine whether two names 'sound' the same; there are some circumstances where names that are similar will not have the same sound-alike value. In these cases, they will not be displayed as soundex alternatives.

For people with difficult or long names, the final search should be a search on the first three or four letters of the family name. The system will display all names commencing with the exact letters provided, thus increasing the probability of locating the required record. When searching for an ethnic name, a search should be conducted using any known second given (or middle) names also. This is necessary as the given name of some names may be unfamiliar in the culture in which the system is operating. For example, Thi = Miss and Van = Mr in a Vietnamese name, is not understood in many English speaking cultures. When entering these names into any system, ensure that Thi or Van is entered as part of the given name and also as titles to support effective search processes. This person would therefore have two names in the system.

As the given name and family names can easily be confused, searches should include searching either name in all of the given, middle and/or family name positions. Also note that, a sex-assisted search may be unreliable in circumstances where the sex has been determined from the client’s name for example, ‘Kim’ could denote male or female. Such assumptions should not be made when collecting data, but many existing systems have data contaminated in this way. When searching for ‘common’ names, the client's sex and age should be entered to reduce search time. However, this should not be the only technique used to establish whether the client is known.

Having a comprehensive search procedure and regular staff training is essential to quality data capture. Procedures should also be in place for disaster management situations or for when the information system is not available.

A.9.12 New registrations

A.9.12.1 General

When modifying an individual’s details, information systems should notify the user if there are any potential matches to the new details being entered.

A.9.12.2 Name details

When collecting name details of a new provider, the following principles should apply:

a) Have the provider enter their own demographic details into an information system if facilities enable this;

b) If administration staff are registering a new provider, the new registrant could provide official documentation giving details of their name and/or address so these data are entered correctly, or could write these details on paper so they are captured in the format preferred by the provider. If they are being collected during an interview type situation, the information should be entered and then displayed for the registrant to confirm the spelling and layout;

c) Systems should allow for the collection of multiple names as these support higher quality identification processes as well as reflecting the desire in health care to use names with which those involved in the health care system will be comfortable.

A.9.12.3 Address details

When collecting address details of an individual, the following principles should apply:

a) Each component of the address should be split out in the information system if possible. Some sophisticated systems allow for collection of data as multiple address lines of free text, which are then parsed by the system into the components and then verified;

b) A postcode (zip code) /suburb file should be used to verify the correct combination of suburb and postcode. However, systems should also allow override of suburb and/or postcode in circumstances where the system does not reflect their correct address details. For example, a new suburb and/or postcode that is not available on the current reference file;

c) Where address is collected as free text, it is recommended that a separate line/field be provided for 'building name';

d) Information systems should allow for the collection of multiple addresses (e.g. residential and postal), as well as current and previous addresses.

A.9.13 Identifiers

Health care provider identifiers can be categorized into two levels: primary identifier(s) and secondary identifiers. The primary identifier uniquely identifies the individual and is the most trusted identifier of information from a particular data source. Primary identifiers shall be present for providers within an information system, and they cannot have a null value.

A secondary identifier can be used in conjunction with the primary identifier as a method for further ensuring that the provider is properly identified, and for validating a match with an existing identifier in another system. Secondary identifiers are most often demographic details such as date of birth, sex, given name, and family name.

A second identifier could include a challenge question and response or secret personal identification number (PIN) or password. Examples of identification confirmation questions include: mother's maiden name, or the street you grew up on. An alternative is to provide the individual with access to his/her own data to ensure their identification data is correct and up-to-date.

A.9.14 Properties of a unique identifier

Where unique identifiers are created for a provider, they should satisfy the thirty criteria adapted from the ASTM *Standard Guide for Properties of a Universal Healthcare Identifier* .

A.9.15 Identifier sources

Health care provider identification information can be received from many sources. Some of these sources are direct (information derived directly from the individual) and some are 'second hand' (automated information sent from one system to another via interface), or from professional or work related registrations. Commonly, there is one source within a system that is considered the 'trusted source' of identifying information. This source, usually the primary client registration system, is termed the authenticated source. The authenticated source is the assigner of the primary identifier.

Other sources can also supply provider information. These systems may have received their information from another source (such as professional body registration system).

Health care provider information from an authenticated source can be accepted and acted on directly, due to the trusted nature of these sources. Information received from an unauthenticated source should be accepted in lieu of the absence of information from an authenticated source, but should be verified against the authenticated source at the first opportunity. Unauthenticated source information should only be used as the basis for patient linkage or health care client record merging when an appropriate level of collaboration or agreement has occurred.

A.9.16 Authenticated sources and existing data

A.9.16.1 Authentication of data

A system receiving data from an authenticated source should accept the primary identifier within the data received and attempt to match it to existing data from the same authenticated source (if it exists) within the system. This can be done if the system tracks the source that originally contributed the information along with the primary identifier itself. The same identifier, received from the same source, is an indication that the information relates to the same provider. In addition to the primary identifier, other secondary identifiers (such as sex, date of birth, family name and given names) can be used to further ensure that the identification of this provider is correct.

A.9.16.2 Evaluation of identifiers

Provider identifiers can be evaluated by an information system in several ways. Most often, identifiers are evaluated by requiring a match between the data in the incoming information, and the data element that already exists in the system. This also requires that the data exists both in the incoming information and in the system database.

By default, the primary identifier should be evaluated in this manner. For secondary identifiers, the data will not always be present in either the information received or the existing record in the system. Systems can allow matches if the data is present in both places, or if it is not present in both. Another setting can allow for the data to not be contained either in the incoming information or the system database, but if it is present in both places, it shall match. Systems should also be able to warn if certain data elements are missing from the incoming information, or are present in both places but do not match.

The option to either require a match or warn only provides for a first level of weighting of secondary identifiers. This can actually be taken further by assigning numerical weights (such as 100 for ‘must match’ to 0 for ‘does not have to match’ and any number in between) to the match criteria. It should be noted that with higher levels of match parameters and weighting, more system overhead will be generated, and system performance may be adversely affected. This can usually be justified by the increased accuracy of matching, but does need to be assessed.

A.9.16.3 Matching of information received

When information is received by a system that has already received information about this provider from this source, and the data has been successfully matched, a system should be configurable to handle the new information in a number of ways. In most instances, once positive identification has occurred, the system will simply update the demographic information already in the system. But, in some cases, it is appropriate to replace all existing information with the new information received. In other cases, the existing information is more accurate or more up to date than what is received, and the system will wish to keep existing information. The new information received can either be discarded, or entered into the system as another instance of the provider.

A problem arises when primary identifiers are received by a system from more than one authenticated source. An example of this is a single central system that may have five individual hospitals, all with their own authenticated source and primary identifier. In this case, the receiving system should first attempt to match the provider data with existing data from the same source. If that is successful, it can then be beneficial to attempt to reconcile provider information from one authenticated source with existing information on that same provider from other authenticated sources. This can be done manually, but many systems allow for automated reconciliation.

A.9.17 Confirming provider details

If a search of a provider registration system is successful in identifying an existing registration for that provider, all data recorded on the registration system should be reconfirmed with the provider (if the information is available or the provider is present). It is very important that all details are confirmed at each contact, within reason. This will ensure that correct and current information is available to everybody who may refer to or use this information.

A.9.18 System quality management processes

Procedures need to be established for the registration of clients when electronic information systems are not available and for disaster management. A designated block of provider identifiers should be set aside for allocation during computer downtime and/or in the event of an external disaster.

In instances of computer downtime, a search should be undertaken using back-up systems (e.g. a copy of the registration system data on microfilm or a freestanding desktop computer) to determine provider information, in the case of a need to refer a patient or send data to a provider. However, when the computer system is back online, it is extremely important that a search is undertaken of the register to determine if the details were correct.

Registration systems and directories typically have well-established security processes and procedures to prevent access to data by unauthorized clients or staff and to record or log details of who has had access to the client/provider identifying information.

A.9.19 Data quality management processes

Data of variable quality is very often matched against other data of variable quality, often leading to considerable imprecision.

Data collected may be of poor quality because of:

- Factors influencing data capture including communication difficulties at the point of collection;
- Recording and transcription errors;
- Changes to key identification information that are not recorded;
- Incomplete searching of existing registration data.

Sound and consistent data collection processes are the basis of accurate data matching and linkage. Accurate identification of providers is reliant on thorough searching processes and consistent methods of registration. A structured quality assessment process to review data quality is highly recommended. Where data is being linked or being used for clinical care, it is vital that data be accurate and that this be measured and monitored regularly.

It is recommended that data be validated at the point of data entry and not on filing of the whole record. In particular, data used to link provider information should be validated at the field level rather than at the function or screen level. This will assist in assuring collection of quality data. Accuracy flags add additional information to support data linkage and allow for exclusion of inaccurate, unreliable or unknown data values from the data matching process. It is also recommended that all the critical data fields have flags to indicate both the quality, the date last verified, checked or updated, and start and end dates where applicable.

The nature of identification of individuals is such that errors are likely to continue to occur, no matter how careful staff are in searching and number allocation. Routine reports and data management processes should be established to identify duplicate registrations. This may include automated and/or manual processes. The resolution of these ‘duplicates’ should follow an agreed process. The processes recommended in this document will reduce these duplicates but processes need to be in place to assist in finding duplicates and to resolve these duplications when they are found.

Systems should check daily all new entries into the database using algorithms to identify any existing entries in the system that might be duplications of the new entries. Manual review of these cases should be done daily and where it is established that a case is not a duplicate this should be recorded in the database, and where the cases are determined to be duplicates these should be ‘merged’ where one identifier (usually the most recent one) is ‘retired’. The retired identifier stays in the computer system but is marked as retired and the unique identifier that is to be retained is clearly identified.

Changes made to an individual’s identification should be recorded by any health information registration or service provision information system. The old identifying information (e.g. name or address) should be retained, with the new correct information being captured as the current identifying details. Acceptable error rates should be determined by each organization and measured for compliance.

A.9.20 Identifier data quality

In some cases, identification numbers of eight or more characters are used. The most accurate method of capturing these numbers is via an automated process such as ‘swipe card’ technology. Where identifiers are captured manually, the risk of data entry error increases with the number of characters.

To improve the data quality of lengthy numeric identifiers, check digits can be employed as a validity check. The check digit is the digit at the end of the number, which is derived using an algorithm based on the other numbers within the identifier. One example of a check digit system, as suggested by AS 3523.1, Identification cards—Identification of issuers—Numbering system is the Luhn formula. This system is based on ANSI X4.13, and is also known as the modulus 10 ‘double-add-double’ check digit.

In order to generate the Luhn formula check digit, the following steps are taken:

Step 1: Double the value of alternate digits beginning with the first right-hand digit (low order);
Step 2: Add the individual digits comprising the products obtained in Step 1 to each of the unaffected digits in the original number;
Step 3: Subtract the total obtained in Step 2 from the next highest number ending in 0. This step is the equivalent of calculating the ‘tens complement’ of the low order digit (unit digit) of the total. If the total obtained in Step 2 is a number ending in zero (i.e. 30 or 40) the check digit is 0.

EXAMPLE Identifier number without check digit 4992 73 9871

Steps

4 9 9 2 7 3 9 8 7 1 1

X2 X2 X2 X2 X2

18 4 6 16 2

4 + 1 + 8 + 9 + 4 + 7 + 6 + 9 + 1 + 6 + 7 + 2 = 64

2 70 - 64 = 6 3

Identifier number with check digit 4992 73 9871 6.

Therefore, the number is validated at the point of data entry using the appropriate formula.

A.10 Privacy and security

Users of this Technical Specification should refer to relevant privacy legislation, codes of fair information practice and other guidelines so as not to breach personal privacy in their collection, use, storage and disclosure of provider information, including any consent requirements. Privacy legislation may require users to consider their particular set of circumstances (i.e. location and sector) and whether privacy legislation covers those circumstances. Provisions in health professional legislation and regulations shall also be considered when unique provider identifiers and any subsequent identifiable information is collected, stored and shared.

Individual provider identification details are personal information. These details shall be only collected where there is a legitimate need to identify providers and their personal and business information shall be maintained in a confidential manner**.**

It is also important to secure and safeguard the information to prevent unauthorized disclosure. Appropriate security measures shall be employed to protect the person-identifiable/sensitive information contained within each organization holding unique provider identifiers.

Consideration shall be given to who has access to unique identifiers (i.e. are they public numbers or private-system numbers) and actions to be taken in cases of fraud shall be considered. Any data matching and linkage procedures shall respect both privacy legislation and professional regulatory provisions.

A.10.1 Data matching

For provider identifiers to be linked, the identifying data about the provider needs to be matched. Data may be matched in one of two ways:

a) Deterministic matching—is where data is only matched where identifying information (such as family name, initial of first given name, date of birth and sex) are identical;

b) Probabilistic matching—is where weights are assigned to identifying data elements to identify whether two records are a true match, a non-match, or a highly probable match.

These techniques/approaches are not mutually exclusive. Errors can easily occur when matching data as there can be:

i) False non-matches or Type I Errors—which is failure to match identifying data which is associated with the same individual; these errors create duplicate records; or

ii) False matches or Type II Errors—which is where records are matched but are in fact not associated with the same individual; these errors are called overlays.

Whenever data linkage involves the use of identifying personal information, providers shall ensure that this use of the information is permitted under the privacy laws that apply to them. If the information has been collected by the organization from the individual for the purposes of providing health care, and the linkage is being performed for this purpose, then ordinarily it will be permitted by such laws as it is being used for the purpose for which it was collected. When the information is being linked for other purposes, the legal authority to use the information in the manner proposed should be ascertained.

A.10.2 Process of data linkage

The selection of appropriate primary and secondary identifiers, and the configuration of provider match and reconcile parameters within a system shall be assessed individually by each health care establishment, based on the number and authenticity of sources, and the quality of the data collected for the identifier itself. Below is a partial list of questions that should be asked as part of the health care client identifier design process:

— What is the frequency of availability of each of the demographic fields being considered as identifiers?

— What is the level of trust of the data collected in the identifier field?

— How does each health care client identifier field rate in comparison to the other identifiers (for example, date of birth may have a greater weight than sex)?

— What is the reliability and consistency with which this identifier is present, and correct, for a given person?

— Is the data collected for this identifier a ‘free text’ field, or do users select from a predefined, codified set of reference data?

Below are some general recommendations for the weighting of certain identifiers:

— Family name should be weighted more heavily than given name, due to the variations that can occur with given name;

— First given name should be weighted more heavily than the second and subsequent given names (if second and subsequent given names are used);

— Date of birth should be weighted more heavily than sex.

And below are some general recommendations on the level and degree of person match:

- Weighted searches, particularly where large databases of provider details exist, often take up more system resources and can impact the system's overall performance. It is generally best to do weighted searches only when necessary, and not on information received from authenticated sources;

- All systems should, if possible, make demographic data elements that are selected as provider identifiers required or mandatory fields. Users should pick the values for these fields from a codified 'drop down' list. Free text fields should be avoided.

Therefore, the configuration of an identification system to effectively identify health care providers, match them to existing health care client records and reconcile across multiple sources of provider information is individual to each health care entity. Often, the parameters selected and the configuration of the match and reconcile will not prove to be optimum from the initial design. It is critical that any configuration be tested thoroughly prior to implementation.

Bibliography

[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Technical Specifications*, 2001

[2] ISO/IEC TR 10000-1:1998, *Information technology — Framework and taxonomy of International Technical Specification Profiles — Part 1: General principles and documentation framework*

[3] ISO 10241:1992, *International terminology Technical Specifications — Preparation and layout*

[4] ISO 128-30:2001, *Technical drawings — General principles of presentation — Part 30: Basic conventions for views*

[5] ISO 128-34:2001, *Technical drawings — General principles of presentation — Part 34: Views on mechanical engineering drawings*

[6] ISO 128-40:2001, *Technical drawings — General principles of presentation — Part 40: Basic conventions for cuts and sections*

[7] ISO 128-44:2001, *Technical drawings — General principles of presentation — Part 44: Sections on mechanical engineering drawings*

[8] ISO 31 (all parts), *Quantities and units*

[9] IEC 60027 (all parts), *Letter symbols to be used in electrical technology*

[10] ISO 1000:1992, *SI units and recommendations for the use of their multiples and of certain other units*

[11] ISO 690:1987, *Documentation — Bibliographic references — Content, form and structure*

[12] ISO 690-2:1997, *Information and documentation — Bibliographic references — Part 2: Electronic documents or parts thereof*

[13] *National Health Data Dictionary*, Australian Institute of Health and Wellfare, 2007

[14] AS 4400-1995, *Personal privacy protection in information systems*

[15] AS 4590-2006, *Interchange of client information*

[16] AS 4700.1-2005, *Implementation of Health Level Seven (HL7) Version 2.4 – Patient Administration*

[17] AS4846 *Provider identification*

[18] AS/NZS ISO/IEC 17799, *Information technology – Security techniques – code of practice for information security management*

[19] AS/NA 17799.2 Part 2, *Specification for information security management systems,* ASTM

[20] E1714-00, *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*, ASTM

[21] Australian Institute of Health and Welfare (1998). *HACC Data Dictionary, Version 1.0 (May 1998).* Commonwealth Department of Health and Family Services, Canberra.

[22] HB 222-2006, *Australian Subject of Care and provider identification implementation guide*

[23] HICKLIN,R& READY, C *Implications of the IDNT/IAFIS Image Quality Study for Visa Fingerprint Processing*, Mitretek Systems, 2002

[24] HL7 V2.4, *Health Level Seven Standard Version 2.4: Health Level Seven Inc*., Ann Arbor.

[25] HNBC 98-10, *HealthNet/BC Provider Data Standard Version 1.0*

[26] IBIA Biometrics Overview

[27] ISO 10646:2003, *Universal multiple-octet coded character set (UCS)*

[28] ISO/IEC 11179-2005, Information technology—Metadata registries (MDR)

[29] ISO/IEC 11179-3:2005, *Information technology—Metadata registries (MDR) - Registry meta-model and basic attributes*

[30] ISO/IEC 19785-1:2006, *Information technology – Common biometric exchange formats framework-Part 1: Data element specification*

[31] ISO/IEC 19785-2:2006, *Information technology - Common biometric exchange formats framework-Part 2: Procedures for the operation of the Biometric Registration Authority*

[32] ISO/IEC 2022:1994, *Information technology – Character code structure and extension techniques*

[33] ISO DTS 21091 Health informatics: *Directory services for security, communications and identification of professionals and patients*

[34] ISO DTS 22600-1, *Health Informatics – Privilege management and access control – Part 1: Overview and policy management*

[35] ISO DTS 22600-2, *Health Informatics – Privilege management and access control – Part 2 Formal models*

[36] ISO 3166-1:2006, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*

[37] Centrelink, *Naming Systems of Ethnic Groups: Ethnic Names Condensed Guide.* Canberra: Centrelink, 1997.

[38] SPENCE, B. *Biometrics' Role in Physical Access Control,* Loss Prevention and Security Journal, 2003

[39] ASTM E1714-95, *Standard Guide for Properties of a Universal Healthcare Identifier (UHID)*

[40] Department of Human Services South Australia, *Client Identification Data Standards. Volume Two: Identification and Registration Procedures – Hospital Standards Only,* 2003

[41] Huffman E. K. *Medical Record Management*. Physicians' Record Company, Berwyn. 1981

[42] ISO/TS 21091:2005, *Health informatics -Directory services for security, communications and identification of professionals and patients*

[43] NSW Health: *Client Registration Standard.* Version 1. NSW Health, July 2004

[44] Standards Australia: AS 3523.1—1998, *Integration cards – Identification of issuers Part 1: Numbering system.* Standards Australia, Sydney.

[45] Standards Australia: AS 5017—2006, *Health Care Client Identification*. Standards Australia, Sydney.

[46] Standards Australia: AS 4846—2006, *Health Care Provider Identification.* Standards Australia, Sydney.