Introduction	NSQHS
Provides direction to assist staff to manage patients/clients who require or request protection of their clinical information and/or identity whilst encouraging optimal documentation standards	Governance for safety & quality in health service organisations

Reference: *Management of patient/client requests to withhold identity for registration (in Electronic Health Information Systems) and treatment purposes*

Introduction

In general, in the absence of special circumstances, it is not recommended that patients/clients be treated without identifying themselves to the health service due to the reduced availability of information for continuity of care, and the difficulty with data matching and integration in information management systems. Patients/ clients should be counselled as to the implications of withholding their clinical information. Relevant instances when a request may be considered include:

- Staff being treated by their employing health facility
- Witness protection
- Clients at risk from potential visitors
- Court and intervention orders
- Patient / clients under police guard
- Patient / clients in custody
- Infamous/Famous/Very important persons (VIP)

Managing Service Requests

1. Client's requesting their file not be visible to another person or persons (i.e. CHIME Service Request confidentiality level to be raised to PARTIAL or FULL and possibly the use of a Secure Org Unit). This means that only staff working in that service or service stream can access and view the file.
   See Section 1 of this Document "Client has requested Confidentiality Level other than Standard"

2. Client has requested to be anonymous in receiving service i.e. file remains anonymous/withhold their identity by way of:

   - Alias in CHIME (Not appropriate for security of file), or
   - New Identity in iPM and CHIME (Needs to handled carefully in iPM so as file merging does not occur, e.g. pattern matching on Medicare Number) or
   - No Provision of Service.

   See Section 2 of this Document Client has requested anonymity/withhold information

Monitoring Access

Service Managers are required to monitor Secure Org Unit access and Inappropriate Access to Client CHIME Records

See Section 3 of this Document "Monitoring of Inappropriate Access and Security Audit Requests"

SECTION 1 - Client has requested Confidentiality Level other than 'Standard'

Have you discussed the 'NSW Health Information on Privacy Leaflet for Patients' and the 'Your Rights and Responsibilities as a client, patient or visitor' Leaflet with your client?

NO

Inform the client about the collection, use and disclosure of their personal health information.
Refer to: Script for discussing CHIME Confidentiality with Clients

Provide a copy of Leaflets: 'Your Rights and Responsibilities as a client, patient or visitor' and 'NSW Health Information Privacy'

Complete the Privacy Rights and Responsibilities Assessment Tool in the Clients CHIME Record.
The Privacy, Rights and Responsibilities must be discussed, and the Assessment Tool completed for each Service Request.

YES

After discussion and Privacy Leaflets provided, has the client requested increased Confidentiality Levels in CHIME greater than 'Standard?'

NO

NO - Nil Changes Required. Confidentiality should remain at Standard
A request for increased Confidentiality Levels in CHIME must be made by the client or if deemed necessary by an appropriate representative for the client.

YES

Attempt to find out why the client or an appropriate representative for the client wants to change their Confidentiality Level in their CHIME record.

Reassure the client that all CHIME users and HNELHD Health Employees are bound by the law & duty of confidentiality as well as the protection of health information under the HRIP Act.

All HNELHD staff are bound by the Act and by NSW Health Privacy Manual for Health Information.

Is a change to the Service Request Confidentiality Level in CHIME still required?

NO

No Changes to be made to the Confidentiality Level in CHIME for this Client

YES

Option 1
PARTIAL Confidentiality

Option 2
FULL Confidentiality

Record the Request for increased confidentiality using the Clinical Note Template: "***AA(All)Request for Increased Confidentiality in CHIME***"

Discuss the request and recommendations with the Service Manager.

The Service Manager documents their response to the ***AA(All)Request for Increased Confidentiality in CHIME*** in a clinical note then changes the Confidentiality Level in CHIME, if required and Submits requests a transfer to a Secure Org Unit if required

SECTION 2 - Client has requested anonymity/withhold information (Before proceeding, The Clients Privacy, Rights and Responsibilities must been discussed and documented as per **SECTION 1** of this document)

Assess the Individual Request
Each request must be assessed on an individual basis by the treating practitioner and the following factors must be discussed with the client:

- Does the client require **follow-up** and, if so can this safely occur if the request is granted?
- Is the client being seen by a **multidisciplinary team**, and, if so, will it be difficult to refer and coordinate care if the request is granted?
- Is the information being withheld substantial enough to **compromise the safety** of the client in care or their health service provider?
- Whether the **Health Service liability** may be increased
- Does **identification have to be provided** in order to access services (e.g. Medicare Card, Department of Veteran's Affairs services)?
- Does a **prescription for a restricted substance** require the name of the recipient?
- Has the client been diagnosed with a **scheduled medical condition** under the Public Health or Mental Health Act that must be reported?

Does your client fall into one or more of the above categories?

NO

Attempt to discover why the client wants to remain anonymous

Depending on the reasons given the following options should be offered in the first instance:

- Reassure the client of the law & duty of confidentiality as well as the protection of their health information under the HRIP Act.
- Where the service records information is held electronically on CHIME, inform client that their record can be raised to PARTIAL (preferable) or FULL confidentiality. This means that only staff working in that service or Service Stream can access and view the clinical record. (See **SECTION 1** of this document)
- Offer the use of an 'alias' that is still linked to the client's true identity.
- Client can be moved to a CHIME Secure 'VIP' Org Unit (used mainly for Mental Health & DACS Services where Data Sharing is given for all MH)

Does the client still wish to protect their clinical information and identity?

NO

Service Manager monitors inappropriate access. See **SECTION 3** of this document.

YES

Refer to Policy: **Draft only-not yet endorsed by ELT**
Management of patient/client requests to withhold identity for registration (in Electronic Health Information Systems) and treatment purposes

YES

The request to protect their identity must be declined on that basis. The treating health professional must explain to the client the reason(s) for refusal of the request and clearly document these in the patient's health record.
If the client does not accept the outcome then a meeting with the District Manager Records Privacy and Information Security records should be convened.

SECTION 3 - Monitoring Access

Secure Org Units

These have been specifically created to enable the segregation, when necessary, of Service Requests which meet point 1 of Managing Service Requests, from Service Streams which have Data Sharing Access to all the standard Org Units across the stream. These are used when the client is related to or is a member of the treating team or there is a foreseeable risk that the information may be accessed inappropriately. Only nominated treating provider(s) should have access to this Org Unit

Monitoring of Inappropriate Access

A monthly report is distributed for Secure Org Units that identifies Data Sharing Access by anyone other than the treating team to the Service Request.

The Service Manager must review this to ensure there is no inappropriate access given (i.e. Staff who have left the service and no longer require Data Sharing Rights for that Org Unit) and submit requests to remove these Data Sharing Rights using the 'Data Sharing Rights' self-help form

Service Managers/Team Leaders for all service types should run RAP Report 'Active Incumbencies by Org Unit' to ensure their Org Unit staffing is up to date in CHIME. The CHIME Self-Help form 'End Date a Position for Existing Provider' should be submitted to remove staff from positions in CHIME for which they are no longer in.

Security Audit Request

The CHIME Database is a secure electronic client health record with personal and clinical client data stored therein. Access to this data is covered by various Policy Directives and Guidelines including Privacy, Confidentiality, and Registration.

Part of the role of the CHIME Support Team is to be responsible for compliance with:

- Policy Directives,
- Appropriate access to Client/Organisation/Provider/System Data,
- Appropriate access to Application functionality,
- Determining appropriate access to data stored in the CHIME Database via
    - User Interface "front end" application usage
    - Data Base tables "back end" data querying
    - Reports accessible via the application
    - Reports accessible via an external Interface

Managers may request an audit should there be a reasonable concern that the above policies have been breached.

CHIME Security Audit Requests are followed up and actioned by the CHIME Support Team Manager and District Manager Records Privacy and Information Security