Data Protection Impact Assessment

Controller details

Name of controller	Carla Jackson
Subject/title of DPO	Finance Director/ DPO
Name of controller contact /DPO (delete as appropriate)	

Step 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.
The National Covid-19 Pandemic has necessitated organisations' to work and adapt new ways of working and to collect and hold information previously not required. CCSL is a care provider and therefore holds and uses both personal and medical information to support the needs of the people who use our services. As an employer we hold personal, financial and at times medical information. Covid -19 has seen the introduction of many new work procedures, national and local guidance along with new employer responsibilities. We have a duty to understand staff's underlying health conditions and risk assess management plans to support staff during Covid-19. The government introduced Shielding to protect and significantly reduce the likelihood of medically vulnerable people contracting the virus. We now need to test staff every 7 days and Residents every 28 days for Covid -19 and to hold this information to report with full access to Public Health England. We use the information for our own internal reporting requirements. Anonymized data to Local Authorities and CQC. The data we collect is: Name, personal address, personal email, personal telephone number, right to refuse, the test result.

Step 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?

CCSL process

We collect personal data from the employment records we hold or the employee

It is used to record and inform appropriate actions based on the result of Covid-19 tests.

Analyse the data to inform Company decisions when managing Covid- 19 in our services and office.

We share the data with Public Health England, Shropshire, Telford and Wrekin Together programme (local PHE) and National testing portal and SATH

Family information- visitor time specific personal name, address and telephone number for track and trace purposes only.

Storing data

Electronically – stored on the "s" drive with designated access to senior staff(Managers, Deputies and administrators, Operations Director and Quality Performance Manager)

HR store the referral form electrically on the CCSL "S" drive with HR access only.

Paper spreadsheet (national document) complete with all personal data and add the ID barcode to the spreadsheet. This kept in a file which is locked away when not in use.

Deleting Data – this sits within our retention policy and holding medical data for 30 years.

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?
Testing information is a special category – we have interpreted this to mean Medical Data. The data covers Shropshire – Telford and Wrekin It relates to approximately 2,000 people (staff and residents) 1175 are tested every 7 days Approximately 800 residents every 28 days. This sits within our retention policy and holding medical data for 30 years.

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)?
We are the care provider or employer. They have the right to refuse They have the right to access the data They have the right to correct or update the data The staff handbook has our privacy policy statement explaining what information we collect and who we may share it with. The resident's contract has a consent section to share information with external agencies to meet medical needs. We support people who are vulnerable – elderly in need of care and support and often with dementia. Not children The technology is a national tool/ portal We are not aware of any concerns or issues with the portal. We are not signed up to any code of conduct or certification schemes

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?
We are monitoring the real time status of staff and residents testing positive with Covid- 19 – this then triggers a set of actions to protect people using, working and visiting our services. The process is a national government tool

Step 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 a regulatory requirement

Step 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?
The data is a Legitimate interest It does achieve our purpose as there is not another process to achieve the purpose or interest and there is not another way to achieve the same outcome. Restricted access and GPR training Data quality- designated individuals assigned to keeping the data up to date. We follow the guidance on only submitting information to national portal for those individuals who have consented and actually had the test. The test results are sent directly to the individual and would give them access to the data if they submit and SAR. The processor is a government body who developed, manage and monitor the processes.

Step 5: Identify and assess 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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Wrong information being shared	Possible	Significant	Medium
Information being sent to the wrong processor	Remote	Significant	Low
Illegitimate access	Possible	Significant	Medium
The Company has no control over the processor	Probable	Severe	High

Step 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**
	No additional measures to be put in place as the high risk sits with the data processor	Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA