FRAMEWORK FOR USE OF AN ELECTRONIC DRUG REGISTER REQUIRING DUAL SIGNATURES

Introduction and scope

An electronic drug register that requires dual signatures may be used to record transactions for Schedule 8 drugs (drugs of addiction, otherwise known as Controlled Drugs) in various settings:

- a public hospital or public health institution under the *Poisons and Therapeutic Goods Regulation 2008* (the Regulation)
- a private health facility licenced under the *Private Health Facilities Act 2007*
- a residential care facility under the Regulation
- a facility (other than a community/retail pharmacy) licenced under the Regulation that administers or supplies Schedule 8 drugs under the NSW Opioid Treatment Program.

The electronic drug register use must be compliant with the Standards for Use of an Electronic Drug Register Requiring Dual Signatures (the Standards) described in this document. These Standards are in addition to requirements set out in the Regulation. Obligations under the Regulation must be met except where expressly stated otherwise in this Framework. Where an electronic drug register is for use in a NSW public health facility, the system must be assessed against requirements set out in NSW Government policies relating to privacy and information security to ensure that the system is acceptable for implementation in the facility.

There are separate Standards for a general (single signature) drug register that is used, for example, in a community pharmacy (see clause 111 of the Regulation). However, a system may be configured for both single and dual signatures.

Background

Persons authorised to be in possession of Schedule 8 drugs must:

a) keep a drug register in the form of a book to record transactions of Schedule 8 drugs, and

b) enter the details relevant to each transaction in the drug register on the day of the transaction

for the purpose of confirming the balance on hand and confirming the associated transaction that created the balance.

Transactions in a register include receipt, supply, administration, compounding/manufacture, credit, adjustment transfer in/out, error/reversal, stock check, periodic audit, damage, loss, and destruction.

These transactions made by an authorised person must be countersigned by the person who witnessed the transaction (see clause 117 of the Regulation). Hence, the register requires dual signatures.

Approval of electronic form of drug register

The Secretary, NSW Health has approved the keeping of a drug register other than in the form of a book, where the use of the electronic drug register complies with the

‘Standards for Use of an Electronic Drug Register Requiring Dual Signatures’ as described in this document.

The approval under the Regulation (clause 117(4)) allows electronic confirmation of entries instead of by a handwritten signature.

The electronic drug register may be used to record transactions of other accountable medications non in Schedule 8 (such as Schedule 4 Appendix D medicines) if required under a local protocol.

Definitions

‘**authorised person**’ means a person who is authorised to possess, supply or administer Schedule 8 drugs under the Regulation and who is required to make entries in a drug register. In many health facilities this will typically be a registered nurse/midwife. Only an authorised person or inspector can make a confirmed entry in the electronic drug register. In any legal proceedings, in the absence of proof to the contrary, the authorised person to whom the unique access credential has been assigned is taken to have made the entry.

‘**confirmed entry**’ means an entry made in an electronic drug register by an inspector, or an entry made by an authorised person that is required under the Regulation to be made in the drug register, including the receipt, supply or administration of a Schedule 8 drug.

‘**eligible witness**’ means a person who countersigns entries made in the electronic drug register by an authorised person. The eligible witness is typically a nurse/midwife but could include a medical practitioner, a pharmacist, or an enrolled nurse. A local protocol should identify who may countersign a register entry in a facility.

‘**finalised entry**’ means a confirmed entry countersigned by an eligible witness or an inspector. In countersigning the confirmed entry, the user is deemed to be ‘finalising’ the confirmed entry.

‘inspector’ means a police officer or a person appointed under section 42 of the *Poisons and Therapeutic Goods Act 1966* who can view, retrieve, print, copy, or make entries in an electronic drug register. An inspector may countersign (or finalise) their own entries.

‘**login**’ of an individual means a password or other secret, a device, a biometric identifier, a combination of these, or any other method of authenticating the identity of the individual at the point of access to an electronic drug register.

‘**pending entry**’ means an entry that is not required to be retained in the register. This entry may be created by a person who has authorised access to the electronic register (a ‘restricted user’) or an entry captured from another system by way of a manual or automated procedure. The pending entry can be made into a confirmed entry by an authorised person.

‘**person responsible for the electronic drug register used at the premises**’ means the person responsible for the management and operation of the system in the facility, for example:

- the nurse or midwife in charge of the ward of a public hospital or public institution under the Regulation
- the nurse or midwife in charge of the ward of a private health facility licenced under the *Private Health Facilities Act 1997*

- the person responsible for a residential care facility under the Regulation
- the person nominated on the licence as responsible for completing and maintaining records for the receipt, administration or supply of methadone and buprenorphine at a facility (other than a community/retail pharmacy) licenced under the Regulation to administer and/or supply Schedule 8 drugs under the NSW Opioid Treatment Program.

'restricted user' means a person who has been granted access to the electronic drug register for the purpose of making a pending entry. A restricted user cannot make a finalised entry.

'Schedule 8 drug' means a drug listed in Schedule 8 of the Poisons Standard, referred to as a 'drug of addiction' in the *Poisons and Therapeutic Goods Act 1966*, and otherwise known as a 'Controlled Drug'.

'**system**' means an electronic drug register.

'**system authorising officer**' means the person who authorises the operation of the system in the facility. The person should have an appropriate level of seniority and understanding of the system, including security risks they are accepting on behalf of their facility. This person may be, for example:

- the Chief Executive of a public hospital under the *Health Services Act 1997*
- the licensee of a private health facility licensed under the *Private Health Facilities Act 1997*
- the approved provider of a residential care facility under the *Aged Care Act 1997.*

'**the Regulation**' means the NSW *Poisons and Therapeutic Goods Regulation 2008*.

'**user**' means a person who has been granted access to the electronic drug register.

Standards for Use of an Electronic Drug Register Requiring Dual Signatures

These Standards ensure secure and appropriate use of an electronic drug register.

The Standards describe the requirements:

1. For the electronic drug register system (Section 1)
2. For the system authorising officer (Section 2)
3. For the person responsible for the electronic drug register used at the premises (Section 3)
4. For an authorised person and eligible witness (Section 4)
5. For each user of the electronic drug register (Section 5)

Section 1: Electronic drug register functionality, security and audit

An electronic drug register may be implemented as a standalone solution or a segment of an enterprise solution. An automated drug cabinet may be used as an electronic drug register where these standards are met.

Standard

1.1 System security must comply with contemporary industry and government standards. The Australian Signals Directorate's Australian Government

Information Security Manual (ISM) and Australian Government's Protective Security Policy Framework (PSPF) provide guidance. NSW privacy legislation outlines protections for personal information which apply to system security.

1.2 The system must authenticate users before they are granted access to the system.

1.3 The system must implement a strong user authentication mechanism. Multi-factor authentication should be implemented rather than single-factor authentication.

1.4 The system must uniquely identify users and authenticate users on each occasion that access is granted to the system.

1.5 Access to information in the system must be via a set of role-based access controls with least access privileges (i.e. read, write, modify).

Standard role-based profiles must be implemented based on responsibilities of user types/roles.

Generic accounts are not permitted.

1.6 Users' access rights and privileges granted must be securely administered.

1.7 Audit logs must be retained for a minimum of two (2) years, or where the system is used in a public hospital or public institution, for a minimum of seven (7) years, after finalisation of the entry.

1.8 Audit logs should include information about access to, use of, and time of use of the system by users, log on attempts (successful or unsuccessful), successful/failed use of any privileged accounts, account changes, and changes (actual or attempted) to system security settings and controls. It should be possible to query and export the information

1.9 Password setup, maintenance and storage, where applicable, must accord with industry and government standards. The Australian Signals Directorate's Australian Government Information Security Manual (ISM) provides guidance.

1.10 Where the system allows a user to change their own password, any change must be based on proper authentication of the user and must prevent any disclosure of the password during the operation.

1.11 The log on procedure must be designed, implemented and configured to prevent unauthorised access and to disclose the minimum of information about the system before the user logs in. It is good practice to have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

1.12 The system must allow a user to log out on demand.

1.13 The system must terminate a session when the user logs out of the system, or a window closes.

1.14 The system must ensure accounts are locked after a maximum of 5 failed log on attempts.

1.15 The system must require a user to re-authenticate after a maximum of 15 minutes of user inactivity.

1.16 The system must record a user's unique identifier against every entry added or modified by the user.

1.17 The system must allow users to make confirmed entries for transactions that are required to be recorded in a register.

1.18 The system must allow a confirmed entry to record the particulars required under subclauses 117(1)-(2) of the Regulation relevant to the transaction (e.g. quantity administered, time of day, patient name, quantity held after the transaction).

1.19 The system must display the stock balance (i.e. balance at hand) following a transaction in the system.

1.20 Where a transaction is an adjustment to the stock balance (i.e. balance at hand), the system must allow for a reason to be recorded against the transaction.

1.21 The system must not allow an authorised person who makes a confirmed entry to finalise that confirmed entry (i.e. an authorised person cannot 'witness' their own entry for the purposes of finalising it).

1.22 The system must assign a unique reference number for each finalised entry with the time and date of the transaction.

1.23 The system must prevent a finalised entry from being altered or deleted under any circumstances.

1.24 The system should allow a note to be entered and associated with a transaction, for example, to record details against a transaction that has been made in error.

1.25 The system should prompt a blind count, i.e. prompt the user to physically count the number of remaining products in that location and enter this count at the time of drug removal, without displaying the expected inventory level.

1.26 The system may allow data elements relevant to a transaction to be entered by a restricted user or transmitted from another computer system, such as a prescribing, invoicing, dispensing or automated drug cabinet computer program or another electronic drug register. These entries may be made into a confirmed entry by an authorised person.

Transmission of data to and from the system should use secure channel encryption and protocols.

1.27 The system must retain, and make available, finalised entries for a period of two (2) years, or where the system is used in a public hospital or public institution, for a period of seven (7) years. (The retention period may be longer in some circumstances such as where the system is part of an electronic medical record system.)

Note: As records contain personal information (e.g. patient name, authorised person name) disposal of records must be performed in a secure manner.

1.28 The system must allow a user to immediately produce the following reports in electronic form and in printed form at the premises where the system is used:

a) All current stock balances

b) All finalised entries for a stated period (date to date) for a stated drug

c) All finalised entries on a stated date

d) All finalised entries to a stated patient for a stated period (date to date)

e) All finalised entries from a stated supplier for a stated period (date to date)

f) All finalised entries by a stated authorised person or eligible witness.

(Note on compliance: It should be possible to export all types of records contained in the system, regardless of format or the presence of the generating application, to safeguard against the loss of data if the application is discontinued, no longer supported or suffers catastrophic failure).

1.29 The system should retain the designation or position of the person responsible for the electronic drug register. If the system cannot retain this information, the details must be recorded elsewhere and be immediately accessible.

1.30 The system should retain the name of any previous person responsible for the electronic drug register for a period of two (2) years commencing on the date they cease to be responsible, or where the system is used in a public hospital or public institution, for a period of seven (7) years. If the system cannot retain this information, the details must be recorded elsewhere and be immediately accessible.

1.31 System components (hardware, software, networks, cloud services) and any interfaces must have security measures that safeguard records, including to the level required for personal information (e.g. patient name) where applicable. The Australian Signals Directorate's Australian Government Information Security Manual (ISM) and the Australian Cyber Security Centre's Strategies to Mitigate Cyber Security Incidents provide guidance.

1.32 Personal information (e.g. patient name) should be encrypted while at rest and when in transit.

1.33 System back-up and restore arrangements must accord with industry and government standards. The Australian Signals Directorate's Australian Government Information Security Manual (ISM) and the Australian Cyber Security Centre's Strategies to Mitigate Cyber Security Incidents provide guidance.

Section 2: Requirements for the system authorising officer

Standard

2.1 The system authorising officer must approve use of the electronic drug register at the premises.

2.2 The system authorising officer must be satisfied that the electronic drug register meets the standards set out in this framework document.

2.3 The system authorising officer must implement a protocol that ensures that:

a) access authorisations needed by users are adequately approved

b) users are issued with a login that identifies them to the system and is attached to the unique identity of the user

c) a record is kept of all user types/roles and their responsibilities (in addition to the roles listed in the Framework, other roles can be established under the protocol, such as a system administrator to manage user accounts)

d) persons responsible for the register used at the premises and persons who must make entries in the register can meet the legal requirements set out in the Regulation or a licence issued under the Regulation

e) users are competent in the use of the system and have access to training, user guides and manuals

f) persons responsible for the register and authorised persons are informed that the electronic drug register used at the premises meets the standards

g) access control procedures are monitored and enforced

h) repeated lockouts by users are investigated before reauthorising access

i) users' rights and privileges are removed as soon as practicable but no more than fourteen (14) days from when a user no longer has authorised access or has a legitimate business need to access the system

j) ensure privileges and user accounts are reviewed on a regular basis to ensure only those who need access to meet their obligations under the Regulation are given access

k) ensure audit logs are reviewed and monitored regularly and security issues are reported to the person responsible for the register (audit log reviews should be performed by a person/s who does not make entries in the system and audit logs should be examined at a minimum every month where the volume of transactions in the system is high)

l) system entries are available immediately both in electronic form and in printed form to an inspector appointed under section 42 of the *Poisons and Therapeutic Goods Act 1966*

m) an inspector appointed under section 42 of the *Poisons and Therapeutic Goods Act 1966* or a police officer has immediate access to the system to make finalised entries

n) written notice is given to the Secretary, NSW Health in accordance with the Regulation if any records in the system, or the system itself is lost or destroyed [clause 119 of the Regulation]

o) during any system downtime, drug register entries are made in a book compliant with the Regulation [subclauses 116(3)-(4)], such that:

   i. the book contains consecutively numbered pages

   ii. the book is bound so that the pages cannot be removed or replaced without trace

   iii. the book contains provision on each page for the inclusion of the particulars required to be entered

   iv. separate pages of the book must be used for each Schedule 8 drug, and for each form and strength of the drug

v. the book must be retained for a period of two (2) years commencing on the date of the latest entry, and for seven (7) years at a public hospital or public institution

p) at the start of downtime, the stock balance (i.e. balance at hand) for each drug must be recorded in the book

q) when any downtime has ceased, if the details in the book are not entered in the electronic register, the stock balance (i.e. balance on hand) for each drug must be entered in the electronic register and the fact that a book was used recorded in the system.

Section 3: Requirements for the person responsible for the electronic drug register used at the premises

Standard

3.1 The person responsible for the electronic drug register must ensure the system is available to persons who require access to make or witness entries.

Section 4: Requirements for the authorised person and eligible witness using the electronic drug register

Standard

4.1. The authorised person and eligible witness must keep secure the assigned unique access credential used to make an entry.

4.2. The eligible witness must directly observe relevant activities that they sign off on as witness.

Section 5: Requirements for each user of the electronic drug register

Standard

5.1. The user must use their login to perform all actions in the system.

5.2. A user must not use another user's login to access the system.

5.3. A user must be competent in the use of the electronic drug register.

5.4. A user must log out after they have completed transactions

For further information or clarification of this document, contact the Duty Pharmaceutical Officer, Pharmaceutical Regulatory Unit during business hours on (02) 9391 9944.

This document has been produced by:

Chief Pharmacist Unit
Legal and Regulatory Services Branch
NSW Ministry of Health
Telephone (02) 9391 9944 Fax (02) 9424 5860

Email: MOH-PharmaceuticalServices@health.nsw.gov.au

Website: http://www.health.nsw.gov.au/pharmaceutical