Justice Health and
Forensic Mental Health Network

Justice Health NSW Policy

Patient Mail – Forensic Hospital

Issue Date: 04 May 2023

[redacted]

Together for
Healthier Tomorrows

Policy title

Policy Number 5.016

Policy Function Safe Practice and Environment

Issue Date 04 May 2023

Next Review Date 04 May 2026

Risk Rating

Summary This policy sets out guidance for the Forensic Hospital staff on the processes to ensure that mail sent from or received by patients does not pose a threat to the safety or security of any individual or organisation.

Responsible Officer Insert Responsible Officer position (must be an Executive Director)

Applies to

☐ Administration Centres
☐ Community Sites and programs
☐ Health Centres - Adult Correctional Centres or Police Cells
☐ Health Centres - Youth Justice Centres
☐ Long Bay Hospital
☒ Forensic Hospital
Other: Justice Health Administration Centre (JHAC)

CM Reference POLJH/5016

Change summary Updated Mental Health and Cognitive Impairment Forensic Provisions Act 2020. Revised process for privileged correspondence and unit-based security stamps. Updated definitions of exempt bodies as per relevant Act.

Authorised by Chair, Policy Steering Committee

Revision History

#	Issue Date	Number and Name	Change Summary
1	Mar 2013	5.016 Patient Correspondence – Forensic Hospital	New policy.
2	Dec 2014	5.016 Patient Correspondence – Forensic Hospital	Updated legislations, policies and procedures. Updated position titles.
3	Aug 2017	5.016 Patient Correspondence – Forensic Hospital	Updated policies and procedures.
4	Aug 2020	5.016 Patient Mail – Forensic Hospital	New policy title. Amended policy to safeguard security of the hospital and public health and safety in response to patient outgoing mail. Incorporate recommendations from mail security breach investigation.
5	May 2023	5.16 Patient Mail – Forensic Hospital	Guidance for Forensic Hospital staff on processes to ensure mail sent from or received by patients does not pose a threat to safety or security

Always refer to the electronic copy for the latest version.

Justice Health and Forensic Mental Health Network
PO BOX 150 Matraville NSW 2036
Tel (02) 9700 3000
http://www.justicehealth.nsw.gov.au

1. Table of Contents

2. Preface

The purpose of this policy is to inform Justice Health and Forensic Mental Health Network (Justice Health) staff of the legal requirements stated in Section 117 of the *Mental Health and Cognitive Impairment Forensic Provisions Act 2020* (the Act) regarding the security conditions for patients. The NSW Health PD2012_50 *Forensic Mental Health Services* also requires each secure mental health facility to have a procedure for preventing the entry of dangerous items into the facility; the searching of patients; their belongings and rooms; and the inspection of postal items entering or leaving the facility.

This policy provides direction to staff in relation to:

- processes which enable staff to monitor, intervene and safely manage all mail (Refer to Section 4 Definitions) in order to protect the security of the Forensic Hospital (FH) and to prevent psychological or physical harm to a patient, staff or any member of the public; and
- Security conditions.

As far as possible all patient privacy should be maintained. Where it is necessary to enact these security conditions, staff are expected to treat legitimate mail appropriately, and not use or disclose any personal information contained in the mail that is not relevant for managing any safety and security risk or required for clinical purposes.

3. Policy Content

3.1 Mandatory Requirements

This policy applies to all staff, visitors, contractors and patients including correctional patients by the operation of the security conditions protocols made with Corrective Services NSW (CSNSW) and Youth Justice NSW (YJNSW) and to any person(s) detained in the FH under the *Mental Health Act 2007*.

Justice Health has a statutory duty to provide a therapeutic and safe living and working environment for patients and staff, and to protect the public. To achieve and maintain a safe therapeutic environment, the inspection of mail within the FH is an essential element of security. This includes not only protecting others from the consequences of the patients' activity, but also protecting patients from their own actions (e.g. drugs) and preventing / deterring others from supplying illicit and prohibited items, which may pose a risk to security or safety.

Risk management is an important function in safeguarding the health, safety and security of staff, patients and the public. Assessment, planning and review processes should routinely include arrangements for delineating, measuring and evaluating rehabilitative outcomes. Where it has been identified that a patient poses a risk to the security of the FH or may cause harm to self or others due to the receiving or sending of mail, the Multidisciplinary Team (MDT) must assess this risk and implement the most effective control measures which are reasonably practicable in the circumstances and ensure that control strategies remain effective over time through periodic and routine reviews. These measures must include that in addition to opening and inspecting mail to ensure that the mail does not contain any prohibited items or substances, designated staff must also read the content and/or withhold

mail from a patient as per documented Clinical Risk Assessment and Management (Refer to Section 3.3).

The power to inspect, open, read and withhold mail is enabled by the power contained in Section 117 of the Act and this policy. Section 117 of the Act, provides discretionary authority to the Secretary of the Ministry of Health (the Secretary) or an authorised delegate, to subject a forensic patient to any security conditions that the Secretary [or delegate] considers necessary. These conditions can authorise subjecting an individual patient to more stringent conditions in relation to sending or receiving mail, including a complete ban, if the authorised delegate is satisfied that the restriction is necessary for any reason associated with security or public safety.

To safeguard security of the FH and public health and safety, and in order to comply with the Act and the NSW Health PD2012_50 *Forensic Mental Health Services*, Justice Health must implement procedures for preventing the entry of dangerous items into the facility, the searching of patients, their belongings and rooms, and the inspection of postal items entering or leaving the facility. In the FH, the inspection of postal items will include the opening, reading and inspecting all mail, unless the mail is classified as privileged correspondence (Refer to Section 4 Definitions).

The Chief Executive may authorise the FH staff to open, read and inspect privileged correspondence, if this is required to safeguard the FH and public health and safety.

All patients must be assessed by the treating team for risk in relation to receiving and sending mail, including patient to patient mail. This individual risk assessment will determine the level of monitoring of the mail required for each patient (Refer to Section 3.3).

In addition to opening and inspecting of all mail, the following two security conditions must be implemented and followed at all times:

1. Patients are strictly prohibited from having the following mail items in their possession:
    - Justice Health branded envelopes;
    - Pre-paid envelopes;
    - Postage stamps.

Justice Health staff must provide plain blank envelopes when requested by patients. Patients must place all outgoing mail in an unsealed envelope provided by the Justice Health.

2. All mail must be withheld immediately if identified as containing:
    - Prohibited items;
    - Non-approved items; or
    - Does not comply with the provisions of this policy.

Prohibited items include:

- any item or substance which, in the opinion of G4S Security or Justice Health staff is likely to threaten the operational management or security of the FH;
- threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or to incite fear;

- any item or substance that could constitute a risk to state or national security, including material which may be connected to or used for terrorist activities;
- any item or substance that, in the opinion of G4S Security or Justice Health staff, is intended to facilitate, incite or be used in connection with any unlawful activity;
- any item or substance which is prohibited by a law of the Commonwealth, a State or Territory from being sent through the post. This includes any poison, drug, weapons, dangerous goods, any object with a sharp edge or point such as needles, any powder, chemicals or hazardous item; and
- may not be appropriate for postage and, in an opinion of the Justice Health staff, may not comply with Australia Post *Dangerous and Prohibited Goods and Packaging Guide*.

A list of prohibited items can also be found in the FH Procedure *Prohibited and Controlled Items – Forensic Hospital*.

3.2 Roles and Responsibilities

3.2.1 Chief Executive and Executives

Have a duty to exercise due diligence to ensure that the business complies with the *Work Health and Safety Act 2011* and *Work Health and Safety Regulations 2017*.

The Chief Executive and Executives must ensure that:

- Provisions of this policy are implemented;
- Provide direction regarding opening, reading and inspecting privileged correspondence, if this is required to safeguard security of the FH and public health and safety;
- Sufficient resources are allocated and available to ensure the requirements of this policy are able to be met; and
- The Work Health and Safety management system provides for periodic auditing of this policy to ensure compliance and relevance with industry best practice.

3.2.2 Director of Nursing & Services, FH (DNS)

Have a duty to ensure that the provisions of this policy are implemented. The DNS must ensure that:

- All Justice Health staff, contractors and visitors comply with the requirements of this policy;
- Adequate resources are available where required to enable compliance with this policy and to allow for implementation of effective risk minimisations controls;
- Actively promoting and encouraging a culture of risk management, including documented risk assessments, throughout the FH operations;
- Risks to health and safety are eliminated and/or reduced to as low as reasonably practicable;
- Consultation occurs with workers and other stakeholders when making decisions about eliminating or minimising risks in the workplace;

- Mail safety issues are escalated to the Co-Director Forensic Mental Health (Operations);
- Suspicious mail is opened, inspected and read, if there are reasons to believe it may contain prohibited or non-approved items, or contain threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or to incite fear;
- Suspicious privileged mail and other issues related to privileged correspondence that could create alarm or to incite fear are escalated to exempt body / person for advice on how to proceed;
- Advice received in relation to mail has been withheld, including reading the mail and approving it for posting if it does not contain any obscene, abusive or threatening material is acted upon; and
- Patient appeals against the decision to mail are reviewed.

3.2.3 Clinical Director, FH (CD) is responsible for:

- Ensuring implementation of this policy;
- Actively promoting and encouraging a culture of risk management, including documented risk assessments, throughout the FH operations;
- Suspicious mail is opened, inspected and read, if there are reasons to believe it may contain prohibited or non-approved items, or contain threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or to incite fear;
- Escalating mail safety issues to the DNS; and
- Assigning appropriate ground access suspensions and restrictions for the duration of investigation and/or until improvements in patient's clinical presentation will reduce a risk of mail security breaches (Refer to Policy 1.249 *Leave, Ground Access and SCALE Forensic Hospital*).

3.2.4 Manager Security and Fire Safety, FH (MSFS), Deputy Director of Nursing, FH (DDON) and After-Hours Nurse Manager, FH (AHNM) are responsible for:

- Overseeing, monitoring and reviewing all aspects relating to patient mail;
- Responding to mail security breaches;
- Opening, inspecting and reading of suspicious mail, if there are reasons to believe it may contain prohibited or non-approved items;
- Advising Justice Health Administration Centre (JHAC) Mail Room staff about mail restrictions imposed on a patient;
- Directing the destruction or disposal of mail where both the recipient and sender cannot be identified;
- Escalating mail safety issues, e.g. privileged mail security risks and potential risk to public health and safety, to the DNS;
- Coordinating health responses during security breach; and
- Liaising with NSW Police Force (NSWPF) and other Emergency Services.

3.2.5 Nursing Unit Manager, FH (NUM) is responsible for:

- Ensuring compliance with this policy by all staff;

- Ensuring adequate staffing and resources are assigned to enable compliance with this policy;
- Ensuring plain blank envelopes and Registered Post, if appropriate, are provided to patients;
- Implementing unit-based 'Mail Security Stamp', 'Confidential Privileged Information' stamp, 'Incoming Patient Mail Register' and 'Outgoing Patient Mail Register';
- Ensuring the processes outlined in this policy are carried out consistently;
- Receiving and acting on advice that mail has been withheld, including inspecting the mail in accordance with established procedures;
- Contacting the exempt person or organisation when there is a reasonable concern about privileged correspondence;
- Ensuring that a detailed handover relating to identified issues with suspected mail is provided to all members of the MDT and comprehensive documentation is maintained;
- Escalating mail safety issues to the DDON, AHNM and MSFS; and
- Coordinating health responses and taking a role of a DLIC during security breach.

3.2.6 Care Coordinator (CC), FH or delegate nominated by MDT is responsible for:

- Reviewing and clarifying Treatment and Management Plan (TPRIM) for any mail restrictions or identified risks;
- Obtaining plain blank envelopes without a postage stamp from the Ward Clerks and providing them to patients;
- Opening and inspecting all mail, with exception to privilege correspondence, prior to giving to a patient or posting approved mail;
    - In addition to the above, the CC/delegate must read the mail if it is documented in TPRIM that patient's mail may contain threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or to incite fear (Refer to Section 3.3).
- Ensuring all outgoing mail has recipient's full details and address;
- Obtaining the unit-based 'Mail Security Stamp' and 'Confidential Privileged Information' stamp for privileged correspondence from the Ward Clerk;
- After the inspection, ensuring all outgoing mail has been sealed and stamped with the unit-based 'Mail Security Stamp' on the back of the envelope (Refer to Appendix 7.1);
- Ensuring all incoming and outgoing mail details are recorded in the unit-based mail register (Refer to Appendix 7.2 and Appendix 7.3) and sending outgoing mail to the JHAC Mail Room for posting;
- Reporting any mail issues to the NUM, DDON, MSFS or AHNM immediately; and
- Recording all mail security issues and incidents on the Incident Management System (ims+).

3.2.7 Ward Clerk, FH is responsible for:

- Safekeeping of the unit-based 'Mail Security Stamp', 'Confidential Privileged Information' stamp and the mail register books;
- Ordering and providing plain blank envelopes without a postage stamp to the CC/delegate when requested; and
- Ordering and providing Registered Post to the CC/delegate when requested and approved by the NUM.

3.2.8 MDT is responsible for:

- Assessing the likelihood that mail may contain prohibited or non-approved items and advising the NUM if a risk is identified;
- Nominating a delegate for overseeing implementation of specific patient mail restrictions;
- Documenting all aspects of patient care, including but not exclusive to the risk of mail security breach and developing TPRIM; and
- Implementing all aspects of the treatment plan.

3.2.9 G4S Security staff are responsible for:

- Overseeing all aspects of permitter security in a safe, efficient, consistent and timely manner without compromise to the high security environment;
- Scanning and examining of all incoming and outgoing mail in the Security Reception or Sally Port;
- Ensuring that all mail is examined and scanned for the presence of prohibited and non-approved items or substances, or for evidence that it has been deliberately damaged, tampered or interfered with;
- Ensuring that mail is not allowed to enter or leave the FH until examination and scanning are completed;
- Advising the relevant unit about any issues in relation to mail, including, but not limited to, outgoing mail missing unit-based 'Mail Security Stamp' (Refer to Appendix 7.1);
- Separating the suspicious mail into an allocated tub;
- Ensuring all incidents involving mail containing prohibited items, which may cause harm to public safety, are reported immediately to the LIC; and
- Securing the area and ensuring the preservation of evidence during mail security breach.

3.2.10 Social Worker, FH (SW) is responsible for:

- Processing all postal remittances, as prescribed in Section 3.4.5; and
- Contacting the AHNM or MSFS/delegate to secure cash in the FH's After Hours Pharmacy safe.

3.2.11 Justice Health Courier is responsible for:

- Collecting mail from Australia Post and delivering it to JHAC Mail Room for processing and sorting;
- Delivering sorted mail to the FH (i.e. patient mail sorted and separated from staff mail);

- Providing incoming mail to G4S Security for examination and scanning prior to delivering it to the relevant unit;
- Collecting outgoing mail from the units and providing it to G4S Security for examination and scanning;
- Returning outgoing mail that did not pass G4S Security examination and security scanning back to the relevant unit; and
- Delivering approved outgoing mail to JHAC Mail Room for posting.

3.2.12 JHAC Mail Room staff are responsible for:

- Receiving, processing, recording and sorting mail (i.e. separating incoming patient mail from staff mail);
- Notifying the relevant unit about any issues related to mail (e.g. missing unit-based 'Mail Security Stamp'; unsealed envelopes; mail in Justice Health branded envelope; ineligible writing; incomplete recipient's details);
- Acting on advice about restrictions imposed on a patient; and
- Not accepting hand-delivered mail from FH staff attempting to post mail on patient's behalf.

3.2.13 All Justice Health staff are responsible for:

- Complying with the requirements of this policy; and
- Reporting all incidents on ims+.

3.3 Clinical Risk Assessment and Management

Care coordination, assessment, planning and review of patients are continual processes from admission through to transfer and discharge. All information in relation to the care planning process must be comprehensively documented in the patient's health record and TPRIM. Refer to *Clinical Risk Assessment & Management (CRAM)* – FH procedure and Policy *1.078 Care Coordination, Risk Assessment, Planning and Review FH* for more information.

If upon admission, during scheduled review process or if the treating consultant or the MDT is at any time made aware of a risk that the patient is compromising security and safety of the FH or public, then all mail to or from the patient, including privileged correspondence, must be withheld immediately until further notice. A recommendation regarding the patients ongoing mail management or proposed restrictions of the patient's right to send or receive mail must be made to the DNS and CD as soon as reasonably practicable.

Where a clinical risk assessment identifies that a patient poses a risk to the security of the FH or may cause harm to self or others by receiving or sending mail, the MDT should implement strategies to mitigate the identified risk. These strategies must be documented in the patients' health record and TPRIM. Strategies to mitigate this risk may include, but are not limited to:

- with exception to privileged correspondence, reading all incoming and outgoing mail based on risk assessment of psychological harm to others; or
- limiting the amount of mail the patient can receive or send; or

- restricting the patient from receiving or sending mail from or to a certain person or organisations; or
- withholding all mail; or
- restricting the patient from receiving or sending mail for a period of time.

The MDT must inform the DNS and CD of the risks and outline the strategies to mitigate them. The DNS must inform the Co-Director Forensic Mental Health (Operations) of high risk patients and the management plan in place to manage this risk. The decisions, conditions or directions which affect the right of the patient to send or receive mail, must be documented in TPRIM and complied with by all staff directly involved in provision of clinical care for the patient.

3.3.1 Circumstances in which incoming mail must be withheld and read

Incoming mail must be withheld and read by CC/delegate if:

- it is documented in the patients TPRIM to do so to mitigate prior identified risks; and
- it is in the interest of the safety and wellbeing of the patient; or
- it is for the protection of staff or any other person; or
- the content of the mail relates to the possible commission of a criminal offence; or
- it is documented in TPRIM that the mail may contain threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or to incite fear; or
- it was obtained by deception (i.e. using fake names; obtaining mail from someone else); or
- it contains or suspected to contain prohibited or non-approved items or substance.

If withheld mail is written in non-English language, an interpreter must be utilised to translate the content (Refer to FH Procedure *Interpreter Services*).

3.3.2 Circumstances in which outgoing mail must be withheld and / or read

Outgoing mail **must** be withheld and / or read by CC/delegate if:

- it is documented in the patients TPRIM to do so to mitigate prior identified risks; and
- it is likely to cause distress or to incite fear to the addressee or to any other person; or
- using a postal or similar service to make to another person a threat to kill or threat to cause serious harm and intends the recipient of mail to fear that the threat will be carried out (Section 471.11 *Criminal Code Act 1995*); or
- using a postal or similar service to menace, harass or cause offence that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive (Section 471.12 *Criminal Code Act 1995*); or
- causing a dangerous article to be carried out by a postal or similar service (Section 471.13 *Criminal Code Act 1995*); or
- it is likely to cause danger to staff or any other person; or
- it relates to the possible commission of a criminal offence; or

- it has been formally requested by a member of the public, family member, friend, carer or any organisation including a privileged body that they do not wish to receive mail or that the mail must be screened for abusive and threatening behaviour or material that may incite fear from the patient; or
- contains threatening, offensive, obscene or abusive written or pictorial material or items that could create alarm or incite fear; or
- contains or suspected to contain prohibited or non-approved items or substance; or
- patient attempted to post or helping someone else to post their mail by deception (i.e. using fake recipients details; deliberately concealing mail's content in order to be posted to someone else other than recipient).

If withheld mail is written in non-English language, an interpreter must be utilised to translate the content (Refer to FH Procedure *Interpreter Services*).

3.4 Incoming Mail

3.4.1 JHAC Mail Room – processing incoming mail

All incoming mail is collected from Australia Post and must be processed and sorted (staff's mail separated from patient's mail) by the JHAC Mail Room prior to providing mail to the Justice Health Courier (Courier). Refer to Policy 2.021 *Courier & Postal Services* for more information.

[redacted]

[redacted]

3.4.3 Unit-based Inspection and Documentation

- The CC/delegate must open and inspect the mail for the presence of prohibited or non-approved items.
- The CC/delegate must document the receipt of mail and completion of inspection in the unit-based 'Incoming Mail Register' prior to releasing the mail to the patient (Refer to Appendix 7.3).

3.4.4 Withholding Incoming Mail

- When the CC/delegate finds a concealed prohibited or non-approved item or suspecting that they mail may contain an item which can cause security and safety risk to staff and patients, the mail must be withheld and isolated immediately.

- Where there is concern that the mail is not safe to be inspected or there is an imminent threat to the safety of staff or any other person (e.g. concealed unknown substance or possible hazardous material; concealed weapons; etc), the LIC, MSFS and the relevant NUM must be notified as soon as reasonably practicable. If required, the LIC will initiate Level 4 (Containment) as per Policy 5.017 *Management of Emergencies*.
- Where a prohibited item or possible hazardous material has been discovered, the mail must be quarantined at the location of the incident and must be handled in accordance with the FH Procedure *Prohibited and Controlled Items*.
- The LIC must determine the options for safekeeping of mail whilst the matter is investigated. Refer to the FH procedures *Patient Property and Valuables* and *Prohibited and Controlled Items* for more information.
- The NUM must ensure where mail is withheld, that the patient and the sender are advised in writing of the reason and of their right to appeal as soon as reasonably practicable.
- Where mail has been withheld the CC/delegate must complete the following:
    - ims+ report; and
    - eProgress Notes.

3.4.5 Postal Remittances

The processes which must be followed when cash, postal orders or cheques are contained in mail sent to a patient are:

- Cash must be returned to the sender. The cash should be securely stored in the FH After Hours Pharmacy room until it can be appropriately dealt with by the SW in the first instance. After that, the following must be carried out:
    - Where the recipient is known, attempts must be made to obtain the sender's contact details/return address to return the cash;
    - Where the recipient is known, but the return details cannot be obtained, cash must be stored securely and documented in the patient's property record by the SW. If the sender's details are confirmed at a later date, the SW must attempt to return the cash and to document it in the patient's property record;
    - Where cash is received and the recipient and sender are both unknown, the cash must be transferred to Patient Accounts. It may then be deposited into the designated Justice Health 'Samaritan Fund' (Refer to Policy 2.124 *Patient Trust Accounts*);
    - Cheques and postal orders must be provided to the SW, who will complete Patient Trust Accounts FIN420 form with the patient. Only authorised staff are permitted to facilitate patient trust account transactions (Refer to Policy 2.124 *Patient Trust Accounts* and FH Procedure *Patient Property and Valuables* for more information).

3.5 Outgoing Mail

3.5.3 Unit-based Inspection and Documentation

- Following a request to send mail, the CC/delegate will obtain a plain blank envelope or appropriate packaging from the Ward Clerk, and then provide it to the patient.

- The CC/delegate must supervise the patient placing the items inside the envelope and writing the recipient's and their details on the envelope (Refer to Appendix 7.1).
- The CC/delegate must inspect the mail, including privileged correspondence, in the presence of the patient to ensure nothing is attached or concealed that is illegal, dangerous or destructive.
- The envelope must be sealed by CC/delegate immediately after completing inspection and placed in designated area for posting.
- Privileged mail is exempt from being read. However, the CC/delegate needs to observe the patient placing the items inside the blank envelope and writing the recipient's details. Privileged mail may be further inspected once the envelope is closed by running fingers down the envelope to illicit the presence of prohibited or controlled Items.
- If a clinical risk assessment has determined that the mail may cause psychological harm to others or incite fear and should be read to determine this, then, with exception of privileged correspondence, the CC/delegate must also read the content (Refer to Section 3.3.1).
- As part of clinical assessment, the CC/delegate should also consider the risk of patients attempting to send mail via a 3rd party or another patient by deception. Where mail has been posted or has been attempted to be posted via a 3rd party or another patient, the CC/delegate must complete the following:
    - ims+ report; and
    - eProgress Notes.
- Where the items need to be sent in a package, the CC/delegate must inspect the items prior to sealing the package to ensure that the items do not contain anything that is capable of causing injury or damage.
- Once the CC/delegate has determined that the mail is cleared for mailing, they must stamp the back of the envelope or package with the unit-based 'Mail Security Stamp' (Refer to Appendix 7.1, point A). By stamping the mail, the CC/delegate is confirming all the above steps have been completed and the mail is safe, as far as can be ascertained, to be posted.
- In addition to the unit-based 'Mail Security Stamp', the front of privileged mail envelope must be stamped with 'Confidential Privileged Information' to identify privileged correspondence (Refer to Appendix 7.1, point B). This is to ensure that privileged mail is not opened and/or read, unless it was required as per this policy and documented risk assessment.
- The CC/delegate must place the mail in the unit's patient outgoing mail tray and record the mail details in the unit-based 'Outgoing Mail Register' (Refer to Appendix 7.3). Patient outgoing mail must be sorted (staff's mail separated from patient's mail) by unit's staff prior to providing mail to Courier.
- Patient mail without the unit-based 'Mail Security Stamp' or incomplete recipient's details and address, will not be accepted by the Courier. Incomplete patient mail will not be collected.

- The CC/delegate must not hand-deliver any mail to the JHAC Mail Room. All mail must be processed as outlined in this policy. Hand-delivered mail will not be accepted by the JHAC Mail Room staff and this will be recorded as an incident on ims+.

3.5.4 Internal Patient to Patient mail

- The suitability of the internal mail between patients, including mail addressed to patients held in custody of CSNSW or YJNSW, must be reviewed and assessed by treating teams, to determine if any restrictions are required. If approved, this should be documented in eProgress Notes and TPRIM.
- In addition to inspecting mail, clinical staff may read internal mail if they have a reason to believe or it was documented in TPRIM that the mail could present a psychological risk to another patient (Refer to Section 3.3).
- If prohibited or non-approved material or substance is detected when the mail is opened, then the staff must ensure that the item(s) are securely stored as soon as possible and in accordance with the FH Procedure *Prohibited and Controlled Items*. When dealing with mail, staff must be vigilant at all times to ensure the patients cannot access prohibited or non-approved items.
- This withholding must be documented in eProgress Notes and TPRIM. The CC/delegate must notify the NUM or AHNM (out of business hours) and the MDT as soon as reasonably practicable and complete ims+ report.

3.5.5 Withholding Outgoing Mail

- Where the clinical risk assessment identifies that a patient poses a risk to security and safety of the FH or public, or may cause harm to self or others, the MDT should implement strategies to mitigate the identified risk.
- Where the CC/delegate finds concealed prohibited or non-approved items, or there is a concern about the content, the mail must be withheld and removed from the patient for safekeeping as per FH Procedure *Prohibited and Controlled Items.*
- Where there is concern that the mail is not safe to be further inspected or there is a health and safety concern (e.g. concealed unknown substance; presence of potentially hazardous material or weapons; or if it relates to the possible commission of a criminal offence), the LIC must be contacted immediately. If required, the LIC must initiate Level 4 (Containment) and determine if the mail can be safely disposed of or provided to the emergency services (Refer to Policy 5.017 *Management of Emergencies*);
- Where the CC/delegate finds threatening, offensive, obscene or abusive written or pictorial material, or if the mail is not matching the recipient's details, or an attempt to post or help someone else to post their mail by deception (i.e. using fake recipients details; deliberately concealing mail's content in order to be posted to someone else other than recipient), the CC/delegate must not accept the mail from the patient, including privileged correspondence. This must be documented in patient's eProgress Notes, logged on the ims+ and the treating team must complete a clinical risk assessment and review patient's TPRIM.
- The NUM must ensure where mail is withheld, the patient is advised in writing of the reason and of a right to appeal as soon as reasonably practicable.
- Where mail has been withheld the CC/delegate must complete the following:

- ims+ report; and
- eProgress Notes.

3.5.6 Request to Stop Mail from Recipient

- Any person or organisation inclusive of privileged bodies may formally request Justice Health that communication to them by a specified patient is to be ceased or to be read prior to posting. When this occurs, the NUM of the relevant unit must be advised as soon as reasonably practicable.
- The NUM must then inform the DNS/MSFS/CD about the request.
- The NUM must ensure that any mail from that patient addressed to the person or organisation making the request is withheld until further notice or read first if requested, or returned back to patient.
- An entry must be made in the patient eProgress Notes and TPRIM updated with this restriction.
- MSFS or delegate must ensure that Patient Information Records Centre (PIRC) is updated and JHAC Mail Room staff is notified about this restriction.
- The patient concerned must be given written notice by the NUM that any mail sent by or on behalf of the patient to that person will be withheld from the date of the notice and dealt with by direction of the MDT.

[redacted]

3.5.8 JHAC Mail Room – processing outgoing mail

- All outgoing mail will be collected by the Courier and processed by the JHAC Mail Room.
- The JHAC Mail Room staff must check the outgoing mail to ensure it contains ‘Mail Security Stamp’. Any patient mail that does not comply with this requirement must be returned back to the relevant unit.

3.6 Patient right of appeal

- A patient has a right of appeal against a decision to withhold any incoming or outgoing mail unless the mail concerned contained a prohibited item or is the subject of a police investigation, or the addressee has requested that the mail from the patient should be withheld by Justice Health.
- The patient must be informed by the CC/delegate of their right to appeal by writing to the NUM.
- The NUM will consider how to proceed by taking into account the patient’s ground of appeal, the patient’s clinical risk assessment, documented TPRIM, the views of the MDT, the CC and where appropriate, the MSFS.
- On finalising a decision on the appeal, the NUM must provide the patient with a notice in writing of a decision on the appeal together with brief reasons for the decision.

- Where the NUM's decision is to still withhold the item complained of, the NUM should include notification to the patient of a further right of appeal to the DNS and how to lodge that appeal.
- The patient may appeal the NUM's decision to continue withholding the mail by writing to the DNS within 14 days of the receipt of the decision.
- The DNS should take into account all relevant matters in making a decision on the appeal.
- On finalising a decision on the appeal, the DNS must provide the patient with a notice in writing of the result of a decision on the appeal together with brief reasons for the decision.
- The DNS should also provide to the patient a notice in writing setting out that the patient has a further right of appeal to the NSW Civil and Administrative Tribunal (NCAT) and/or make a complaint to the NSW Ombudsman.

4. Definitions

Mail

In this policy, 'mail' includes email, facsimiles, letters or packages and any other postal materials, which are posted to or by a patient. Mail may arrive at the FH in different ways, such as:

- standard or courier delivery by Australia Post;
- other commercial courier;
- Corrective Services NSW and Youth Juvenile NSW;
- visitors; and
- facsimile, computer or any other communication medium.

Mental Health Review Tribunal

The Mental Health Review Tribunal is a specialist quasi-judicial body constituted under the Mental Health Act 2007. It has a wide range of powers that enable it to conduct mental health inquiries, make and review orders, and to hear some appeals, about the treatment and care of people with a mental illness.

Must

Indicates a mandatory action required to be complied with.

Privileged Correspondence / exempt body / exempt person

Mail is privileged correspondence if it is addressed to or from:

- the NSW Ombudsman
- the Commonwealth Ombudsman
- the Mental Health Review Tribunal
- the Mental Health Advocacy Service (Legal Aid NSW)
- the Law Enforcement Conduct Commission

- the Health Care Complaints Commission
- the NSW Civil and Administrative Tribunal (NCAT)

In accordance with Crimes (Administration of Sentences) Regulation 2014 – REG 3, Clause 3

- **"exempt body"** means:

(a) the Ombudsman, the Judicial Commission, the New South Wales Crime Commission, the Law Enforcement Conduct Commission, the Anti-Discrimination Board, the Civil and Administrative Tribunal, the Independent Commission Against Corruption, the Inspector of Custodial Services, the Privacy Commissioner, the Information Commissioner, the Legal Aid Commission, the Legal Services Commissioner or the Legal Services Tribunal, or

(b) the Commonwealth Ombudsman, the Australian Human Rights Commission or the Australian Crime Commission.

- **"exempt person"** means a Member of Parliament, a legal practitioner or a police officer.

Reasonably Practicable

Is a legal requirement for employers. Employers and business (and other Person Conducting Business or Undertaking) always need to try to eliminate, so far as is reasonably practicable, any health and safety risks in the workplace.

Risk Management

The process of identifying hazards, assessing risks and eliminating or controlling risks in the workplace.

Should

Indicates a recommended action to be complied with unless there are sound reasons for taking a different course of action.

5. Related documents

Legislations	*Australian Postal Corporation Act 1989* *Crimes (Administration of Sentences) Regulation 2014 – REG 3* *Criminal Code Act 1995* *Health Records and Information Privacy Act 2002* *Mental Health Act 2007* *Mental Health and Cognitive Impairment Forensic Provisions Act 2020* *Ombudsman Act 1974* *Privacy and Personal Information Protection Act 1998* *Work Health and Safety Act 2011* *Work Health and Safety Regulations 2017*

Justice Health NSW Policies, Guidelines and Procedures	1.078 *Care Coordination, Risk Assessment, Planning and Review Forensic Hospital* 1.249 *Leave, Ground Access and SCALE Forensic Hospital* 2.021 *Courier & Postal Services* 2.030 *Incident Management (ImpG)* 2.124 *Patient Trust Accounts* 5.002 *Access to the Forensic Hospital* 5.017 *Management of Emergencies – Forensic Hospital* 5.110 *Work Health and Safety* 5.135 *Security Risk Management* *Clinical Handover* – Forensic Hospital procedure *Clinical Risk Assessment & Management (CRAM)* – Forensic Hospital procedure *Interpreter Services* – Forensic Hospital procedure *Patient Property and Valuables* – Forensic Hospital procedure *Prohibited and Controlled Items* – Forensic Hospital procedure *Searches* – Forensic Hospital procedure *Work Health and Safety Risk Management – Hazard Identification, Risk Assessment and Control* procedure
Justice Health NSW Forms	FIN420 Patient Trust Accounts Deposit FH022 Incoming Patient Mail Register FH023 Outgoing Patient Mail Register
NSW Health Policy Directives and Guidelines	PD2012_50 *Forensic Mental Health Services* PD2020_047 *Incident Management*

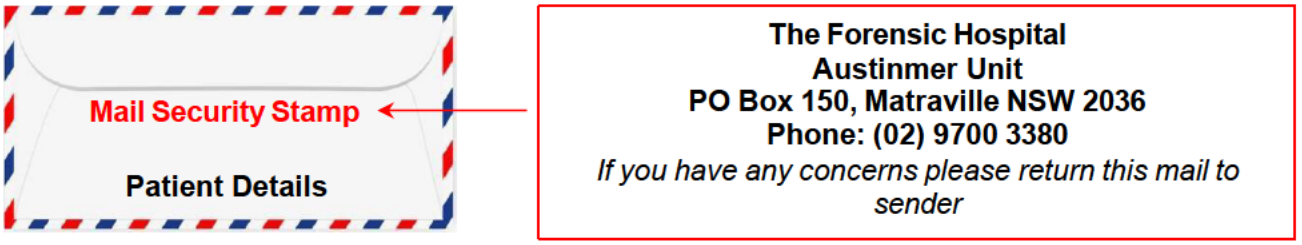
6. Index

7. Appendix

7.1 Unit-based mail security stamp

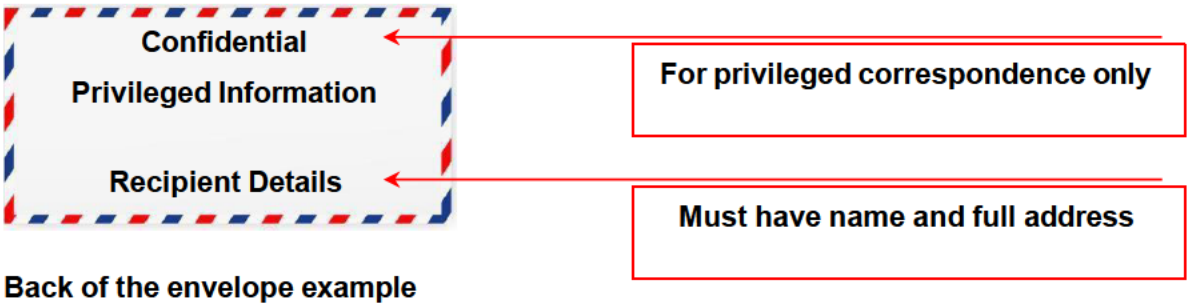
A. Front of plain blank envelope without postage stamp example

Back of the envelope example

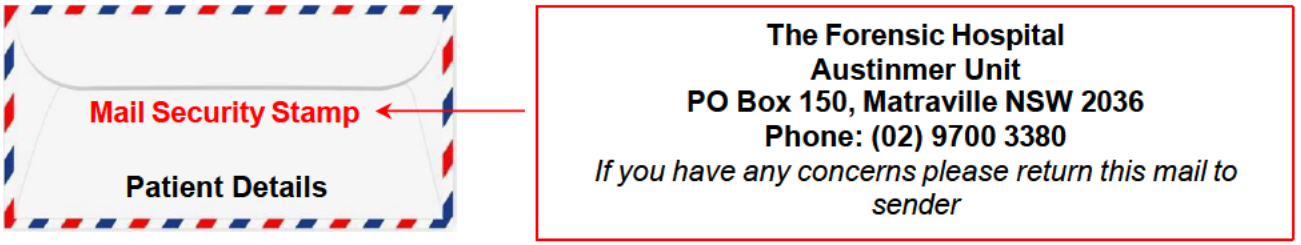


Note: Do Not post mail without unit-based 'Mail Security Stamp'.

B. Front of Privileged Correspondence envelope without postage stamp example



Back of the envelope example



Note: Do Not post privileged mail without unit-based 'Mail Security Stamp' and 'Confidential Privileged Information' stamp.

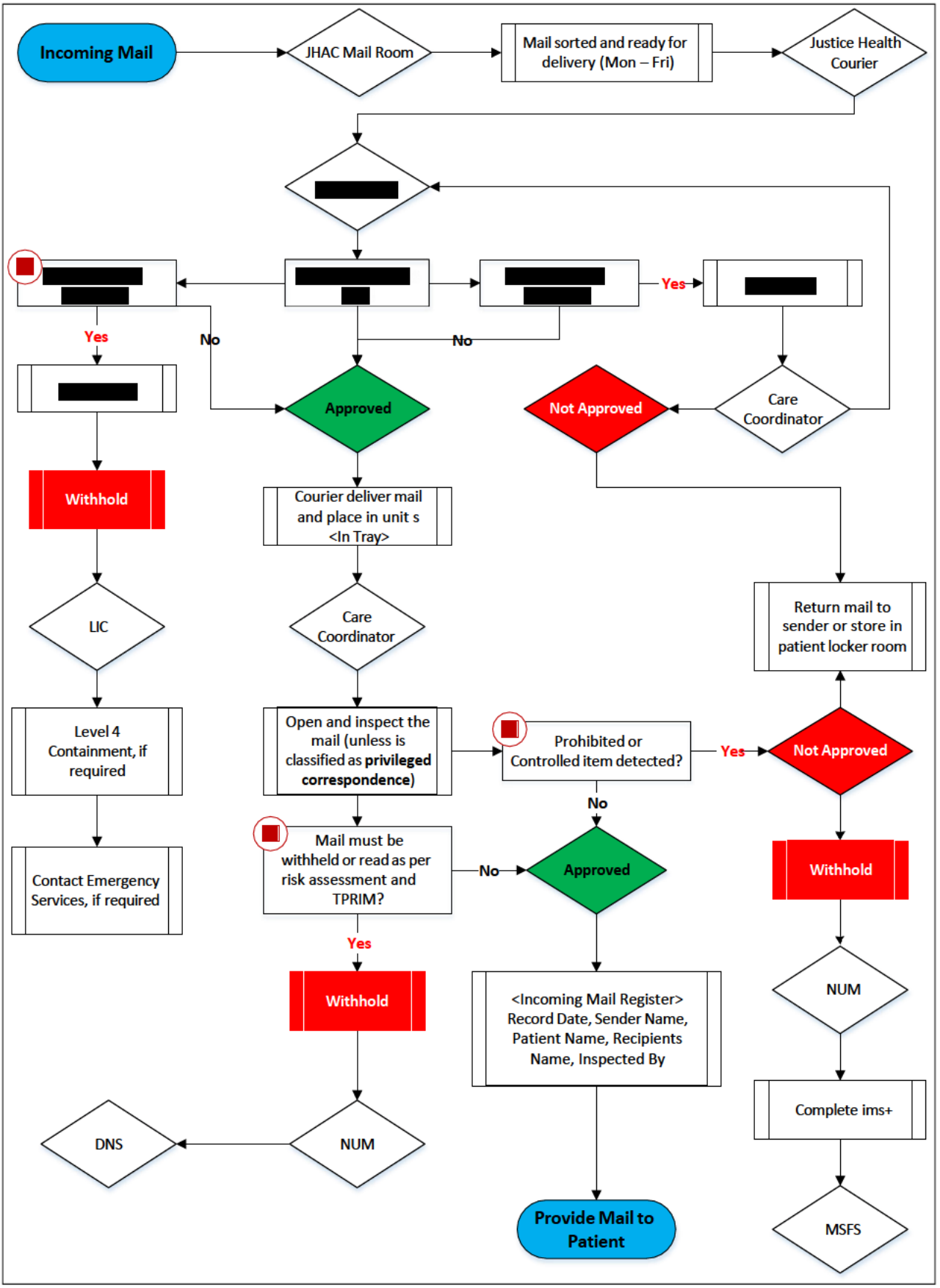
7.2 Incoming patient mail register template

Date	Sender Name	Patient Name	Inspected by

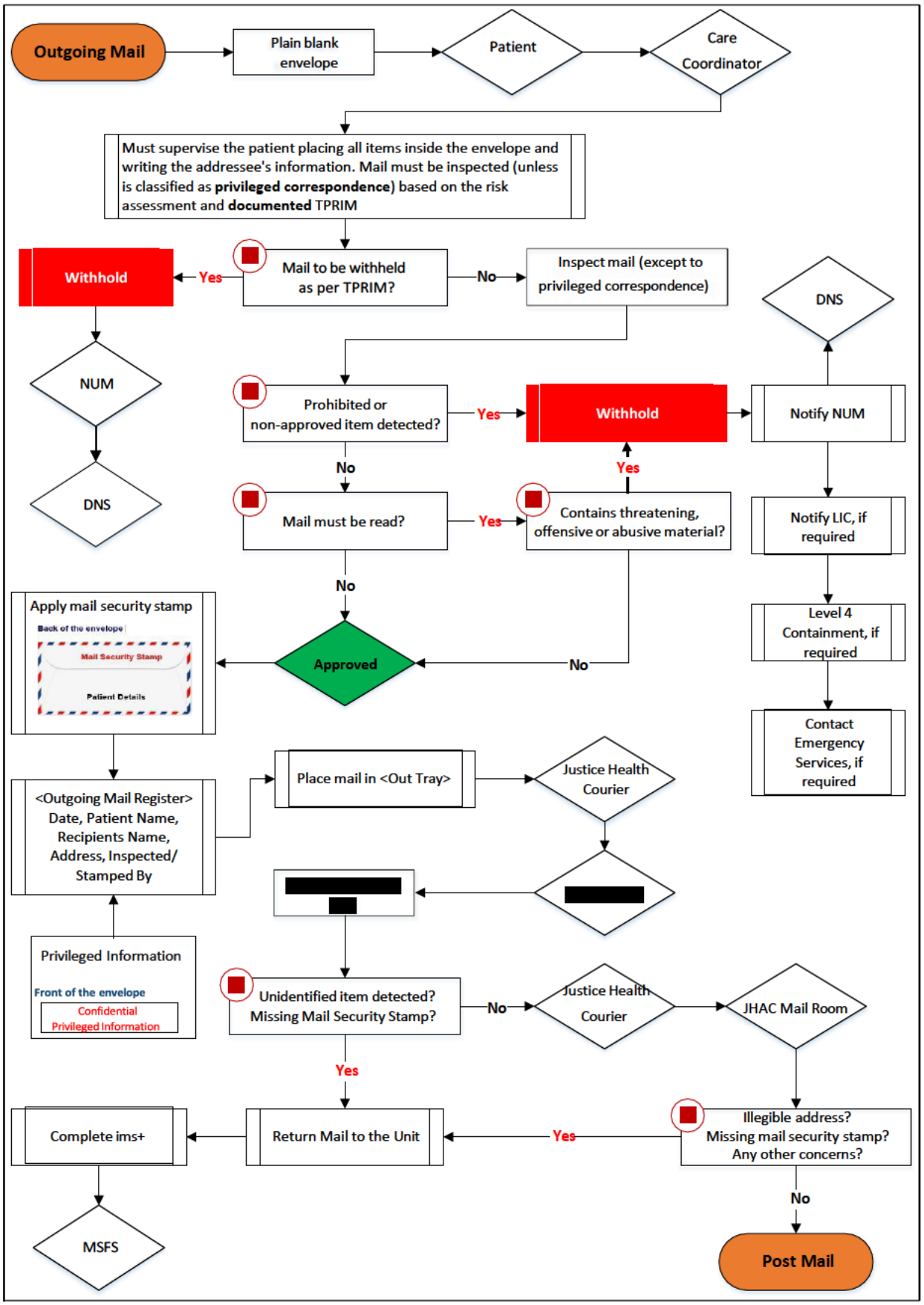
7.3 Outgoing patient mail register template

Date	Patient Name	Recipient's Name	Recipient's address	Inspected and stamped by

7.4 Incoming mail flowchart



7.5 Outgoing mail flowchart



7.6 Hazardous mail risk assessment

This assessment process can be used for all categories of hazardous mail which consists of:

- Biological and chemical substances, including powdery, granular or sand like solids, gases or liquids.
- Sharps and dangerous items, including razor blades and needles.
- Offensive mail, including death threats, grossly objectionable matters, racial vilification and rant letters.

How to assess possible hazardous mail [1]

You need to carry out a risk assessment to determine if the mail item is suspicious. The risk assessment involves answering the three questions below. If the answer is yes to any of these questions, you may consider the mail is suspect and warrants further attention.

Question 1. Does the item have one or more hazardous mail indicators? [2]

A suspect item may have several hazardous mail indicators but you need to be aware that it may also have none. There are three categories of hazardous mail indicators.[2]

i. ***Emissions and releases from the item***
   - Powdery, granular or sand like substances visible on the outside or leaking from it
   - Ticking or unusual sound
   - Unusual odour from the letter or package
   - Sparks, fumes, clouds or smoke
   - Oily stains or discolorations
   - Causes skin irritation when touched
   - Melts or alters the surfaces it touches

ii. ***Strange labelling, postage and markings on the item***
   - Address handwritten or poorly typed
   - Misspellings of common words
   - Not addressed to a specific person but to a position title
   - Incorrect position title
   - Strange return address or no return address
   - Postmarked from a city, state or country that does not match the return address
   - Excessive postage stamps
   - Marked with warnings, threatening language, signs and restrictions such as *Confidential*, *Dangerous ideas inside*, *Do not x-ray* and an image of the skull and crossbones

iii. ***Unusual shape and form of the item***
   - Strange shape or weight
   - Lopsided or unevenly weighted envelope
   - Stiff or rigid envelope
   - Powdery, granular or sand like substances felt through the envelope/package
   - Razor blades, bullets or other dangerous items felt through the envelope/package
   - Excessive weight for size
   - Protruding wires, tin foil and sharps (needles)
   - Excessive security materials, such as masking tape and string

Question 2. Does the item have characteristics which are not typical of normal mail received?

You need to determine what is typical of the mail you receive. To do this, you need to consider the mail you have received over the preceding months and identify:

1. Who are the typical senders?
2. What is typical labelling, postage and markings on the items you receive?
3. What is the usual shape and form of the items you receive?

Question 3. Was it delivered in a non-typical way?

You need to determine how mail is typically delivered. To do this, you need to consider the mail you receive over the preceding months and identify:

1. What types of mail are delivered by post, couriers and by hand?
2. Is there some mail which is delivered in unusual ways and how often does this occur? (For example, samples of products which come from overseas once every six months or legal documents delivered by hand to the Legal Officer whenever a board election is to occur.)

Notes:

1. Managers should apply risk management principles for managing mail security risks.

2. The hazardous mail indicators - use points from the Australian Federal Police fact sheets: https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-factsheets.pdf

Adopted from:
The Australian Homeland Security Research Centre

7.7 Recognising potential hazards

- It is critical that staff handling mail remain vigilant and cautious at all times. It should be remembered, however, that most reports of suspicious packages are false alarms.
- All staff handling mail items in a work environment should be aware of the emergency procedures for responding to and reporting a suspicious item. Refer to your Emergency Control Organisation (ECO) structure.
- Where possible, the sorting and processing of mail and packages should be conducted in an area that is separate from the main organisation and which can be easily contained.
- If your staff receive a package or letter that you believe is suspicious, follow the procedures outlined below.
    1. HANDLE WITH CARE – Do not shake or bump.
    2. ISOLATE IT – Immediately.
    3. DO NOT OPEN – Smell, touch.
    4. TREAT IT AS SUSPECT – Call for help.

WHAT TO DO IF YOU RECEIVE A SUSPICIOUS PACKAGE OR MAIL ITEM

If you suspect that you have received a package that may contain hazardous material and HAVE NOT OPENED IT.

- Place item in a plastic bag and seal it.
- Place all items in a second plastic bag and seal that also.
- Stay in your office or immediate work area. This also applies to co-workers in the same room. Prevent others from entering the area and becoming contaminated. Remember you are not in immediate danger.
- Call for help. This may be your manager or call Triple Zero (0-000) to ask for the Police or Fire & Rescue.
  Advise:
- Exact location of the incident - street address, building, unit.
- Number of people potentially exposed.
- Description of the package/device.
- Action taken e.g., package covered with black coat, area isolated.
- Keep your hands away from your face to avoid contaminating your eyes, nose and mouth.
- If possible (without leaving your work area) wash your hands.
- If possible have the building ventilation system shut down and turn off any fans or equipment that is circulating air around the workplace.
- Wait for help to arrive.

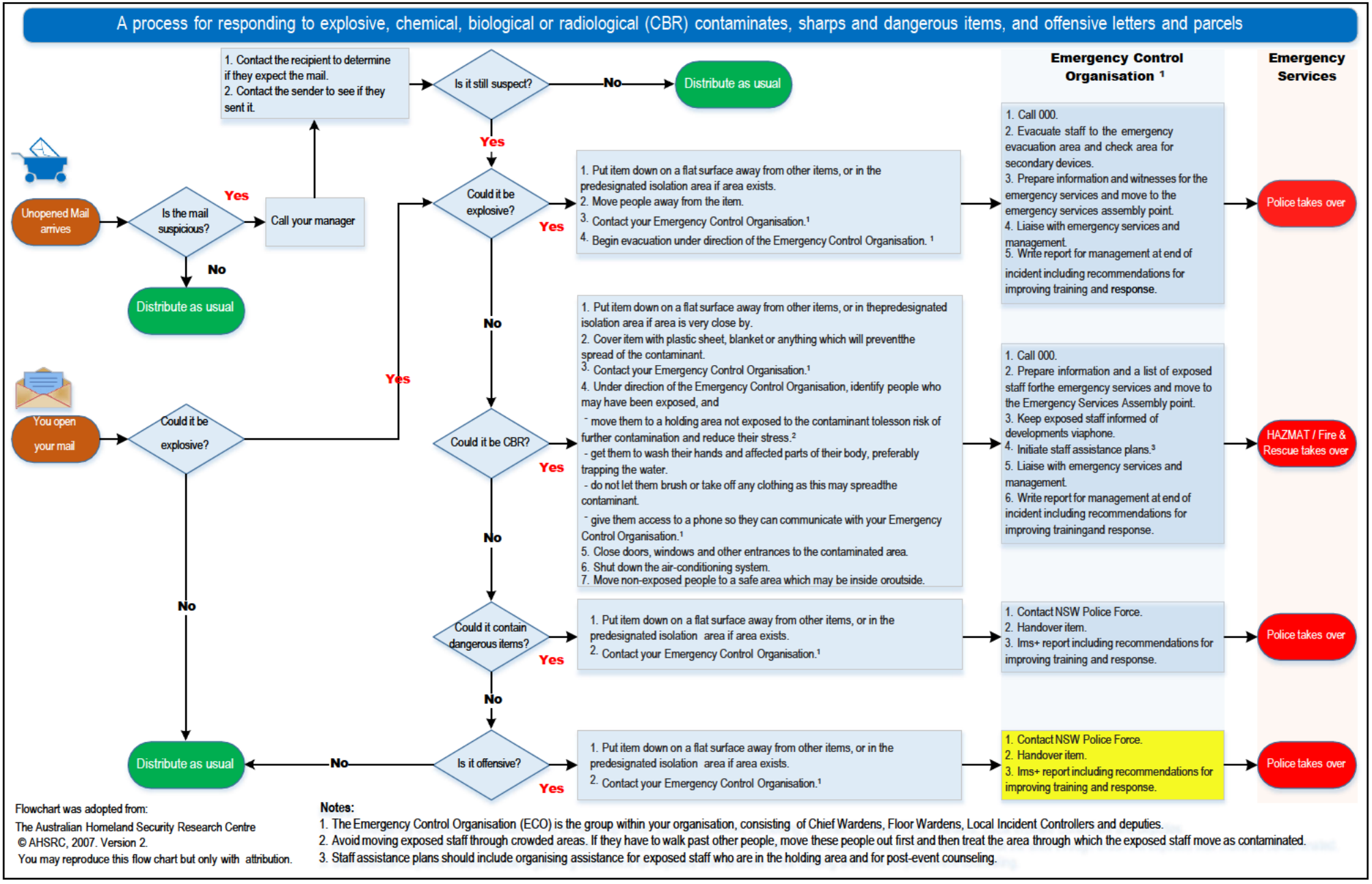
If you suspect that you have received a package that may contain hazardous material and HAVE OPENED IT

- Do not disturb the item any further. Do not pass it around. If any material has spilt from the item, do not try to clean it up, or brush it from your clothing.
- If possible place an object over the package without disturbing it such as a large waste bin.
- Stay in your office or immediate work area. This also applies to co-workers in the same room. Prevent others from entering the area and becoming contaminated.
- If there is a strong/overpowering odour move to an adjoining room closing all doors and windows and stay in that area until help arrives.
- Call for help. This may be your Local Incident Controller or call Triple Zero (0-000) to ask for Police or Fire & Rescue depending on your situation.
  Advise:
- Exact location of the incident - street address, building, unit.
- Number of people potentially exposed.
- Description of the package/device.
- Action taken e.g., package covered with black coat, area isolated.
- Keep your hands away from your face to avoid contaminating your eyes, nose and mouth.
- If possible (without leaving your work area) wash your hands.
- If possible have the building ventilation system shut down and turn off any fans or equipment that is circulating air around the workplace.
- Wait for help to arrive.

If you suspect the mail item may contain an explosive device

- Follow your normal emergency procedures
- Ring Triple Zero (0-000) and report the package to the Police
- Evacuate the area

7.8 Dealing with suspicious and hazardous mail flowchart



Flowchart was adopted from:
The Australian Homeland Security Research Centre

Notes:

1. The Emergency Control Organisation (ECO) is the group within your organisation, consisting of Chief Wardens, Floor Wardens, Local Incident Controllers and deputies.
2. Avoid moving exposed staff through crowded areas. If they have to walk past other people, move these people out first and then treat the area through which the exposed staff move as contaminated.
3. Staff assistance plans should include organising assistance for exposed staff who are in the holding area and for post-event counseling.