IMPLEMENTATION TOOLKIT

GOLD STANDARD INFORMATION SHARING PROTOCOL

GUIDANCE NOTE

Implementation Toolkit ITIG0004
Gold Standard Information Sharing Protocol: Guidance Note
Release v.1.0
June 2008

1 Foreword

Information sharing is vital to the concept of modernising government. However, there are often both real and perceived barriers to effective information sharing. In March 2004, the Scottish Executive's 21st Century Government Unit and the eCare Programme jointly commissioned further work to develop understanding of the information sharing issues facing the Modernising Government Fund (MGF) programme as a whole and in particular, to address eCare Information Sharing Protocols (ISPs). Key deliverables included:-

- Comparative analysis of ISPs;
- Assessment of awareness of, compliance with and suitability of the DCA guidance on ISP development;
- Feedback on ISPs to individual partners/local groups;
- Production of a gold standard document with added key issues.

All current eCare partners are currently working on, or have already developed ISPs. However, the absence of central guidance has resulted in some national inconsistencies. Different interpretations of both the law and the provisions of ISPs can in practice result in refusals to share information which is relevant to the care of a service user. The evaluation of existing ISPs and the production of a gold standard document aim to facilitate greater consistency in approach.

Partners can use the gold standard ISP in its entirety, or may choose to refer to this as appropriate. The gold standard should be read alongside this guidance note, which has been produced to allow partners to make the best use of the ISP. Hopefully, partners will find this helpful and informative.

Section 1 –Introduction, Scope and Methodology

1.1 Introduction

The gold standard is a general ISP. This is a high level document which sets out the general principles which will be observed by the parties to the ISP in the sharing of any personal information relevant to the delivery of health and social care services. It ensures that information can be shared in accordance with professional and legal obligations. By its very nature, it requires to be a lengthy document as it contains cross-references to other relevant procedures. It should not be treated as a manual for staff. As it extends to all health and social care services, for both adults and children, it requires to be supplemented with specific staff guidance on information sharing for each client group.

It should be noted that even the most comprehensive ISP is only one part of the information sharing process and so, it is not a substitute for detailed guidance procedures for each information sharing application. However, by agreeing a general framework for secure information sharing, partners can concentrate resources on the development of appropriate policies and procedures in each specific area.

1.2 Scope - Two Tier Approach

Adequate guidance for each information sharing context should however dispense with the need for individual ISPs. It was originally envisaged by the eCare Programme that the two tier approach to eCare would consist of a general ISP outlining the framework for all information sharing, supplemented by an individual ISP, which could address the specific issues pertinent to each client group. However, as stakeholders have indicated that further guidance is still needed, it is now considered that the time spent drafting individual ISPs would be better spent on devising detailed staff guidance for each client group. Otherwise, the approach to information sharing will develop a third tier.

This is further complicated if partners choose to treat adults and children separately, as this will result in partners operating under a general ISP for each, as well as individual ISPs for every individual adult and children client group, which will be difficult to manage and could confuse staff. This would effectively mean a three tier approach for adult services and a further three tier approach for children's services. Although there are specific issues surrounding information sharing on children, for example capacity and consent, the gold standard ISP attempts to address these with broad principles which should be expanded on in detailed guidance procedures.

1.3 Methodology

All available general ISPs have been evaluated by way of a checklist for feedback to partners. This checklist, which incorporates the Department for Constitutional Affairs' Protocol Checklist with additional components, is designed to make feedback as meaningful as possible. The completed checklists refer partners to the gold standard for guidance on areas which have been omitted, or could benefit from further detail. Observations made during this evaluation process have been used to formulate the gold standard, which is based on Glasgow's general ISP. Glasgow appears to be the first local area which is addressing adult and children's services in the same ISP, although a number of other ISPs follow a similar structure in respect of adult services.

Section 2 –Key Provisions of Gold Standard

This remainder of this guidance note will address each of the clauses of the gold standard ISP in turn and give a brief explanation of what they say and why the relevant provisions have been included.

2.1. Introduction

This simply outlines the need for information sharing and the benefits of the ISP. Reference is also made to the requirement for a set of unique guidance procedures for each information sharing context.

This ISP can be adapted as necessary and used as the basis for multi-agency and multi-disciplinary information sharing. Some local areas may wish to extend its application beyond Health and Social Work, for example, to Education and Housing, or perhaps the Police. The Parties should be listed at Section 1.2

Unlike some others, the ISP is drafted as a binding legal agreement between the parties. A binding agreement illustrates the commitment of the parties to the agreed principles and clearly outlines each party's responsibilities for compliance.

Various overarching principles are listed at 1.5. The importance of confidentiality is stressed and one of the fundamental principles is that routine sharing of information will be on the basis of explicit consent of the service user.

It is important to note that the age of capacity is dealt with at 1.5.2. There is a presumption that service users aged 12 or over have capacity to give, withhold or modify consent.

The Data Protection Act 1998 (DPA 1998) does not cover personal information relating to the deceased. However, clauses 1.5.5 -1.5.7 apply the provisions of the ISP to the deceased, subject to the provisions of the DPA 1998 on crime prevention or detection and the access rights contained in the Access to Health Records Act 1990.

2.2 Objectives and Purposes

This section is fairly self-explanatory and simply lists what the ISP is intended to achieve. A good ISP, in the simplest of terms, should broadly outline why information should be shared, how, when and with whom. Focusing on the purpose of the ISP and its objectives should provide clarity for the parties. Although a high level document, this will also ensure transparency should a service user wish to consult this.

2.3 Key Legislation

2.3.1 The Data Protection Act 1998, the Human Rights Act 1998 and Vires

Clause 3 outlines the legislative framework for information sharing. The most relevant legislation is the DPA 1998, the Human Rights Act 1998 ("HRA 1998") and the various legislative provisions which provide public authorities with administrative power. This clause explains that both local authorities and NHS organisations require to act at all times within their legal powers ('intra vires') and that once it has been established that they are not prohibited from sharing information, they must comply with the DPA 1998 and HRA 1998. **Should local areas decide to extend the application of this ISP to areas outwith health and social care services, any other relevant legislation can be outlined here.**

Each party will have their own legal adviser and advice should always be sought if in any doubt about the legality of any particular information sharing exercise. In general however, the ISP proceeds on the basis that most routine information sharing will be done on the basis of consent, which should not present any legal difficulties. If consent has been obtained and relevant information is being shared for one or more of the purposes listed in the ISP (at clause 4), staff cannot go far wrong. The ISP does however stress that in certain limited circumstances, information **must** be shared without consent. On occasion, staff may need to make difficult decisions on whether to share information. The law means that information should not be shared without consent unless this is necessary, yet if it is necessary, the law should not be perceived as a barrier to effective inter-agency communication. Although there are inevitable tensions between information sharing and data protection, the DPA 1998 should not be perceived as conflicting with the protection of individuals. On discussing this project with the Office of the Information Commissioner, who police the DPA 1998, they stressed that data protection must never be used as an excuse for not sharing information when this is necessary.

A service user's data may need to be shared without consent if this is necessary to protect someone's vital interests. This is clearly a fairly high threshold, which will require staff to carry out a risk assessment. The rights of the service user will, on such occasions, require to be balanced with the protection of that service user or perhaps even another individual. Risk assessments are very important. Staff should never refuse to share information without considering the risks associated with this refusal. Such an assessment will ensure that the proportionality principle contained in HRA 1998 (referred to at 3.1.9 and 7.4.4) is complied with. Proportionality recognises that rights are not always absolute and those involved in service delivery often need to balance competing rights. However, this also requires that any interference with rights is the least intrusive possible. This means that if there is a viable alternative to interfering with someone's privacy, which achieves the same level of protection for the individual considered to be at risk, then this is the option which must be taken. It also means that if sharing information is the only way of securing the required protection, careful

consideration must be given to what level of information **needs** to be shared. Staff should always consider whether they can share less information and still achieve the same level of protection. In general terms, if there is a reasonable concern that someone is at risk of serious harm and the best way of avoiding this risk is to share information, this will always override a professional or legal duty to keep information confidential.

It is extremely difficult to provide staff with a formula on how to carry out a risk assessment in an ISP. As already stated, the ISP is not a staff manual. The ISP does however oblige parties to provide staff guidance on risk assessment and to have procedures in place to ensure that staff are not afraid to share information as necessary. However, no guidance can obviate the need for the exercise of professional judgment. It is inevitable that different professionals may have different opinions on risk thresholds. What one member of staff perceives as necessary, another may not, especially when staff are operating under different organisational structures. Staff are in the difficult position that sharing information without justification could expose them to disciplinary action and their employer to legal action, whilst failure to share could have serious repercussions for an individual's protection. The ISP refers, at 7.4, which deals with disclosures without consent, to recent inquiries into service failures in health and social services, where agencies have been criticised for failing to share relevant information. Such inquiries highlight the need for information sharing in specific cases and the fact that in exceptional cases, refusals to share information may also need to be justified. It is essential that staff do not consistently err on the side of caution to the detriment of service users or others. If a decision to share information is challenged, the person who made that decision will be able to defend his position if he can show that the risks were assessed, all relevant factors taken into account and the reasoned view was that there was a sufficient need for the recipient of the information to know.

2.3.2 Caldicott Principles

In addition to DPA 1998, HRA 1998 and the common law duty of confidentiality, NHS parties are committed to the Caldicott Principles, which are listed at 3.1.15. Although the ISP obliges non-NHS parties to respect this, a provision has also been inserted whereby parties agree that the Caldicott Principles do not extend beyond the requirements of the DPA 1998. In this way, the Caldicott Principles should not be a barrier to information sharing which complies with the DPA 1998. Although staff are right to be concerned that the service user's confidentiality is maintained, there is anecdotal evidence that in practice, even when there is a legal justification and in some cases a necessity, to share information, NHS staff are reluctant to do so for fear of falling foul of Caldicott. A concession by the NHS such as that contained in the ISP, could perhaps avoid such situations arising, especially if this is reflected in detailed staff guidance procedures.

2.3.3 Freedom of Information

The Freedom of Information (Scotland) Act 2002 ("the 2002 Act") is referred to at 3.1.16 to ensure that parties are aware that joint procedures will need to be in place to handle requests for information under this Act, as of 1 January 2005. However, although the 2002 Act covers all information held by Scottish public authorities, there is an exemption for personal data, if disclosure would breach the DPA 1998. The 2002 Act will operate alongside the DPA 1998. Any requests from service users for their own personal details will continue to be dealt with under DPA 1998. Requests by an individual for access to someone else's data will however be considered under the 2002 Act. The ISP acknowledges that most information exchanged under its provisions may well be exempt from the freedom of information legislation, as disclosure to a member of the public could breach the DPA 1998.

2.4. Purposes for Which Information is Shared

This section is quite straightforward. Notably, there is provision for additional purposes which cannot be foreseen at the time of drafting. This enables flexibility by ensuring that the same general principles can be applied to such other purposes. As with information sharing already covered by the ISP, guidance procedures should be developed to cover each new information sharing context. **Parties are free to add to the suggested purposes and should outline any other relevant functions and statutory powers as necessary.**

This clause also contains provisions on use and control of personal data.

2.5. Joint Procedures

Although the ISP obliges parties to adhere to any jointly agreed policies and procedures, it also acknowledges that each party will have its own internal procedures which must be followed. Some of the obstacles to effective information sharing arise as a result of inconsistency in approach to procedures on disclosure, access and security. Different organisations often operate under different cultures, especially when dealing in different areas. The ISP obliges the parties to at least attempt to streamline internal procedures and allows partners to require the employees of other parties who are accessing their systems to abide by their policies.

This clause also stresses the importance of good records management and urges the parties to seek advice from records managers. Failure to address this issue when establishing and managing information systems may hinder the effectiveness of information sharing as this is likely to result in time delays and increased costs. If systems are not validated or refreshed regularly, there is a risk that information held will be inaccurate and out of date.

2.6. Subject Access Requests

Dealing with subject access requests is not always straightforward as although the starting point is that an individual has a right to access all of his data, there are a number of exemptions to this right. This can be further complicated when a number of parties hold service user personal information. This clause makes it clear that it is the recipient of a request who is responsible for dealing with this. It does not provide a comprehensive list of the exemptions to the right of access. It simply focuses on the specific exemptions which may apply to health and social work data. It is therefore essential that the parties have detailed subject access request procedures in place for use by staff should a service user request access to his personal information. The ISP is not a substitute for those. 6.1.2 obliges parties to have such procedures in place and to synchronise those where possible. From discussion with stakeholders, it would seem that some partners are further ahead than others in the development of such procedures. Greater sharing of what is already available would therefore be helpful. Renfrewshire Council and Glasgow City Council are two examples of parties who, in addition to corporate subject access request guidelines, have specific social work subject access procedures in place. Presumably, there are also NHS equivalents available.

Although each party will have mechanisms for dealing with subject access requests, clause 6 tries to ensure that the specific procedures which should be followed, should the information requested consist of social work or health data, are clear. This should avoid any delay and enable requests to be dealt with within the statutory time limit. In summary, where the information requested consists of health data, an appropriate health professional, as detailed in 6.1.6, should be consulted before the request is complied with. This is not to obtain his consent to release of the health information, but simply to seek his professional opinion on whether disclosure would be likely to cause serious harm to the physical or mental health or condition of the service user or any other person.

Social work information should also be withheld if this would be likely to prejudice the operation of social work by reason of serious harm to the physical or mental health or condition of the service user or any other person.

Furthermore, information need not be disclosed to someone making a request on behalf of a service user who is a child or an adult with mental incapacity if the service user expects that information not to be disclosed to that person. This provides a safeguard against abuse or potential abuse.

2.7. Disclosure of Personal Information

This clause is extremely important as it broadly outlines when and with whom information should be shared. It covers:-

- How consent should be obtained;
- How consent should be recorded;

- Checking for Consent;
- Disclosures without consent;
- Refusals of consent;
- The duty to have more detailed guidance in place for staff on consent;
- Maintaining contact details;
- Adults with Incapacity;
- Capacity of children.

2.7.1 Obtaining Consent

This section is about ensuring that processing is fair and lawful. The summary of the DPA 1998 at clause 3 explains that fair processing usually means that service users should be told how their information will be used and by whom, whilst lawful processing requires at least one condition from Schedule 2 to the Act (and an additional condition from Schedule 3 if dealing with sensitive data) to be met. (Both Schedules are listed at Appendix 2 of the ISP). Informed consent means that the processing will be both fair and lawful. The need for this is therefore stressed. Service users must be able to understand what information will be shared with whom and for what purpose. This clause describes the best way of achieving this. Although everyone has the right to prevent disclosure of their own information, the consequences of withholding consent must also be explained, as information sharing is for the benefit of the service user. There is however recognition that, in exceptional circumstances, there may be an overriding justification for sharing information without consent. As such, this too should be explained to service users. 7.1.11 obliges the parties to have material available to explain the rights of service users and the procedures which will be followed in relation to their information.

7.1.12 deals with fair processing notices and the need for service users to be told how their information will be used and by whom. **Parties should consult their Data Protection Officers or legal advisers to ensure that their fair processing notice clearly outlines all purposes for which they wish to use personal information. Once the wording for this has been agreed by the parties, the notice should be included as Appendix 5.**

2.7.2 Recording Consent

7.2 is fairly self-explanatory. It is clearly important that refusal to consent is recorded and the consequences of this explained to service users. Systems must be able to accommodate this. Provision is made that when a service user chooses to withhold consent, this information will only be shared in the limited circumstances described in 7.4.

The period of validity of consent must also be clear to both staff and service users. This should therefore be addressed on any consent forms, even if this is explicitly an indefinite period e.g. until consent is explicitly withdrawn. The ISP provides that a child's consent to disclosure to a parent or guardian should be reviewed at the age of 16.

2.7.3 Checking for Consent

7.3 is also straightforward. This merely details the practice to be followed and requires no further explanation.

2.7.4 Disclosure Without Consent

The parties are obliged by 7.2 to have procedures in place which give clear guidance on the circumstances in which information may be disclosed without consent. The general principles outlined in 7.4 must therefore be read alongside more detailed guidance. 7.4 covers the legal framework, the importance of risk assessment, the need to record reasons for, and details of disclosures and for adequate security to be in place.

Although this clause details the penalties for non-compliance with the DPA 1998, it also emphasises that failure to disclose information when this is necessary can have serious repercussions. Decisions must at all times be proportionate. This clause explains the proportionality principle. Professional staff are no doubt accustomed to carrying out balancing exercises in their everyday roles. When deciding whether or not to share information, they must balance the privacy rights of the service user with the protection of that service user or, in some circumstances, another person. If there is a risk to any individual and sharing information is the best way of minimising that risk, the information must be shared. In short, staff should not refuse to share information in any given case, if this would pose a risk to anyone.

Whilst detailed guidance on the mechanics of a risk assessment are outwith the scope of the gold standard ISP and guidance, the importance of reaching a clear and reasoned judgment is clear. It is all too obvious from recent, high profile cases which have highlighted service delivery failures as a result of poor inter-agency communication, that consideration should always be given as to what impact a refusal to share information will have on the particular circumstances.

2.7.5 Staff Guidance on Consent Seeking

Even the best ISP cannot, and indeed is not intended to, cover all practical issues. 7.6 simply stresses the need for more detailed guidance on the whole issue of consent.

2.7.6 Maintaining Contact Details

7.6 also relates to practical arrangements, obliging the parties to maintain details of key members of staff and allocation of responsibilities.

2.7.7 Cases of Uncertain Capacity

The provisions of 7.7 seek to ensure that the best possible treatment is administered to anyone lacking capacity in accordance with the law in this area.

2.7.8 Capacity of Children

Although children are deemed capable of consenting from the age of 12, parental rights and responsibilities are acknowledged at 7.8. **In some cases, there may be a tension between the right of the young person to confidentiality and the need for a parent to know about issues which could affect the welfare of their child. The ISP stresses that under the DPA 1998, disclosures to parents without consent of a young person with capacity require to be justified in the same way as any other disclosure of information, in the absence of consent, to a third party and refers to the possible justifications for this, detailed in 7.4. Professionals should therefore be aware that parents do not have an automatic right of access to information about their children between the ages of 12 and 16. This is not to say that when there is no basis for disclosing without consent, young people cannot be encouraged *if the professionals think it is appropriate* to share or allow the sharing of information with his/her parents.**

2.8. Access and Security Procedures

Clause 8 contains detailed provisions on the transfer or personal information, use of personal information for purposes other than those agreed, restrictions on use of statistical and anonymous data and recording of service user data. All are designed to ensure that a service user's data is kept as safe and secure as possible. Adoption of ISO 17799 (formerly BS 7799) is not obligatory. However, it will be considered best practice, **so ideally, parties could commit to achieving this.** In addition, it would be desirable for parties to streamline existing security procedures where possible. Work is currently ongoing on an NHS Security Compliance Charter which will be of interest to parties once available.

It is stressed that the parties must not use the shared information for secondary purposes. Once in receipt of this information, the recipient has a duty to comply with the DPA 1998, in particular, the first and second data protection principles i.e. personal data must be processed fairly and lawfully and it should not be further processed for any incompatible purposes. The ISP imposes a further obligation on the recipient to seek the consent of the original data controller to any such use, who will decide whether the consent of the data subject should be sought or indeed, if any of the other conditions for processing apply.

2.9. Protocol Management Procedures

ISP implementation is covered by clause 9. It deals with formalities such as formal approval and adoption. However, it also addresses practicalities such as dissemination of information to both staff and the public, as well as staff training. Procedural guidance should only be circulated to staff after internal training to ensure that it is meaningful.

There is also provision on monitoring and review as ISPs should not simply be put in place and be forgotten about. For this reason, it is also important that any breaches of the ISP are monitored. Parties need to focus on how ISPs are working in practice. This should ensure that although the ISP is a high level document, it is not a useless one.

2.10. Contractual Agreement

This clause is important as it outlines the legal responsibilities of the parties. Each party is a joint data controller of shared information and must be registered as such with the Information Commissioner. Parties should check with their Data Protection Officers, or equivalent that their organisations' Notification document contains covers the exchange of information under the ISP.

As explained at Paragraph 2.1 of this guidance, the ISP is a binding legal agreement. It therefore contains an indemnity to ensure that if one party breaches their obligations, all parties do not suffer as a result of this. Resolution of disputes and termination arrangements are also detailed.

Appendices

The Appendices provide further information on the legal framework. These are as follows:-

- Appendix 1 - The Eight Data Protection Principles
- Appendix 2 - Conditions Relevant to the Processing of Personal Data
- Appendix 3 - Determining Disclosure Flowchart
- Appendix 4 - Procedures for Assessing Capacity and Gaining Consent
- Appendix 5 - Template for Fair Processing Notices

Section 3–Further Work

The work done on ISPs is just one part of the Scottish Executive's strategy on information sharing. Other guidance on information sharing has been produced and that the ISP gold standard and guidance should be used in conjunction with these:

Scottish Executive (2003) *Sharing Information About Children at Risk: A Guide to Good Practice*
Scottish Executive (2004) *Data Sharing: Legal Guidance for the Scottish Public Sector*
Scottish Executive (2004*) Sharing Information About Children at Risk: A Brief Guide to Good Practice*

The ISP is also in line with the forthcoming guidance from the Executive on information sharing in Children's Services

The eCare team is commissioning a separate work package to produce user-friendly staff guides. This is being taken forward by one of the local eCare projects. In addition, "standard" eCare training pack is being explored, which will include guidelines on ISP/C&C training/awareness.

A Working Group is also being convened to look at consent and confidentiality issues.