

USING PERSONAL INFORMATION FOR SECONDARY HEALTH AND SOCIAL CARE PURPOSES¹

This guidance should be of particular interest and relevance for those staff who have specific responsibilities for information management in the health and social care sector. It should also be useful for staff who are dealing with requests for access to service user information for secondary purposes and for implementing data sharing protocols.

The guidance is based on the DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information (2012).

Introduction

This guidance note considers the uses and disclosures of service user information for purposes of health and social care not directly related to the care of an individual service user, commonly referred to as secondary uses. Service user information is increasingly required for evidence-based practice and for a rational approach to health and social care service provision. The following are examples of such secondary uses: planning; financial management; commissioning of services; investigating complaints; auditing accounts; teaching; health and social care research; public health monitoring; registries; infectious disease reporting.

Consent

Consent for secondary uses is informed by a general consideration of the requirements of consent. Consent is the means by which service users can exercise control over the dissemination of their confidential information. Use or disclosure of person identifiable information is normally justified by the consent of the service user².

As with any other intervention forming part of the provision of *direct care* for a service user, the service user's consent occupies a pivotal role in legitimising the uses and disclosures of their information. Service users must be informed in a manner appropriate to their communication needs of what information sharing is necessary for their care and the likely extent of the sharing for a particular episode of care. Provided service users are adequately informed in this way, express consent is not necessary for their health care and their consent to the disclosure of information necessary for their health care may be inferred from their acceptance of that care.

Any proposed disclosure for purely social care purposes for direct care (ie unconnected to any health care provision) is not a "medical purpose" under the Data Protection Act and express consent should usually be sought³.

Review of care

Review of care, including clinical audit and case review carried out by members of the care team and those supporting them, is for the purpose of improving the direct care of that service user. Such purposes have sufficient connection with that direct care for the sharing of information during the review of care to be justified on the basis of implied consent, provided the individual has been informed⁴.

Secondary uses⁵

From a consent perspective, a clear distinction must be drawn between disclosures which are necessary for the purpose of the care of the service user and disclosures

which are for maintaining or improving the general functioning of health and social care services (secondary uses).

While the informed co-operation of a service user can provide a basis for inferring their consent to the use and disclosure of information required for their care, there is no behaviour which clearly implies consent to other uses and disclosures. Therefore when the proposed use or disclosure relates to health and social care, but is not directly for the care of that service user, the express consent of that service user is usually required, unless the information is in an unidentifiable form. The possible exceptions to this requirement for consent are where a statute, court or tribunal imposes a requirement to disclose or there is an overriding public interest in the use or disclosure.

Principles for Good Practice⁶

The following principles for good practice should be followed when considering use and disclosure of personal identifiable information for any secondary purpose:

- All organisations seeking personal identifiable information for other than direct care should be seeking anonymised or pseudonymised data.
- To assist the process of pseudonymisation the Health and Care Number (HCN) of service users should be used wherever possible. It should be noted that the HCN is a potential identifier and not a pseudonymiser. Nevertheless its use facilitates pseudonymisation, for example by encryption of the number.
- All organisations seeking to use personal identifiable information should provide information to service users describing the information they want to use, why they need it and the choices they have.
- Any proposed use of personal identifiable information must be for some clear general good or for the clear benefit of service users. That is, there must be a clear public interest involved.
- Service users and/or service user organisations should be involved in the development of any project involving the use of confidential information and the associated policies.
- Where an organisation has a direct relationship with a service user it should be aiming to implement procedures for obtaining the express consent of the service user. For all proposed research uses of personal identifiable information the express consent of the service user should normally be sought.
- Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user.
- Organisations should not use personal identifiable information for secondary uses where a service user has opted out by specifically refusing consent.
- Where data is to be disclosed only in aggregate form the potential identification of individuals from small numbers should be considered and appropriate protections applied (for example Barnardisation).

Situations arise where the consent of service users cannot practicably be obtained for use or disclosure, yet there are clearly public health and social care interests at

stake. Examples include disease registries for secondary uses, administrative and financial monitoring, and financial inspections - including probity checking to provide assurance on the level of service provision.

The Department is presently giving consideration to the development of 'safe haven and honest broker provision' - and to the introduction of legislation to deal with situations where it is considered necessary to set aside the common law duty of confidentiality for essential health and social care purposes.

For all proposed secondary uses or disclosures information must be held under high standards of security.

On issues relating to Data Sharing Agreements and associated information governance provisions please refer to the Information Commissioner's *Data Sharing Code of Practice*, Sections 8 and 14, and the *DHSSPS & HSC Protocol for Sharing Service User Information for Secondary Purposes*.

For further information see the *Code of Practice on Protecting the Confidentiality of Service User Information 2012* at:

<http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf>

Privacy Advisory Committee Northern Ireland April 2013

1. Replaces CONSENT AND SECONDARY USES OF SERVICE USER INFORMATION IN NORTHERN IRELAND (2009)

Cross-references to the DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information (2012):

2. Code of Practice 2.6

3. Code of Practice 3.4

4. Code of Practice 3.6

5. Code of Practice 3.15 - 3.16

6. Code of Practice 3.17 - 3.24