INRstar
safe, effective anticoagulation support

External Patient Lookup – Acceptable Use Policy

1. About this document

This document explains how the INRstar 'External Patient Lookup' functionality should be used. It is your responsibility to ensure that you understand and comply with this policy. It ensures that:

1.1 You understand your responsibilities and what constitutes acceptable use of the functionality

1.2. Patient data is not put at risk

1.2.1 Sullivan Cuff Software Ltd reserves the right to update this document as necessary. A copy of the current version can be found at: https://help.inrstar.co.uk/BrickwallResource/GetResource/7697658a-04aa-49dc-9fb9-6f6e3e830ced

1.2.2 Supporting information can be found via the INRstar Helpsite at http://help.inrstar.co.uk

1.2.3 This functionality has been developed based on the guidance provided by The Information Governance Review, published March 2013, also known as Caldicott 2.[1]

2 General information about External Patient Lookup

The 2013 Information Governance Review states that:

"The duty to share information can be as important as the duty to protect patient confidentiality … Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles."[2]

"Most people who use health and social care services accept that health care professionals will need to share personal confidential data if they are going to provide optimum care" [3]

2.1 The External Patient Lookup functionality has been provided to aid the provision of direct patient health care and this should be your only use of the functionality.

2.2 This functionality allows both View Only and Treatment Locations to search for patients managed by other locations and to view or treat the patient as necessary.

2.3 Healthcare professionals are required to treat the patient on the basis of their needs and keep the patient's information confidential. However; if a patient is outside of their usual

treatment area or in difficulty; implied consent means that registered healthcare professionals can share personal confidential data in the interests of direct care.

2.4 The patient record should only be shared between registered and regulated health and social care professionals who are registered on the system as clinical level 2 or above and who have a legitimate relationship with the individual for the purposes of the individual's direct care.

2.5 Sullivan Cuff Software Ltd reserves the right to withdraw External Patient Lookup functionality from use should operational or legal requirements dictate.

3 Terms of use

3.1 For a user to be able to use External Patient Lookup, they must be able to self-certify that they are a Registered and Regulated Health Care Professional. In addition the user must have INRstar permissions level of clinical level 2 or above. The user will be prompted to add their professional registration number (GMC/GPC/NMC).

3.2.1 External Patient Lookup functionality within INRstar should be used under the following conditions:

3.2.2 The patient presents themselves to the professional for the purpose of their care.

3.2.3 The patient agrees to a referral from one registered and regulated health or social care professional to another.

3.2.4 The patient is invited by a professional to take part in a screening or immunisation programme for which they are eligible and they accept.

3.2.5 The patient or client presents to a health or social care professional in an emergency situation where consent is not possible.

3.2.6 The relationship is part of a legal duty e.g. contact tracing in public health.

3.2.7 The patient is told of a proposed communication and does not object.

4 Responsibilities when using the INRstar External Patient Lookup functionality

4.1 You should familiarise yourself with the External Patient Lookup Guidance pages on the INRstar Helpsite which include important policy guidelines, information about the functionality and user/administration guides.

4.2 You should not attempt to use a log in which is not your own. 4.3 You should not record any patient information which does not relate to the patient's

4.3 You should not record any patient information which does not relate to the patient's direct care.

4.4 Anonymised data under the Freedom of Information Act 2000 and the Data Protection Act 1988: External Patient Lookup should be treated like any other clinical communication and care should be taken to ensure that content is accurate and appropriate.

4.5 It is your responsibility to make sure that your user details in INRstar are correct and up to date.

4.6 You should not use External Patient Lookup to identify patients on behalf of a third party.

5 Example scenarios of acceptable use

5.1 Consulting on an unstable or complex patient who is not present (at the request of another healthcare professional who is treating the patient).

5.2 Treating a patient who has "turned up" and is requesting treatment – e.g. in hospital or on holiday.

5.3 Checking a patient has been adequately monitored before dispensing a drug to them.

5.4 Treating a patient who is not present and who is not your normal patient, but for whom you are part of a chain of services involved in providing their direct care. For example, an Out-Of-Hours service may receive a blood test result and need to treat the patient based on it.

6 Patient consent

6.1 In the opinion of the SCSL Caldicott Guardian the above scenarios do not require the individual patient's explicit consent.

6.2 Caldicott 2 states that: For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

6.3 However, in the unlikely event that a patient chooses to dissent from this function, an "Opt Out" Flag can be set at a patient level within INRstar.

7 Audit trail and data security

7.1 A full audit trail of all patient views and actions is recorded against the patient record. This can be viewed by anyone with access to that patient record at their “normal” location.

7.2 A system audit trail is maintained at the “external” location to record all views and treatments that have taken place at that location. This audit trail does NOT contain any demographic data.

7.3 A note is placed on the Patient record that the patient has been viewed or treated at an external location. The external location cannot remove or edit this note.

7.4 A report is available at every treatment location to show a list of all external views and treatments that have taken place for the patients managed at that location.

Source: Information: The Information Governance Review March 2013

[1] * Caldicott 2 (Information Governance Review)
[2] * Information Governance Review Page: 38,
[3] * Information Governance Review page 20