Privacy Impact Assessment – Activity Recording and Scheduling Project (Adult Care)

Version 0.4

Version History			
Version	**Date**	**Detail**	**Author**
0.1	23/11/2017	First Draft	
0.2	15/01/2018	Review and amendments	
0.3	16/01/2018	Additions	
0.4	16/01/2018	Final Review	

CONTENTS

INTRODUCTION 3
ANNEX A 3
PRIVACY IMPACT ASSESSMENT SCREENING QUESTIONS 3
ANNEX B 4
PRIVACY IMPACT ASSESSMENT TEMPLATE 4
ANNEX C 14
LINKING THE PIA TO THE DATA PROTECTION PRINCIPLES ERROR! BOOKMARK NOT DEFINED.

Introduction

The Council has undertaken a Privacy Impact Assessment (PIA) of its Procurement for an Activity Recording and Scheduling Solution to be used by Adult Care.

Annex A

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Will the project involve the collection of new information about individuals? No

Will the project compel individuals to provide information about themselves? No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? No

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? No

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. No

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? No

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. Yes

Will the project require you to contact individuals in ways that they may find intrusive? No

Annex B

Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The introduction of an Activity Recording and Scheduling Solution will provide visibility of the service delivered through real time monitoring of actual service delivery against commissioned hours for the entire Home Care Service as provided by both Direct Care and Independent Sector Providers. Payment to Independent Sector Providers will only be made on approved and agreed business rules embedded in the system. This process will be based on actual care delivered and monitored, rather than paying suppliers on invoices provided for the care carried out. This will provide the Council with the means to use and control its budgets effectively.

The current systems used to support Home Care services do not contain sufficient functionality to support Adult Care's future requirements, particularly in relation to utilising innovative technologies and ensuring additional identified efficiencies and benefits can be realised (both for the Council and for clients supported by Adult Care).

The procured Solution will be used by the Council's Direct Care Home Care Teams as well as the Independent Sector Providers that are commissioned to deliver Home Care Services on behalf of the Council. The Solution will also be used by Direct Care to schedule Home Care Worker visits and record information including arrival and departure times of each visit as well as activities undertaken. The recording of information will be carried out using mobile phones with an application installed, which will allow the Home Care Workers to move away from using the clients' landline phones to record the start and end of visits. In doing this, it will allow the Home Care Worker more contact time with the client, resulting in a more personal level of care and more efficient use of time. The integrated solution will also allow payments to be made to the Council's in-house Direct Care staff as well as payments to the Independent Sector Providers.

The new Solution will act as an enabler to improve the quality of service delivered and also generate cashable savings by ensuring that the care commissioned by Adult Care on behalf of clients is what is actually delivered,

whilst also enabling a clients' service needs to be matched with the most appropriate Home Care Worker.

The PIA screening questions were answered and provided 'yes' answers to the following questions:

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

The collection of data will be done via the Council's ESCR system Mosaic (previously Frameworki). The Activity Recording and Scheduling (AR&S) Solution will display certain information which is held in the ESCR through an integration between the two systems. The fields required for the AR&S would then be imported from the ESCR. Client demographic information which will be held in the new AR&S solution (imported from the ESCR) will include; Client PIN, ESCR Ref, NHS Ref, First and Surname, D.O.B, Telephone, Emergency Contact details, Power of Attorney details, GP details, key safe number and full address. This information will be used to schedule care visits using a best match algorithm and to contact the individual/next of kin with regards to any changes to a scheduled visit.
The AR&S Solution will also be required to store information relating to the Home Care Worker. This includes HR data such as name, address, contact details, training records, medical clearance and contracted hours. The majority of the information held relating to the Home Care Worker will be fed from the Corporate SAP system; amendments to this data will be performed in SAP. Additional information which is not stored within SAP relating to a Home Care Worker will be inputted and maintained via the solution. This information will be used by the solution to schedule visits to clients and assist manager's communication, and maintaining professional development. This will cover, for example, whether a worker smokes, is allergic to animals and any particular requirements about availability and non-availability for work.

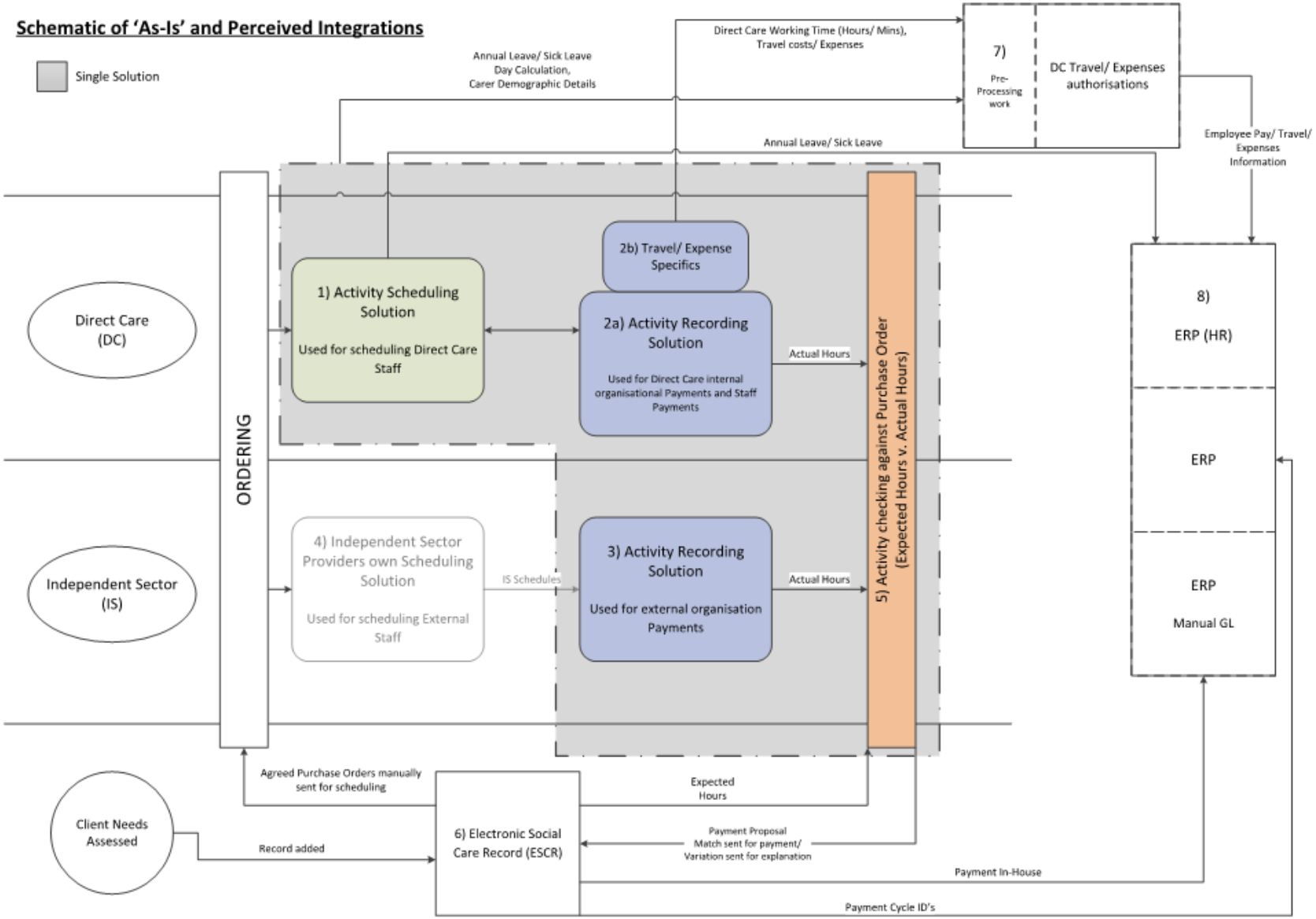
Both sets of data will be used:

- To produce a best match when scheduling the home care workers visits to clients;
- To send the relevant information to the home care worker in the form of a schedule using a mobile application; and
- General contact information for the Home Care Worker's manager and client.

The weekly provision of Home Care services across the county consists of approximately:

- 1,550 Clients; and
- 1,000 Home Care Workers;

Please see the following page for a flow diagram of how the data is envisaged to be processed:


Schematic of 'As-Is' and Perceived Integrations
Single Solution
Annual Leave/ Sick Leave
Day Calculation,
Carer Demographic Details
Direct Care Working Time (Hours/ Mins),
Travel costs/ Expenses
7)
Pre-Processing work
DC Travel/ Expenses authorisations
Employee Pay/ Travel/ Expenses Information
Annual Leave/ Sick Leave
Direct Care (DC)
Independent Sector (IS)
Client Needs Assessed
ORDERING
1) Activity Scheduling Solution
Used for scheduling Direct Care Staff
2b) Travel/ Expense Specifics
2a) Activity Recording Solution
Used for Direct Care internal organisational Payments and Staff Payments
Actual Hours
4) Independent Sector Providers own Scheduling Solution
Used for scheduling External Staff
IS Schedules
3) Activity Recording Solution
Used for external organisation Payments
Actual Hours
5) Activity checking against Purchase Order (Expected Hours v. Actual Hours)
8)
ERP (HR)
ERP
ERP
Manual GL
Agreed Purchase Orders manually sent for scheduling
Expected Hours
Record added
6) Electronic Social Care Record (ESCR)
Payment Proposal
Match sent for payment/
Variation sent for explanation
Payment In-House
Payment Cycle ID's

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Audit Services and the Information Security team have reviewed the Invitation To Tender documents and Audit Services have performed due diligence on the selected highest scoring tenderer which included a site visit to the head office and testing of the solution and mobile application to ensure that data is held in a secure manner at every stage. Further assurance was gained from the independent ISO27001 accreditation of the data centre which holds the solution and the penetration testing that is undertaken.

Once the Solution is live, the Contractor will be expected to undertake regular security checks to ensure that the data cannot be breached, as defined in the Contract.

Contract management meetings will include an operational review of any incidents relating to individuals.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Client/staff data is accessed by unauthorised persons and used or shared inappropriately.	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information	Breach of Principle 7 of the Data Protection Act	Financial and reputational damage. Legal action could be taken against the LA and possible substantial fine

If a retention period is not established, information might be held for longer than necessary.	Data becomes out of date and could be inaccurate	Breach of Data Protection Principles 4 and 5	Financial and reputational damage
Ensuring data subjects, i.e. Clients and Staff, are aware of rights under data protection legislation relating to processing of data for these requirements.	Individual's privacy is compromised by breaching rights of a data subject in relation to their personal data, including right to withdraw consent.	Breach of Principle 6 of the Data Protection Act	Reputational damage and potential fines
Data may be updated manually within the system but due to the nightly data feed from the ESCR or SAP the manual changes will be overwritten and data could be incorrect	Inaccurate data and consequent risk to the safety of clients and staff.	Breach of Principles 4 & 7 of the Data Protection Act	Reputational damage and potential fines

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Client/Staff data is accessed by unauthorised persons and used or shared inappropriately.	Access to the System / mobile app will be limited to only those with the correct role based access activity. How this is managed will be determined by system administrators (desktop solution) and Home Care managers (mobile app). This will be managed by Adult care locally through relevant training and guidance.	Accepted/Reduced	
If a retention period is not established, information	Information will remain in the solution for a period of	Accepted/Reduced	

might be held for longer than necessary.	time defined by Adult Care retention periods.		
Ensuring data subjects, i.e. Clients and Staff, are aware of rights under data protection legislation relating to processing of data for these requirements.	Personal data used by the Local Authority will be compliant with the new GDPR regulations and will refer to rights of data subjects, including right to withdraw consent and process for doing so.	Eliminated	
Data may be updated manually within the system but due to the nightly data feed from the ESCR or SAP the manual changes will be overwritten and data could be incorrect	Ensure that correct training is provided to Home Care Managers to ensure they are aware of which solution they should be updating client records in.	Reduced	

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
Could be accessed or hacked if not secure.	The system is held in a robust network, protecting data integrity and holding data securely. The solution can also provide separate environments for test, quality assurance and production where required. The data is secured in transit via SHA256 certificates. The supplier works in compliance with their ISO27001 (Information Security), ISO22301 (Business Continuity) and ISO9001 (Quality) accredited Management Systems.	DCC Information security, Audit Services and Server Management teams.
Person(s) accessing the data and using it for unauthorised means.	All staff who have access to the data are DBS checked. Secure storage of data complies with Audit requirements as part of due diligence process and all access to the data requires password protection in line with DCC requirements and all access produces an audit trail for additional security.	As above

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Project team to review PIA outcomes and ensure implementation plan reflects the approved solutions.	Expected to be by the implementation of the system. It is anticipated the solution will go live towards the end of 2018	Project Team. Situation monitored via DCC contract management review and operational review process
Testing of technical solution including mobile application and controls before 'Go-Live'	Autumn 2018	Project Team (Project managers and Adult Care DSOs)
Oversight and evaluation of the project against the success criteria.	TBC	Project Board

Contact point for future privacy concerns

Annex C

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project? **Yes**

How will you tell individuals about the use of their personal data?
Consent is sought at the point when Adult Care becomes involved with a client and a statement on the use of data is included on appropriate assessment and review forms. New home care staff are told about the PID information held and why at the point of induction.

Do you need to amend your privacy notices? **No**

Have you established which conditions for processing apply? **Yes**

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn? **N/A**

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8? **No**
Have you identified the social need and aims of the project? **Yes**
Are your actions a proportionate response to the social need? **Yes**

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data? **Yes**

Have you identified potential new purposes as the scope of the project expands? **No (The scope of the project will not expand)**

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used? **Yes**

Which personal data could you not use, without compromising the needs of the project? **We only use the required data to provide the service.**

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary? **Yes**

How are you ensuring that personal data obtained from individuals or other organisations is accurate? **N/A – DCC data sources used only.**

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?
In line with the Adult Care retention policy.

Are you procuring software that will allow you to delete information in line with your retention periods?
The ability to delete information was specified in the tender documentation and can be achieved.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily? **Yes**

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose? **N/A**

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified? **Yes**

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

- **3 x Council Technical Support;**
- **4 x System Administrators;**
- **5 x Home Care Managers;**
- **3 x Adult Care Finance Officers.**
- **Train the trainer approach will be used to train other system users.**

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA? **No**

If you will be making transfers, how will you ensure that the data is adequately protected?
The provider will ensure any data transfer from/to their data centre is secure.

Conditions for processing under the Data Protection Act can be found at;
https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/