Data Privacy Impact Assessment

Document Control Sheet

Q Pulse Reference Number	SOP-F-IG-5
Version Number	02
Document Author	Information Governance Manager
Head of Department/Executive Director Job Title	Director of Finance & Resources
Head of Department signature	
Date Approved	17 July 2018
Date form Effective From	17 July 2018
Next Review Date	17 July 2021
Keywords	Data controller; data processor; data protection; DPIA; information asset owner; governance; privacy; risk assessment; system.
Target Audience	Senior Managers, Information Asset Owners

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

Introduction

This DPIA template is based on the Information Commissioner's Office (ICO) template of how you can record your DPIA process and outcome. It follows the process set out in the ICO DPIA guidance, and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

1. Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Microsoft SharePoint has been evaluated against current Trust solutions, in particular the intranet and QPulse. Every member of staff throughout NEAS rely on these systems and through research, it is clear they fall short in numerous aspects. A business case has been approved to replace them with SharePoint Online, a cloud based Microsoft solution. An investment has already been made in this technology with a number of proof of concept solutions in use today.

The ultimate aims are:

- better user experience for finding, using and sharing information anywhere at any time via any device
- a more productive workforce due to increased levels of collaboration and better communication across the Trust
- modern document management with intelligent search functions to enhance and improve the current user experience of locating policies and procedures
- replacing inefficient paper based / outdated processes with efficient electronic workflow

Microsoft is recognised as a leader by analysts in six Gartner Magic Quadrants and Forrester Waves. SharePoint is Microsoft's enterprise digital workspace and is widely used throughout the NHS and in 85% of the Fortune 500 organisations. Using this technology means members of staff can access all the information, data and applications needed to do their work and in the most efficient and flexible way.

Objectives of using SharePoint
- A new intranet platform
- Team Sites for collaboration, repeating the success of The Lamp
- Electronic workflow to supplant cumbersome paper process
- A new Document Management System to replace QPulse

Business_case
PID

2. Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Collection:
Data (in the form of Word, Excel, PDF, PowerPoint files) will be saved by all end users to SharePoint in the form of team sites, document libraries and lists. Information storage will be overseen by a Digital Ambassador who will administer the site.

Use:
Information stored on SharePoint can be access controlled and this will be managed via job role. Departments will have a forward facing site open to everyone and a closed site only available to staff working on draft documents, working files etc. No confidential data will be stored on SharePoint. This will continue to be held in the current solution on the network.

Store and deletion:
Files will be stored and deleted by end users as and when necessary – similar to the N Drive process now. Record retention rules can be set up against the information to send alerts when nearing time for deletion as per legislation.

Information Sharing:
Information used on SharePoint will be shared much in the same way it is now, however with the added benefit of version control and live links. Instead of sending bulky attachments that result in several versions with different amendments, a single link can be sent to a person/team. Information sharing between colleagues in different departments can be managed through links across team sites and document libraries and through the use of workflows which sends only what is needed for approval to those who require it. Further, the access to data can be limited by restricting access to documents, folders, and parts of team sites.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is corporate and will be similar to that currently held and used on the N Drive. However, it is anticipated information stored will be better managed and data that should be held in systems will reside exactly there.

Data will be stored in the cloud at a data center based in England. Only staff working for NEAS will be using the SharePoint solution.

In the first phase of the Digital Transformation Project, no personally identifiable data will be included and the "Confidential Drive" will stay in place. Going forward from this, a further assessment can completed to reflect the shift from on premise confidential data to it being stored in the cloud.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Informatics Manager is the Project Manager and will be the IAO of SharePoint. There is also a Project Lead in place to engage staff and oversee progress.

In terms of processing data on SharePoint, there will be different levels of control:
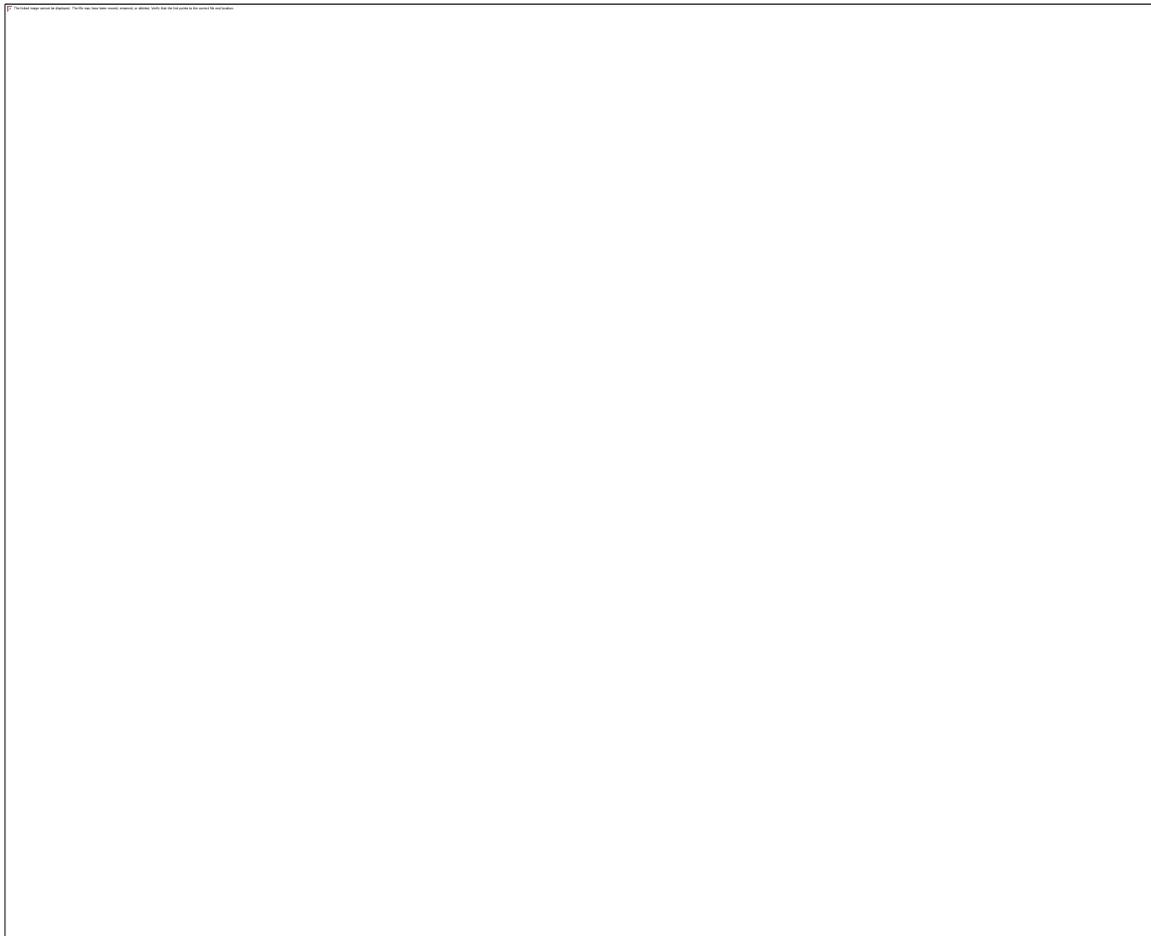
Admin and Developer will have the most rights and will be limited to only a few people in the Trust. Digital Ambassadors will cover the Power User and Content Editor. The access rights to these roles will differ and be limited to those who need each level of access depending on job role. All staff will be End User.

Those with Develop and Admin level of access control the permissions granted during team site role out. They will go on to devise and implement request procedures for team site permissions this may well be handled by submitting an IM&T Service desk request moving forward after the closure of the Project. This information could then be updated in the Information Asset Register to keep track of who has what level of access in the system.

The Power User will develop and maintain team site work flows ensuring they are fit for purpose and efficient in their process flow and output. They will create surveys and will be daily involved in SharePoint. Again, this role will be given to those depending on job role within a team.

The content editor will be responsible for the maintenance of their respective Team Site, ensuring documents are up to date and the correct version in displayed. They will ensure site content is up to date and relevant and discussion forums are in line with NEAS policy.

The Digital Ambassador role will only be open to employees of NEAS and will not include volunteers or those otherwise outside of the NEAS network. When creating team sites for HART, Ambulance volunteers and medicines management for example that can be shared with third party companies with whom we are contractually tied the senior manager in each team will be responsible for the release of information to third parties in line with the contractual agreements in place.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Replace the current intranet with a SharePoint based solution to improve the user experience and functionality of the intranet.

Replace the corporate Policies and Procedures management system which is currently based on QPulse. This will benefit NEAS by not renewing our annual license. Manual updates to QPulse regarding staff job roles will cease as SharePoint automatically integrates with ESR / AD. This will take a huge burden off staff to administer. As the SharePoint document management solution will be part of the intranet, additional log in steps will no longer be required.

Roll out team sites within NEAS to repeat the success of The Lamp. This includes the creation of consistent fully branded templates to enable collaborative working, reduce time taken by staff to find and access documents / information and reduce duplication of work. There will be an ongoing facility to support and further develop these processes via the Informatics Department.

Provide a service to introduce electronic workflow to replace manual paper based processes which are inefficient, error prone and costly. To ensure this is contained, electronic workflow will be built in with team site creation. There will be an ongoing facility to support and further develop these processes via the Informatics Department.

Use "in the cloud" based hosting to facilitate agile working through electronic information sharing, and make all functionality available to staff anywhere at any

time.

Cost saving relating to:
- Cessation of QPulse license costs
- Reduction in travel costs
- Reduction in stationary
- Reduction of paper costs and waste disposal / recycling
- Reduction of paper storage and transport of paper to Iron Mountain

The benefits of SharePoint will be seen in patient and user experience and efficiencies as well as organisational reputation. The workforce stands to be more productive as time is saved with simpler automated processes as opposed to time consuming, repetitive and paper-based processes. Staff will be able to communicate more effectively with the introduction of features such as shared working on documents, discussion forums and enhanced collaboration across the Trust with electronic workflows. Staff will see an increase in knowledge with faster, version controlled access to the latest policies and SOP's and will see a reduction in travelling to various locations with the introduction of skype for business through the Office 365 suite.

3. Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

This is being managed through the project. Engagement with all stakeholders (both support services and operational staff) has been underway for some time through presentations, focus groups and ride outs with operational staff. The findings from observations which relate to improvements in business process (whether through the use of SharePoint or another means) are then shared to the project team and end user accordingly. As part of the project there is an established Project Team (chaired by Project Manager / Lead) and Project Board (chaired by Director of Finance). Project Board and Team meetings are bi-monthly and the key Informatics and Communications team members meet separately each month to discuss progress, trouble shoot and set goals to progress the project aims. Recruitment of Digital Ambassadors has already begun with regular updates available on the Digital Transformation Project Team Site. A specific communications strategy has been devised and will be regularly adapted to suit each phase of the project.

Regular consultations are had with AMT Evolve (our chosen Microsoft partners) and the Project Team are liaising with other organisations to learn more about SharePoint and it's benefits for other industries.

4. Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
There will always be a requirement to process corporate data. This is a new software solution which has been accepted by Executive Team to implement taking advantage of our Microsoft investment and utilising latest technology. There has been a number of successful "proof of concept" initiatives which have demonstrated the benefits SharePoint can bring to NEAS over current solutions. As this piece of work is being managed as a project, feature creep will be prevented. SMART objectives have been set and agreed. Digital Ambassadors will be recruited to ensure data quality and data minimisation. All information access will be subject to job role and managed through a process starting with creation on ESR.

5. Identify and assess the risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
1. Staff are reluctant to adopt / use SharePoint / Staff are "too busy" to get involved.	2	4	8
2. Resource from the Trust needed to support implementation / adoption including IM&T, training, OD, corporate services as well as commitment from all staff	3	2	6
3. ESR data not accurate enough to enable correct authentication for access to information	4	4	16
4. Issue with Migrating QPulse leads to scope creep of replacing this with SharePoint. (Errors with policy retention dates already reported)	2	2	4
5. Delay in Office 365 implementation	5	4	20

6. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
1	1) Communications strategy is now underway with newly appointed Communications officer. OD have attended first Project Board Meeting and are regularly updated as to needs and issues as they arise. 2) Initial training module is under construction. NEAS need SharePoint environment to design further training. This can be released early as AMT can give us access to their systems while we wait for O365 to be completed 3) Digital Ambassador role is being discussed and developed. 4) Initial interest from teams has been gathered and workflows are being set up with those who have initially come forward. 5) Communications strategy will facilitate this. 6) Departmental presentations are the first stage of these. Further work with AMT will train us further about the benefits to our organisation specifically. 7) Executive Team presentation to generate more	Reduced	1 x 3	Yes

	'top down' support" 8) Regular liaison with Project Sponsor and Directors to advise and recruit extra support <u>Update:</u> Intranet Focus Groups are spreading the word and are getting positive feedback. Departmental Presentations are progressing well and are resulting in Operational Ride outs and system/process reviews			
2	1) Departmental presentations used as initial overview to pique interest from staff. Communications will handle engagement across the Trust with dedicated comms resource OD involvement from outset with representation in Project Team, any issues will be escalated to project board 2) Strategy being devised with Communications Officer" 3) Information session, workshops, surveys and training can all be used to maximise effectiveness of roll out. 4) Development of Digital Ambassador to cascade knowledge and training. 5) Emphasis on 'top down' support. 6) ET to get the team site first and drive success of their	Reduced	1 x 1	Yes

	efficiencies and savings. Update: 7) Project Board is efficient at handling escalated risks in terms of staff availability to attend meetings and get involved. 8) Project Team and sub meetings continue to take place			
3	1) Work to ensure ESR is up to date is already underway due to organisational restructure. 2) It is vital this is continued and staff HR records continue to be updated in a timely manner. 3) This is being ran as a separate project (Daniel Crawford PM) 4) Good links forged with Daniel and attendances on both Project Teams. 5) Liaison outside of this also. 6) Request for A Harris to attend DTP Project Team meetings to advise on ESR. 7) ESR Self Serve will mitigate some of this impact. 8) Development Manager now single point of contact between ESR & DTP Project Teams 9) Project Sponsor aware of cross over and need of regular communication. 10) Strategy and Transformation Director (Caroline Thurlbeck) aware of	Reduced	3 x 2	Yes

	importance of this need also. Update: 11) Mark Birkett to also attend ESR meetings to add technical aspect to this monitoring. 12) Project Board also monitoring and setting actions accordingly			
4	1) Initial meeting with J. Boyle and team to discuss. 2) Background work starting early to circumvent any delays 3) Work being carried out to manually over ride these errors. 4) Follow up contact to request update on this work and anything else that may be known. 5) Regular feedback from J Boyle can be given at Project Board level Update: 6) Naming conventions discussion to take place with IG and QPulse team prior to migration of policies	Reduced	1 x 1	Yes
5	1) Brought other elements of project forward to prepare and offset the impact of these delays. 2) Project Sponsor aware of this issue. 3) Requesting regular feedback at Board & Team level 4) Requesting regular updates	Reduced	4 x 3	Yes

	re e-mail 5) Mark Cotton / Paul Nicholson to feedback to Project Team re delays and what is being done to address them. <u>Update:</u> 6) Other work continuing: Ride outs, Digital superheroes meetings, Departmental presentations, Project Board aware and happy with progress			

7. Sign off and record outcomes

Residual risks approved by:		Comments / recommendations *If accepting any residual high risk, consult the ICO before going ahead.*
Name	Zarna Phipps	.
Email	Zarna.Phipps@neas.nhs.uk	
Signature		
Date	Click here to enter a date.	

Measures approved by:		Comments / recommendations
Name	Lynne Hodgson	
Email	Lynne.Hodgson@neas.nhs.uk	
Signature		
Date	Click here to enter a date.	

Information Governance Manager (DPO) approval		Comments / recommendations *DPO should advise on compliance, step 6 measures and whether processing can proceed*
Name		
Email		
Signature		
Date	Click here to enter a date.	

DPO advice accepted/overruled by:		Comments / recommendations *If overruled, you must explain your reasons*
Name		
Email		

Signature		
Date	Click here to enter a date.	

This DPIA will kept under review by:		Comments / recommendations
Name		
Email		
Signature		
Date	Click here to enter a date.	

Appendix A

What are privacy risks?

Privacy risks include the following:

- Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
- Compliance risks e.g. breach of the Data Protection Act (DPA).
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public).

A PIA is suitable for:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring.
- Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed.

Types of privacy risk

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Compliance risk

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Associated organisation/corporate risk

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.