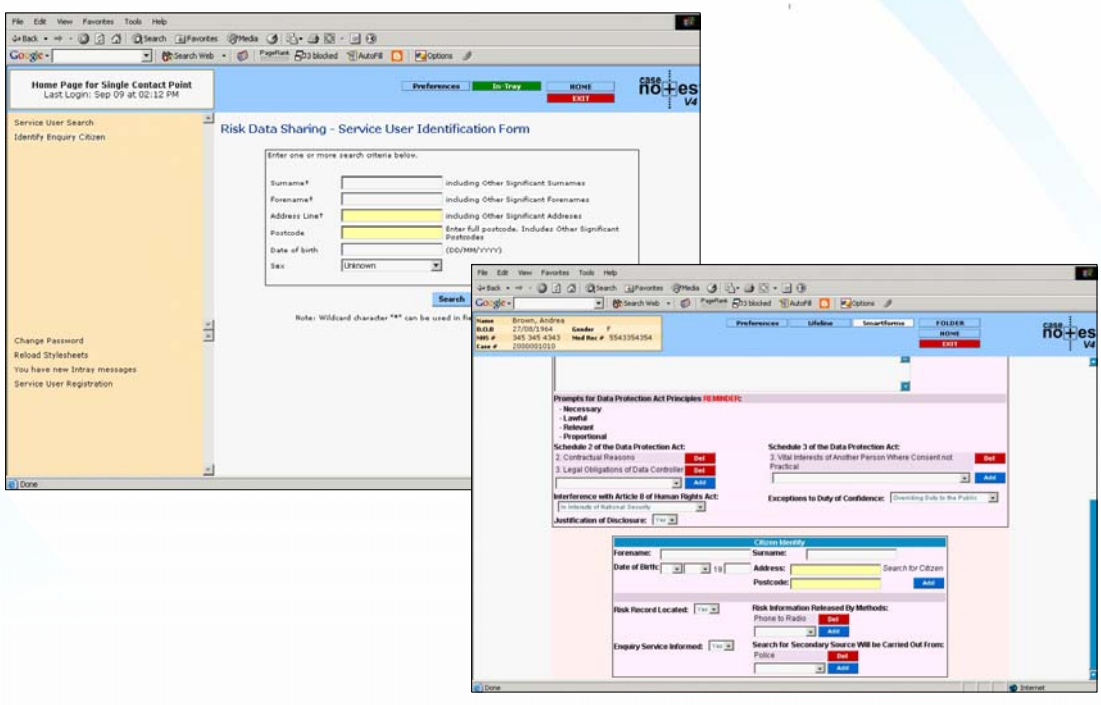
CSW HEALTH LTD

Case Study:

London Risk Data Sharing Service

Sharing Information about Mental Health service users



Case Study – London Risk Data Sharing Service

Introduction

CSW Health Ltd were selected by the London Development Centre for Mental Health to develop and implement a system for sharing information about mental health service users, with the objective of reducing serious incidents involving people with severe mental illness.

In order to achieve this objective, the participating organisations in London needed to share risk-related information in specific circumstances through a Single Contact Point staffed by mental health professionals. They hoped that this would overcome their existing difficulties of paper-based health and social care information, and the availability of professional staff to make a decision to disclose it, by maintaining a central database and having the Single Contact point staffed on a 24-hour basis.

The organisations that agreed to participate in the London Risk Data Sharing Service include:

- the Metropolitan Police
- the London Probation Area
- London Ambulance Service NHS Trust
- Camden & Islington Mental Health and Social Care Trust,
- Westminster City Council Social Services Department
- Central and North West London Mental Health NHS Trust

Sharing Information to meet the Objectives

The objectives of the London Risk Data Sharing Service were:

- to ensure that mental health service users have access to appropriate treatment and care when in contact with any of the organisations taking part in the project
- to reduce the number of serious untoward incidents involving mental health service users
- to help professionals working for the organisations involved manage risk better when dealing with mental health service users

The organisations participating in this project believed that the best way to achieve these objectives would be by sharing information, particularly relating to risk. By working together, this would help them provide the most appropriate treatment and care to the people they were dealing with, giving them the knowledge to manage the risk as effectively as possible.

The Solution

CSW worked with the London Development Centre for Mental Health to create a web-based database of risk-related information. The solution, which uses Case Notes™ - CSW's XML-based product for Shared Care Records, can be accessed through a standard web browser allowing data entry and data viewing for the participating organisations from over 40 different locations.

Case Notes™ provides structured access to all risk-related information using a multi-tiered web architecture that allows for easy configuration and scalability on the server side, which reduces the client configuration to

zero. All that is needed for user access is a standard web-browser such as Microsoft Internet Explorer or Netscape Navigator. Case Notes™ uses open standards technology such as the eXtensible Markup Language (XML) and is fully extensible through a system of plug-in modules.

The Smart Forms module provides the template upon which all information is held and displayed at the Single Contact Point. Smart Forms is a form-based, version-controlled mechanism for entering and updating dynamic events directly within an individual's care record. The Smart Forms module enables the system user to design, create and publish all the Forms they are using in their daily work so that they can deal with them electronically. Access to these forms for specific actions such as read/ edit/ delete/ can be controlled via the Case Notes™ Access Control Framework (ACF).

The Single Contact Point

The process of requesting and disclosing risk–related information is managed through a Single Contact Point. The Single Contact Point is available by telephone 24 hours a day and is maintained by mental health professionals with appropriate qualifications and experience.

Single Contact Point staff are responsible for managing the interface between the mental health organisations (2 Trusts and 3 social services departments) and non mental health organisations using the service. The information exchanged relates only to identification of the individual concerned, the nature of the risk involved and advice on managing that risk, on the basis that these data items are the minimum necessary to successfully manage the situation.

The Single Contact Point provides access to the following information from the database of risk-related information:

- *Information necessary for identification* eg. name; address; date-of-birth
- *Information necessary to assess the nature of the risk* eg. type of risk; history; access to drugs; access to harmful instruments; triggers and precedents; previous specific threats and outcomes; factors which might make the risk worse
- *Information necessary to manage risk* eg. factors which could make the situation better/worse; language spoken and the need for an interpreter; physical or learning disability or medical condition; and family awareness of mental health issues.
- *Additional information provided by the service user.* The service user has the option to provide any additional information they think might be helpful to someone dealing with them in a crisis situation.
- *Information is also provided for reference and audit purposes only (and is <u>not</u> shared)*

The risk information held on the secure database relates to people who have been assessed by mental health services as being a risk to themselves or to others. Multi-disciplinary mental health teams decide which individual service users under their care should have their details on the central database.

Requesting Information

Information from the risk database is shared only if disclosure can be legally justified in the circumstances. Indicative thresholds for disclosure have been developed in consultation with the organisations involved and with regard for the legal context of disclosing information, but the staff working at the Single Contact Point must ensure that any decision they make complies with:

- the Data Protection Act 1998
- the Human Rights Act 1998
- the common law Duty of Confidentiality

Security

All transfer and holding of information is secured through the use of Secure Sockets Layer (SSL) protocol, and the firewall of the organisation hosting the database server.

Access to the central database of risk-related information, is controlled by the SCP team and the Case Notes™ Access Control Framework (ACF). The ACF is a generic security and access control framework, essential to the controlled sharing of information and tracking of user and system access to the underlying XML repository within Case Notes™. The ACF also ensures that any access to risk-related information is fully recorded for audit purposes.

Moving Forward

This initial phase of the London Risk Data Sharing Service will be evaluated with a view to rolling out further across London and the surrounding communities. This will include a detailed evaluation of both the outcomes and the processes of information sharing by a research team. As the project moves forward, it is hoped that the benefits harnessed by mental health professionals, emergency services staff, service users and the general public will continue to grow.

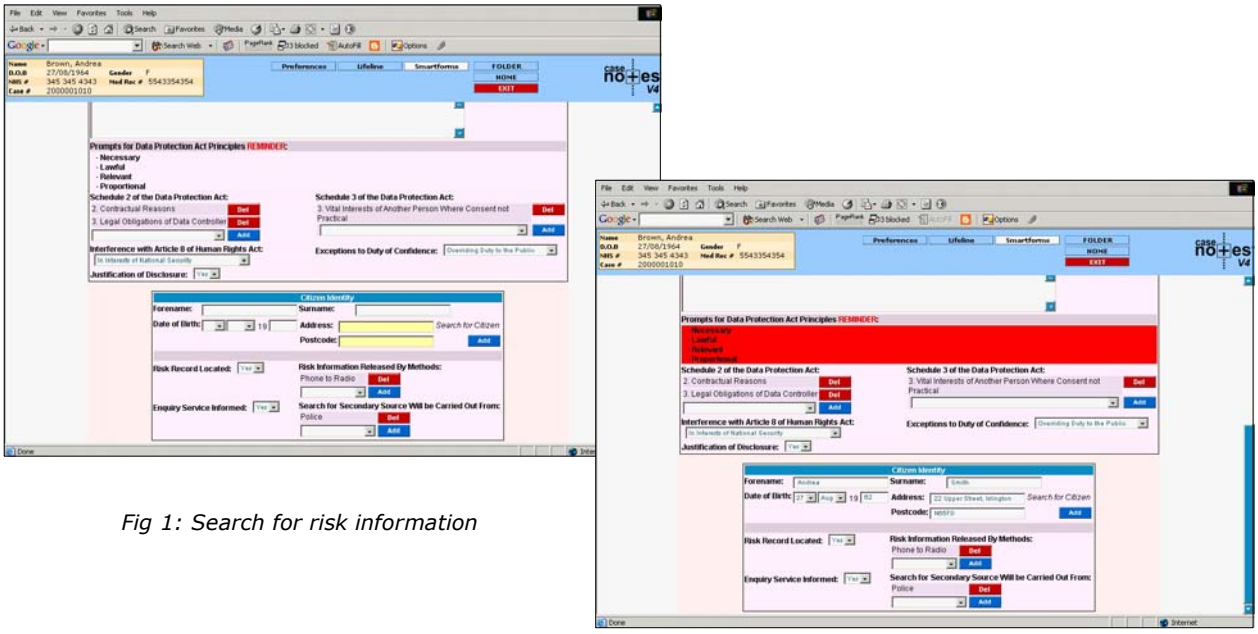


Fig 1: Search for risk information