Privacy Impact Assessment with PRAIS

Rae Harbird[1], Mohamed O. Ahmed[1], Anthony Finkelstein[1], Elaine McKinney[2], and Andrew Burroughs[3]

[1] Department of Computer Science, University College London, Malet Place, London, WC1E 6BT
Email: Firstname.Lastname@cs.ucl.ac.uk
[2] Logica UK Limited, 81 George Street, Edinburgh, EH2 3ES
Email: E.Mckinney@logica.com
[3] Coram, Coram Community Campus, 49 Mecklenburgh Square, London, WC1N 2QA
Email: Andrew.Burroughs@coram.org.uk

Abstract. Recent government initiatives have actively promoted information sharing for staff working in social care in the delivery of services. Research has shown however that social workers are sometimes reticent to share or may share information inappropriately despite the availability of guidelines from both government and local authorities. There are no computer-based tools in general use to support practitioners in resolving the issues they are confronted with in deciding when to share, what to share and with whom to share information. To address this deficiency, we are undertaking research intended to clarify the requirements for a privacy mediation tool, PRAIS, which can be used by agencies to ensure that information sharing conforms to legal requirements, fair information processing principles and the conditions set out in local data sharing agreements. In this paper the rationale and design of our prototype for PRAIS are explained.

1 Introduction

UK governments are promoting multi-agency information sharing as a key component of new work practices for those providing services to children and families. At a local level, data sharing between public sector agencies such as health, education, police and social care is governed by data sharing agreements or protocols. These formal agreements cover the collection, sharing and storage of personal data and are ratified by the participating groups. For the individual practitioner data sharing guidance is available from such sources as the Information Commissioner's Office [1], the government [2, 3], and manuals produced by individual agencies. Despite the amount of information available, staff do not always feel confident to share what they know. The need to communicate seems straightforward until you consider that at least seventeen different documents on information sharing have been produced by the UK Government since 2002 [4]. Further problems are reported around the effectiveness of the communications [5]. Where there are no child protection issues and sharing is not mandated,

there have been several instances where sharing has been performed without due diligence or reference to codes of ethics or good practice [6]. It is clear that the process of information sharing in the domain of children's social care is far from clear-cut, and, at the very least, more training and education is needed. Computer-based information sharing is still fairly limited. Data sets are, or soon will be, made available in large, regional repositories such as ContactPoint in England [7], or via a central hub like the eCare system in Scotland [8]. Decisions relating to the privacy protection of individuals have effectively been made during the design phase of the computer software and there are no decision-support tools which aid the practitioner in making complex decisions about whether specific information should be submitted for sharing in a particular context.

More generally, information sharing by organisations and government departments facilitated by new computer systems is increasing apace and the widespread use of computer systems to collect, analyse and share personal information has given widespread cause for concern. Technologies offering opportunities for mass surveillance promise improvements and exciting opportunities in areas such as healthcare services and crime prevention but there may be unintended and undesirable consequences. There are risks associated with growing numbers of people having access to large databases particularly in a healthcare context. In addition, the length of time that records persist might facilitate profiling or social sorting for undesirable purposes. The key challenge for engineers is to design for privacy from the outset [9], and in recognition of this governments around the world are developing their own variation of the Privacy Impact Assessment (PIA) processes. The main objective of performing a PIA is to gain an understanding of the impact which a new process, system or technology may have upon the personal privacy of individuals. Fundamentally the PIA should ensure that the risks to privacy are mitigated and that data is not inaccurate or out-of-date, excessive or used in unacceptable or unexpected ways beyond the control of data subjects. This summary of key PIA principles is taken from [10–14].

1. **Accountability:** An organisation must appoint someone to ensure that privacy policies and practices are followed. Audit functions must be present to monitor all data accesses and modifications.
2. **Purpose:** There must be a clearly specified purpose for the collection and sharing of personal information. Data subjects should be told why their data is being collected and shared at or before the time of collection.
3. **Scope:** Only information that is required to fulfil the stated purpose should be collected or shared.
4. **Limiting use - disclosure and retention:** Data can only be used or disclosed for the purpose for which it was collected and should only be divulged to those parties authorised to receive it. Personal data should be aggregated or anonymised wherever possible to limit the potential for computer matching of records. Personal information should only be kept as long as is necessary.

5. **Personal information:** Treatment of the information must conform to fair information processing practices. Information must be collected directly from the person unless there are very good reasons why this is not possible.
6. **Accuracy:** Every effort must be made to ensure that the personal information shared is accurate.
7. **Safeguards:** Personal information must be protected from loss or theft. Safeguards must prevent unauthorised access, disclosure, copying, use or modification.
8. **Consent:** Data subjects must give their consent to the collection, use and disclosure of their personal information.
9. **Openness:** Privacy policies must be made available to clients.
10. **Individual access:** Clients have the right to ask to see their personal information and to request the correction of perceived inaccuracies. Clients must be informed about parties with whom it has been shared.
11. **Challenging compliance:** Clients must be able to challenge an agencys privacy processes.

All the elements of the PIA process are essential but the process itself is not directly applicable to the situation where a practitioner needs to share information on an ad hoc basis and must consider at least some of these principles as they apply to the immediate situation before acting. There is a need for a privacy impact assessment tool which can be used to address privacy implications dynamically *at the point of sharing*. Such a tool must be integrated into the daily work practices of the individuals using it. It is not intended that PRAIS will ever make decisions on behalf of properly trained personnel but will assist practitioners in making privacy-aware decisions where required.

The remainder of this paper is laid out as follows: Sect. 2 contains a description of our privacy tool, PRAIS which has been designed to address the requirements identified above and Sect. 3 contains information about the prototype developed for the project. In Sect. 4 the related research is reviewed and following this, Sect. 5 contains an critical analysis of PRAIS. Section 6 describes the future work planned and, finally, Sect. 7 concludes the paper.

2 PRAIS

The PRAIS research project has involved a short-term collaboration between: computer scientists from University College London, child protection experts from Coram and information technology professionals from Logica UK. The aim of the project is to develop a prototype decision support tool for context-sensitive, privacy-aware information sharing in children's social care. PIA principles have been used to guide the vision and development of PRAIS, so called because it provides PRivacy impact Analysis for Information Sharing.

Development of a prototype has been an important and necessary first step to encourage potential partners from the Social Services domain where software application development and deployment is sometimes hampered by insufficient

human resources, limited budgets and the unimaginative use of ICT. From previous experience we have found the lack of a prototype through which we can bring abstract ideas to life has been a barrier to participation.

2.1 User Scenario Diagram

The information sharing process is illustrated in the user scenario diagram below; PRAIS sits between the practitioner and the social care data store and mediates all information sharing actions. The privacy policy interpreted by PRAIS is based upon PIA principles, the local data sharing agreement as it pertains to the social care agency and relevant information sharing guidelines. PRAIS is based on the architecture developed for the Identity Governance Framework (IGF) [15]. Information sharing is based on a pull model; this means that the recipients are alerted that information is being made available to them after which it is retrieved from the source. At first this may seem counterintuitive but the IGF architecture supports this design choice because it allows the owner of the information to retain liability for the data and to audit each use. PRAIS will be fully integrated with other social care information systems although these are not shown here.

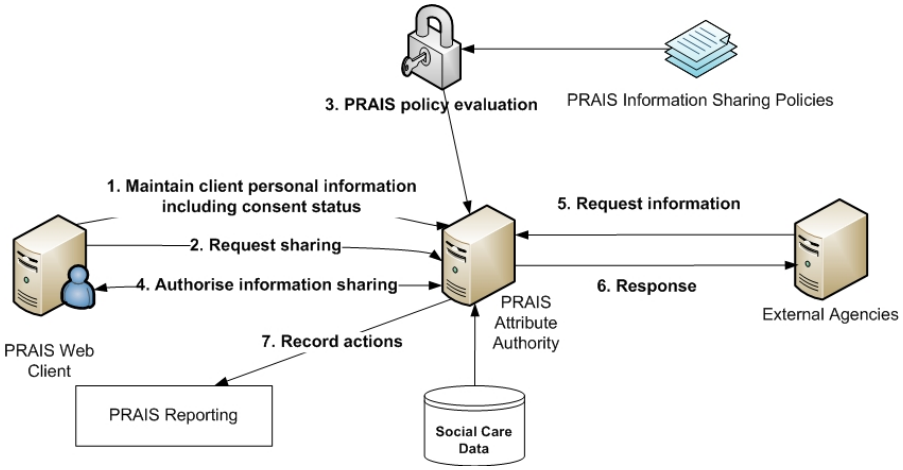

Fig. 1. User scenario diagram

Description.

1. The practitioner uses the computer system to create and maintain all personal information about clients and their consent status.
2. Using PRAIS, a practitioner requests information sharing with an external agency for a specific purpose.

3. PRAIS evaluates the practitioners request. First it retrieves the policy associated with the information sharing purpose and evaluates the rules associated with it. The rules may cover:
   (a) Context - PRAIS will evaluate whether the intended recipients are permitted to receive information about the client for the purpose specified.
   (b) Resources what data may be shared? Is it accurate and up-to-date?
   (c) Consent - has consent been obtained from the data subject for the purpose specified?
   (d) Obligations these are the rules which receiving parties must obey, e.g., data may not be propagated further by the receiver.
4. PRAIS presents the user with a short on-screen report containing recommendations relating to the information sharing decisions and at this point the practitioner may accept or reject these recommendations. If information sharing is authorised then the system sends the intended recipients a message indicating that they may retrieve data.
5. In due course the target agencies request the shared information, stating:
   (a) The attributes to be retrieved,
   (b) The promises made with respect to the data, e.g., recipients may undertake not to propagate the information further.
   (c) The legal context within which the information is requested.
6. The PRAIS system responds with:
   (a) A set of attributes and their properties.
   (b) Exceptions: some of the attributes requested may be unavailable.
   (c) Obligations.
   (d) Consent status, the information may have been shared with or without the owners consent depending upon the reason for sharing information.
   (e) Legal references to legislation relating to the data.
7. Every PRAIS transaction is logged. The system can be configured to notify staff with responsibility for monitoring information sharing with alarms and exceptions.

3 PRAIS Prototype

The PRAIS prototype demonstrates how PRAIS could be used in a social worker's daily routine and is based upon a set of use cases and user scenarios developed by the project team. One of the main findings from early requirements gathering is that although PRAIS can be used for sharing information electronically this may not necessarily be its primary purpose. In social care, information is often shared in multi-agency meetings or over the telephone. This is common working practice enabling staff to explore the meaning and consequences of the information with the person sharing it. To support this type of scenario, PRAIS can be used by practitioners on an ad hoc basis to explore privacy implications where information will be shared verbally. For example: a social worker might want to know whether it is acceptable to share information at a meeting involving particular agency representatives or she may want to telephone a colleague

in another agency to complete enquiries yet feel unsure about how much detail to discuss. In this way, PRAIS is able to act as a comprehensive information sharing resource that can be consulted on any occasion a professional needs to share personal information or learn more about information sharing parameters.

3.1 Information Sharing Scenario - Duty Social Worker Deals With Referral

Much social work practice involves the ongoing evaluation of knowledge and information as a means of assessing risk for children and families. In this scenario the use of both social care information systems and PRAIS is described as a way of showing how the information systems relate to each other. The background to the scenario is followed by a description of a subset of the tasks that a social worker might perform using a computer system. These are:

1. Record information about the referral using a social care information system, described in Tab. 1,
2. Assess whether to share information with other agencies using PRAIS, described in Tab. 2.

The social worker is not bound to follow the information sharing actions advocated by PRAIS, staff will be aware that all information sharing decisions are taken at their own discretion based on, amongst other things, their assessment of risk to the individuals involved. The PRAIS system is designed to assist in the professional's decision making process and not to replace it.

Scenario. A member of the public telephones the Children and Young People's Services (C&YPS) department to report that the children belonging to a family in the street are often playing out until late at night with no apparent parental supervision causing disruption in the neighbourhood. The police have been called to the house and on several occasions, including the previous evening, at least one of the parents returned home late in the evening shouting and behaving in an aggressive manner to the children. The caller believes that the parent was drunk. The duty social worker records information about the call using a computer system to create a referral and information record [16]. Over the next 24 hours, the social worker completes the referral record and performs a risk assessment based upon the available information as it unfolds. A risk assessment tool such as [17] may be used to determine whether the children involved are:

1. At risk of harm and that this is a child protection case or,
2. In need of services,
3. Not in need of further assistance from the C&YPS department at this stage (case closed).

PRAIS is used during the referral completion process by the practitioner to determine which other professionals and organisations may be contacted in relation to the family. Finally, the duty social worker formulates a case workplan

and the completed referral record including the plan is passed to the duty social workers manager for approval. The duty social worker decides that the children may be at risk of harm and she plans to investigate further with other agencies as part of an initial assessment.

Table 1. Task 1 - Complete Referral and Information Record

Task Name	Complete Referral and Information Record
Description	The duty social worker creates a referral and information record for the call. The computer system will automatically fill fields where the child or family have already had contact with the department and will indicate whether there is a worker assigned to the family.
Applications	Social care database application
Actors	Duty Social Worker
Input	1. The social worker completes as much information as possible in the referral and information record. Reasons for referral are taken from [18] and are: (a) FDO1 - Suspected Poor Parenting Skills and, (b) MS08 - Children affected by the misuse of alcohol by parents or other family members. 2. If the children are or family is already known to the C&YPS department then their details will be completed automatically for the social worker. In this case, the duty social worker is able to tell immediately that the family in question does not seem to be known to the department. 3. Based on the information gathered, the duty social worker decides that since the family have allegedly received visits from the police concerning alcohol-related incidents the case merits child protection status at this stage.
Output	The output is a completed or partially completed referral form.

3.2 Information Sharing

The PRAIS prototype has been engineered as an expert system comprising three components: a user interface, a knowledge base containing privacy-related facts and rules and an inference engine which can interpret the knowlege base and draw conclusions. The user interface has been developed as a web application and the expert system is written in prolog. As a result, it is possible to perform what is known as forward and backward chaining through the facts and rules. This means that if we have reached the conclusion, say, that it is acceptable to share certain information with an agency, the expert system will be able to tell us how the decision was reached; this is known as backward chaining. Alternatively,

Table 2. Task 2 - Evaluate with whom to share information

Task Name	Evaluate with whom to share information
Description	The duty social worker uses PRAIS to assess whether she may share information with the police in order to find out whether they have had any recent contact with the family.
Applications	Social care information system and PRAIS
Actors	Duty Social Worker
Input	1. The duty social worker brings up the referral and information record on the screen and selects the PRAIS information sharing function. 2. The system asks the duty social worker to input some details about: (a) the information sharing purpose, in this case: gathering information for completion of the referral and information record, and, (b) the agency that she wishes to share information with, in this case, the police. 3. PRAIS evaluates whether it is desirable to share under these circumstances, taking into account the fact that the duty social worker has recorded that the case may warrant child protection status.
Output	1. PRAIS informs the duty social worker that she is mandated to share information about the family at this stage. Primarily, this is because the social worker has decided that the children in the family may be at risk of immediate harm.

PRAIS could be queried to determine what else is required to satisfy the sharing constraint; known as forward chaining. The prototype embodies a subset of the PIA principles described in Sect. 1 as a means of illustrating the dynamic PIA process. The information sharing process is illustrated in the semantic network in Fig.2.

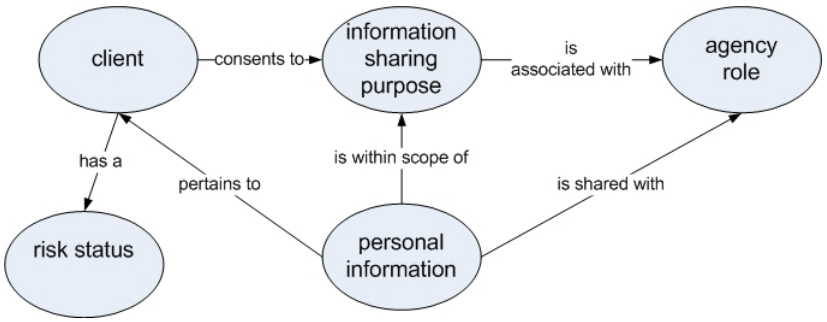

Fig. 2. Information Sharing Policy Model

Description of Nodes and Edges.

1. **Client:** any person about whom the agency records information. A client must explicitly give consent for their information to be shared for a specific information sharing purpose.
2. **Personal information:** this is any information about a client. Information is expected to be structured conforming to well-known formats to enable a high-level of granularity with respect to sharing conditions. Although sharing rules can be specified on a field-by-field basis it should also be possible to specify rules for groups of information items such as records.
3. **Agency role:** this is a member of staff in an agency performing a particular role, for example: A teacher at a child's school or the health visitor at the child's GP surgery. Information is shared with a specific agency role and to control this, PRAIS has elementary role-based access control functionality embedded in it. Sharing is tightly constrained and is only permitted if all the relevant rules have been satisfied.
4. **Information sharing purpose:** an organisation will have a set of valid reasons or purposes governing the circumstances under which information may be shared. This can be thought about as the sharing context. Each context has items of personal information associated with it and this association is used as a means of limiting the scope of information sharing, confining it to only those items of information that are relevant. The information sharing context is also associated with a set of agencies. Again, this relationship is used to limit the scope of information sharing so that personal information is not distributed to those parties who do not have the right to see it.

5. **Risk status:** every child or young person has an associated risk status. The significance of this is that when a child is considered to be at risk of harm, a practitioner must override any other conditions that prohibit information sharing with agencies; they are mandated to share the information. The social worker assigned to the child is responsible for assessing and recording risk status and will generally use a risk assessment tool for doing so.

3.3 Information Sharing Logic

PRAIS makes information sharing decisions using the rules listed in Fig.3.

Rule 1 (R1): If the child is considered to be at risk of harm then the information must be shared with the target agency roles.
Rule 2 (R2): A client must have given consent for their personal information to be shared for the specific information sharing purpose chosen.
Rule 3 (R3): The target agency role must be permitted to receive information for the sharing purpose selected.
Rule 4 (R4): The personal information selected for sharing must be within scope of what it is appropriate to share for the context chosen.

Fig. 3. Information Sharing Rules

The rules are evaluated according to the pseudocode in Fig.4

```
if R1 is true then
        share information
else if (R2 is true and R3 is true and R4 is true) then
        share information
end if
```

Fig. 4. PRAIS Logic

which can be more concisely expressed in formal logic as:

$$share \Leftrightarrow R1 \vee (R2 \wedge R3 \wedge R4) \tag{1}$$

3.4 PIA Report

The information sharing decision is presented to the user as a summary on-screen report elaborating the the reasons why information sharing is recommended or

discouraged. In recognition of the fact that information sharing decisions may not always be clear cut, future versions of the prototype will represent the risk to a person's privacy inherent in a sharing action using probability calculus. In this case a practitioner could be given information about the risk of compromising the personal information through the sharing action. The results could be presented to the user in terms of the liklihood of compromise.

4 Related Research

To date research relating to the electronic sharing of information in a social care context has been limited. One notable exception is the Framework for Multi-agency Environments or FAME. FAME was initiated in 2003 [19], as part of the UK's e-government project funded by the Office of the Deputy Prime Minister. The project materials provide guidance to groups of agencies wishing to share information. The core architecture is a hub and spoke model and a brokerage system at the hub takes requests from one agency and retrieves the appropriate data from the information provider. Organisations using the FAME model are free to implement it as desired as FAME is not based on any particular technology nor is it standards-based. Each information-sharing project must be implemented as a separate solution and the security measures are also project specific. Privacy impact assessment takes place prior to development and decisions about privacy are not taken dynamically.

Conversely, information security in the healthcare domain have been very actively researched over more than a decade. In 1996 Ross Anderson developed a security policy for healthcare computer systems on behalf of the British Medical Association [20]. Fundamentally, the way we design computer systems has an impact upon the level of protection that can be afforded to person-related information. This has been borne out in practice many times as modern information systems with poor design have contributed towards the violation of individuals' privacy. In particular, the centralised storage of records containing private information is likely to cause the breakdown of privacy and confidentiality as the subversion of security systems by humans is much easier where large amounts of information is managed in one place.

At the enterprise level, the enforcement of data protection principles in the management of information been addressed in work at HP Labs [22]. The authors investigated new ways to implement privacy obligation policies suitable for the entire information management lifecycle including data retention and deletion. Parallels exist in [23], where compliance with data protection legislation is achieved using the set of technologies that form part of IBM's Hippocratic Database including a policy creation interface, an enforcement engine and a compliance auditing component. This work has been extended [24], to address requirements for distributed regional healthcare entities sharing information. Policy constraints are packaged with data at the point of transfer and interpreted by the receiver.

Secure information dissemination in distributed healthcare environments using publish/subscribe mechanisms is described in [25]. Again, data is packaged with security policies relating to both publisher and subscriber and policies are enforced by brokers in the network controlling the flow of data between domains. In [26] the secure use of electronic health records in a distributed environment is achieved using OASIS, a distributed, extended role-based access control system. Unlike the previous examples, policy does not travel with the data and access to information sources is mediated by a network of OASIS servers.

Privacy policies governing access to data can be expressed as a set of rules using machine-readable languages such as EPAL [27] or XACML [28]. Both languages allow the representation of privacy-related concepts such as the purpose of an action, whether consent has been given for the action and the identity or role of the user requiring access. EPAL and XACML have comparative strengths and weaknesses and these are explored in [29]. Other research groups have started from the premise that privacy considerations should be fully integrated with an access control model and have extended Role Based Access Control to accomodate privacy enforcement [30]. Usability with respect to privacy policy authoring tools is explored in [31] and SPARCLE, a privacy policy workbench, is used to define privacy policies using either natural or structured language. User-defined policies can be translated to a variety of machine readable formats by the workbench.

5 Discussion

Our vision of PRAIS is as a tool which will enable personnel working with personal information to assess the privacy implications of information sharing actions dynamically and to share information with confidence, whether verbally or electronically. This has been achieved by accommodating the daily routines of social care staff from the outset thus realising the intention to place privacy considerations at the forefront of work practices. PRAIS is based on a secure, standards-based framework which supports electronic information sharing between federated information sources. This a more secure model than that offered by a centralised architecture enabling the owners of the information to retain better control. PRAIS encompasses a set of simple privacy rules which are implemented as an expert system. This enables reasoning about sharing decisions reinforcing the training capabilities of the tool and helping users to understand why decisions have been reached.

The design of PRAIS has a wider application than the scenarios depicted here and could be used in other areas where professionals have to share such information even where this takes place across legal jurisdictions. PRAIS encapsulates fair information processing principles and, as such, could assist a wide spectrum of organisations to deal with sharing personal information and training staff in privacy issues.

6 Future Work

In the immediate future we will be working towards securing a partner in a UK Social Services department with whom we can develop an operational version of PRAIS and evaluate its efficacy in a realistic environment. We intend to refine and develop the requirements and design for PRAIS so that we have a more complete picture of how the domain should be modelled as a precursor to expressing and enforcing privacy policies. Recent work with privacy-extended RBAC models seems a promising starting point as these appear to encapsulate some of the concepts we have used such as consent, information sharing purpose and obligations.

PRAIS cannot exist in isolation and must be supported by a set of subsidiary security-related capabilities, these are:

1. Identity management functions for authentication and authorisation of both practitioners and external agencies.
2. Privacy policy management functions to support policy authoring and policy compliance management.
3. A common data model for social care. A widely accepted Electronic Social Care Record (ESRC) is needed to support information sharing facilitating electronic data sharing agreements which are at least part-validated by machine.
4. Data matching and mapping functions. Information transfer between organisations with heterogeneous information sources may imply the need for data matching and mapping so that that records and fields can be linked without the need for common identifiers or a common schema.
5. Information life-cycle management. Organisations have responsibility for managing the data they collect securely and this includes disposing of data once it has served its intended purpose. Tools to assist with automatic information housekeeping are a necessary part of the privacy toolbox.

In the longer term our vision is broader: we envisage that PRAIS will help both policy makers and decision makers to address, not only the legal, but the moral and ethical issues involved with information sharing. PRAIS will improve the timeliness and the quality of data sharing and help staff to manage the negative impacts of information sharing where these occur. PRAIS may also be used as a training tool to help professionals learn experientially about the issues in managing personal information.

7 Conclusion

Much of the information sharing in social care can be described as ad hoc and workers are expected to interpret written guidance to ensure that proper care is taken with personal information. It is our belief that the privacy implications of sharing can be at least partially evaluated by computer. The aim of the PRAIS project is to develop a a policy-based tool which can analyse information sharing

decisions on-demand. To date we have developed an innovative prototype and our next step is to implement a set of representative scenarios using a policy engine to demonstrate the feasibility of the PRAIS vision. This initial work should be seen in context as part of a much broader picture in which PRAIS will form an integral part of the day-to-day business process of information sharing. Eventually, PRAIS will operate as part of a risk assessment framework evaluating the predictability of particular sharing outcomes using mechanisms which are generic yet flexible enough to be applied to a wide range of industry sectors such as finance, education and healthcare.

References

1. Information Commissioner's Office: Framework code of practice for sharing personal information. http://www.ico.gov.uk/, last accessed on February 17th, 2008 (2007)
2. Department for Education and Skills: Information sharing: Practitioners' guide. http://www.ecm.gov.uk/, last accessed on February 17th, 2008 (2006)
3. Department for Education and Skills: Information sharing: Further guidance on legal issues. http://www.ecm.gov.uk/, last accessed on February 17th, 2008 (2006)
4. Richardson, S., Asthana, S.: Inter-agency information sharing in health and social care services: The role of professional culture. British Journal of Social Work **36** (2006) 657–669
5. Munro, E.: What tools do we need to improve identification of child abuse? Child Abuse Review **14** (2005) 374–388
6. Anderson, R., Brown, I., Clayton, R., Dowty, T., Korff, D., Munro, E.: Children's databases - safety and privacy. http://www.ico.gov.uk/, last accessed on February 17th, 2008 (2006)
7. Department for Children, Schools and Families: Contactpoint. http://www.ecm.gov.uk/deliveringservices/contactpoint/, last accessed on February 17th, 2008 (2007)
8. Scottish Executive, Data Sharing & Standards Division: eCare technical workshop. http://www.scotland.gov.uk/Resource/Doc/923/0019775.ppt, last accessed on February 17th, 2008 (2005)
9. Royal Academy of Engineering: Dilemmas of privacy and surveillance: Challenges of technological change. http://www.raeng.org.uk/, last accessed on February 17th, 2008 (2007)
10. 6, P., Birch, A., Copping, M., Raab, C.: Information sharing for children at risk: Impacts on privacy, eCare programme. http://www.scotland.gov.uk/About/FOI/Disclosures/2007/06/Impacts/, last accessed on February 17th, 2008 (2004)
11. Clarke, R.: Xamax consultancy - PIA guidelines. http://www.xamax.com.au/, last accessed on February 17th, 2008 (1999)
12. Office of the Privacy Commissioner of Canada: Fact sheet: Privacy impact assessments. http://www.privcom.gc.ca/, last accessed on February 17th, 2008 (2007)
13. The Office of the Privacy Commissioner: Privacy impact assessment guide. http://www.privacy.gov.au/, last accessed on February 17th, 2008 (2006)
14. Information Commissioner's Office: PIA handbook. http://www.ico.gov.uk/, last accessed on February 17th, 2008 (2007)

15. Liberty Alliance Project: Id governance - identity privacy and access policy, marketing requirements document. http://www.projectliberty.org/, last accessed on February 17th 2008 (2007)
16. Department for Education and Skills: Referral and information record. http://www.ecm.gov.uk, last accessed on 17th February, 2008 (2003)
17. The Bridge Child Care Development Service: BridgeALERT, key information for identifying children in danger (1998)
18. Scottish Social Care Data Standards: Recording of children and families referral reasons. http://www.scotland.gov.uk/, last accessed on 17th February, 2008 (2004)
19. Morrison, K.: FAME - the key to multi-agency working. eGov monitor (2004)
20. Anderson, R.: A security policy model for clinical information systems. In: IEEE Symposium on Security and Privacy. (1996) 30–43
21. Denley, I., Weston-Smith, S.: Implementing access control to protect the confidentiality of patient information in clinical information systems in the acute hospital. Health Informatics Journal **4** (1998) 174–178
22. Mont, M.C., Beato, F.: Tech report: Hpl-2007-7: On parametric obligation policies: (2007)
23. Johnson, C.M., Grandison, T.W.A.: Compliance with data protection laws using Hippocratic database active enforcement and auditing. IBM Syst. J. **46** (2007) 255–264
24. Grandison, T., Ganta, S.R., Braun, U., Kaufman, J.: Protecting privacy while sharing medical data between regional healthcare entities. Stud Health Technol Inform **129** (2007)
25. Singh, J., Vargas, L., Bacon, J.: A model for controlling data flow in distributed healthcare environments. In: Proceedings of Pervasive Health 2008: 2nd International Conference on Pervasive Computing Technologies for Healthcare, Tampere, Finland 30 (2008)
26. Eyers, D.M., Bacon, J., Moody, K.: OASIS Role-based Access Control For Electronic Health Records. In: IEE Proceedings on Software, 153(1), IEE (2006) 16–23
27. IBM Zurich Research Laboratory, Switzerland: Enterprise privacy authorization language EPAL 1.2, IBM research report. http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/index.html/, last accessed on April 11th 2008 (2003)
28. OASIS: eXtensible access control markup language (XACML) v2.0. http://www.oasis-open.org/home/index.php, last accessed on April 11th 2008 (2005)
29. Anderson, A.H.: A comparison of two privacy policy languages: EPAL and XACML. In: Proceedings of the 3rd ACM Workshop on Secure Web Services, New York, NY, USA, ACM Press (2006) 53–60
30. Ni, Q., Trombetta, A., Bertino, E., Lobo, J.: Privacy-aware role based access control. In: SACMAT '07: Proceedings of the 12th ACM symposium on Access control models and technologies, New York, NY, USA, ACM (2007) 41–50
31. Brodie, C., Karat, C.M., Karat, J., Feng, J.: Usable security and privacy: a case study of developing privacy management tools. In: SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security, New York, NY, USA, ACM (2005) 35–43