BRYN MELYN CARE
DATA PROTECTION IMPACT ASSESSMENT

Revision History

Version	*Revision Date*	*Revised by*	*Section Revised*
V1	24/10/2018	BY, MOD and SK	None

Document Control

Document Owner: ***Director of People and Culture***	***Document No:***	***Status:*** Approved	***Date Approved:*** ***24/10/2018***
Security Classification: Low	***Next Review Date:*** ***24/10/2019***	***Version:*** V1.1	***Department:*** People and Culture

1 INTRODUCTION

The terms Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) are often used inter-changeably within the security and privacy worlds but can sometimes have different meanings. The PIA is a long-standing term for an assessment that looks at the effects and risks of privacy of a project or process, with privacy being considered and not just the data protection implications. Whereas DPIA is the term the GDPR utilises for the risk-based approach and pre-assessments for high-risk processing.

For the purposes of this document, Bryn Melyn Care *(hereinafter referred to as the **"Company"**)* expands upon the GDPR requirements as set out in the Regulation and encompass data protection and privacy, with all aspects and facets being included and considered. We use the DPIA reference, but aim to exceed the Regulation requirements, using The Article 29 Working Party *'Guidelines on Data Protection Impact Assessment (DPIA)*', as well as the ICO reference to "*Privacy Impact Assessments"* (PIA).

2 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Data Protection Impact Assessments (DPIA) are a requirement of the GDPR and a tool that can assist those with data protection obligations in identifying the risks associated with data processing and posed to data subjects. It enables a pre-emptive approach to assess the risks and apply corrective actions and mitigating controls before a breach occurs.

This Data Protection Impact Assessment (DPIA) document accompanies our GDPR Policy & Procedures and aids in the privacy by design ethos advocated in the ***General Data Protection Regulation (GDPR) (EU)2016/679).*** Article 35 of the Regulation provides the situations and provisions for DPIAs and require those obligated under the GDPR to have processes in place to assess data protection risks and identify when a DPIA is required.

The overall aim of the Company DPIA is to apply solutions and mitigating actions where a processing activity is deemed likely to cause a high risk to one or more individuals. The mitigating actions are then implemented into the project plan and then reassessed to ensure that the risk(s) has been eliminated or reduced to an acceptable level***. The overall scope of the risk solutions is to either: -***

- Eliminate
- Reduce
- Accept

Where an impact assessment report indicates that the processing involved will or is likely to, result in a high risk to an individual(s) and we are unable to mitigate such risk(s) with appropriate measures or controls, we consult the Supervisory Authority prior to the processing taking place.

2.1 ASSESSMENT REQUIREMENTS

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by any organisation. When the risks of processing are high, we employ the use of impact assessments to assess the risk, the impact and the likelihood, and to document the origin, nature, particularity and severity of that risk, along with the processing purpose, reasons and mitigating measures and/or proposed solutions.

We rely on the Article 35(3) conditions and accompanying Recitals as to when completing an impact assessment is necessary. This list is included below; however, it is not exhaustive, and we assess each process activity on its own merits and carry out a DPIA where we believe that the processing is likely to result in high risk.

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

2.2 IMPACT ASSESSMENT TEAM

A lead is appointed to carry out the DPIA, follow the process, record the necessary information and report the results to the Senior Management Team. All DPIAs are carried out in conjunction with the Data Protection Officer who provides advice and support for the compliance of the processes with the GDPR rules. Where there are systems and/or new technologies involved, the DPIA team also includes an I.T representative.

If the screening questions indicate that an impact assessment is required, the DPIA Team Lead will assess the processing operations that will be involved in the DPIA (*using the positively answered screening questions*) and decide if any further team members are required. ***This includes choosing specific team members who: -***

- Understand the project's aims and the organisation's objective
- Authority to influence the design and development of the project and participate in decisions
- Expertise in data protection and compliance matters
- Ability to assess and suggest solutions to risks and develop mitigating actions
- Ability to communicate effectively with stakeholders and management
- The DPIA Team Lead can at any point in the PIA process, engage other members to assist in specific areas as they deem fit or necessary.

3 DPIA STAGES

We have divided the Data Protection Impact Assessment into stages to ensure that all aspects are covered, reviewed and documented. Each stage is covered in detail under its category heading.

- **Stage 1.** *Identify the Need for a Data Protection Impact Assessment* - review the GDPR Article 35(3) conditions and use the screening questions to ascertain if the processing is likely to result in high risk to individuals
- **Stage 2.** *Project Brief & Plan* - description of the information flows, what data is being processed, where it is coming from, who it is going to etc
- **Stage 3**. *Identify the Risks* - risks will include those to individuals, the organisation and compliance (law/regulation breaches) and after speaking to management, employees and stakeholders
- **Stage 4**. *Identify and Evaluate Privacy Solutions* - develop and document corrective actions, solutions and mitigating controls that can reduce or eliminate the risks. Evaluate costs and benefits of each solution
- **Stage 5**. *Integrate Outcomes* - the solutions and actions to reduce/remove the risks must be added back into the project plan so that the risks can be reassessed with the mitigating actions in place
- **Stage 6.** *Authorisation & Recording* - all stages of the DPIA must be recorded using the provided templates and sign off must be obtained from the DPIA Lead, DPO and Director/Senior Manager

3.1 IDENTIFY THE NEED FOR A DATA PROTECTION IMPACT ASSESSMENT

Not all processing activities will require a DPIA to be completed, it is therefore essential that we carry out a check and use our predefined screening questions to ascertain which *(if any*) of the high-risk operations we intend to carry out, will require an impact assessment to be completed.

The questions provided in the screening template cover most of the risks that could be classed as high to a data subject and can be used prior to each assessment proposal, however we also judge each processing operation on its own merits and add questions if they are specific to the project or objective.

We also start our internal and external consultations at this stage and involve stakeholders, employees, senior management and any associated third parties who play a part in the processing or can lend insight and feedback to the processing operation and proposed risks. If any risks are identified via consultations, these are also added to our impact assessment template.

Note: Each screening question should be answered, and you should add any new relevant question at the bottom dependant on the risk and/or processing operation you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and the areas to focus on.

REF	SCREENING QUESTION	YES	NO	N/A	NOTES
1	Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects of an individual(s)?				
2	Will decisions be based on such evaluations that are likely to produce legal effects concerning the individual(s)				
3	Is the processing on a large scale and involves special categories of data?				
4	Is the processing on a large scale and involves data relating to criminal convictions and offences?				
5	Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (*i.e. CCTV*)				

6	Will the project involve the collection of new information about individuals?				
7	Will the project compel individuals to provide information about themselves?				
8	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?				
9	Is the information about individuals likely to raise high risk privacy concerns or expectations?				
10	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?				
11	Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?				
12	Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?				
13	Will the project require you to contact individuals in ways which they may find intrusive?				
14	Will any of the processing activities make it difficult for the data subject(s) to exercise their rights?				
15	Will the operation involve processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects?				
16	Will the processing involve individuals who are considered ‘vulnerable’?				

17	Does the processing operation involve any significant risk of the personal information being leaked or accessed externally?				

If you answered **NO** to <u>all</u> the screening questions, it is unlikely that you will need to carry out a DPIA. You should retain a copy of this completed sheet along with your justification for any your answers in the notes section.

If you answered **YES** to one or more of the screening questions, you should proceed through the DPIA stages and complete the full assessment. When completed, a copy of your finished screening questions, answers and notes should be retained along with the recorded DPIA documents.

3.2 PROJECT BRIEF & PLAN

Where data is obtained and how it is processed, stored and destroyed, is an essential part of a data protection impact assessment and as such, we utilise our existing Information Audit data to complete this part of the assessment.

The information audit enables us to identify, categorise and record all personal information obtained, processed and shared by our company in our capacity as a controller/processor and includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Access level (*i.e. full, partial, restricted etc*)

We use the data on the existing Information Audit to help us populate the below project brief and plan. This plan serves as the basis for carrying out the audit and for demonstrating our compliance with the GDPR impact assessment requirements. We understand that an incomplete understanding of how information is obtained, processed and stored, can be a risk itself and must be documented to ensure a full assessment is possible.

Examples:

(a) If we do not know how data has been obtained, we are unlikely to be able to verify the consent.

(b) If we have not documented and evidenced that we have met all the lawfulness of processing conditions when the data was obtained, we may be unfairly processing information or be preventing an individual from exercising their data protection rights.

How information audits are documented is bespoke to each business and can involve several methods to ensure a complete profile of the data is obtained and accessible. We use one or more of the below methods for recording the personal information obtained, processed, stored and transferred by us: -

- Information Audit
- Data maps
- Information flow charts
- Information asset register

The project brief and plan templates also consist of the project background information, such as objectives, purpose, proposals, consultation reviews, outline/summary and previous DPIAs. This gives an overall picture of the project and enables a better assessment of the privacy impact and risks.

The third part of the project brief and plan template is the main assessment questions which provide the basis for identifying the risks. The questions are predefined; however, we do add to these if the project requires specific questions or assessment criteria.

A DPIA is intended to be flexible and can accommodate any form of processing assessment. The responses to the assessment questions then give us the issues and associated risks that are transferred over to the Privacy Issues and Risks template, detailing who is impacted, how they are impacted and providing a risk rating.

DPIA PROJECT BRIEF & PLAN		
PROJECT NAME:		***DIRECTIONS:*** *1. Complete each section and answer all the assessment questions.* *2. Use the reference number to refer to any responses that pose a risk and complete the Privacy Issues & Risks template.* *3. Provide as much detail as possible to ensure a complete assessment is made.*
PIA LEAD:		
DATE:		
CONTACT DETAILS:		

1. PROJECT BACKGROUND		
1.1	**PROJECT SUMMARY:** *Give an outline of the project, the processing and describe what is being planned.*	
1.2	**OBJECTIVES:** - *What are the aims of this project? What do you want to achieve from the processing? Why is it important/beneficial?*	
1.3	**PURPOSE:** - *What is the purpose of obtaining and processing the data?*	

1.4	**POTENTIAL RISKS:** - *Prior to carrying out the assessment question section, are there any privacy impacts or risks that have already been identified?*	
1.5	**CONSULTATIONS:** - *What insights or feedback have been obtained through consultations with stakeholders, third-parties and employees?*	
1.6	**EXISTING DATA:** - *Have any previous PIAs or compliance assessments been carried out on similar processing activities that can provide guidance for this assessment?*	
1.7	**SYSTEMS/TECHNOLOGY:** - *If the processing involves the use of new technology or systems, provide any relevant information obtained from the initial implementation assessment of such systems.*	
1.8	**OTHER:** - Detail any other *information or suggestions that can add to the impact assessment?*	

2. INFORMATION AUDIT			
PERSONAL DATA		**JUSTIFICATION**	**PROCESSING ACTIVITY**
What data will be collected?		*Why does this data need to be collected? Is there anything you can omit if not necessary?*	*What processing operation(s) will the data be used for?*
Name			
Address			
Postcode			
DOB			
Age			
Gender			
Email Address			
Home Tel No.			
Mobile Tel No.			
NI Number			
NHS Number			
Income/Expenses			
Employment Data			
Ethnic Origin			
Religion			
Health Details			
Convictions			
Credit Data			
Other			

3. ASSESSMENT QUESTIONS		
REF	**ASSESSMENT QUESTIONS**	**RESPONSE**
3.1	*What is the legal basis for processing the information?*	
3.2	*Who will have access to the information?*	
3.3	*Will there be restrictions applied to access?*	
3.4	*Does the data need to be transferred to a third-party?*	
3.5	*Do you have safeguards in place for transferring?*	
3.6	*Will you need to obtain consent to process?*	
3.7	*How will consent be obtained and the right to withdraw consent be made available?*	
3.8	*Will you have control over the data and be able to update/complete it where applicable?*	
3.9	*Will you be using data minimisation techniques?*	

3.10	*Will data be encrypted and/or pseudonymised?*	
3.11	*How will information be destroyed after it is no longer necessary?*	
3.12	*How will information be stored?*	
3.13	*Will you be able to act on all rights of data subjects? (i.e. objections, rectifications, erasure, access etc)*	
3.14	*Will you be able to meet the deadline for supplying information?*	
3.15	*Does the processing operation require the Supervisory Authority to be notified?*	
3.16	*What security measures are in place to protect identifiable information?*	
3.17	*Have all employee, agents and third-parties involved in the project been trained on the data protection regulations and impact risks?*	
3.18	*What consultations are involved in identifying the privacy issues and risks associated with this project?*	
3.19	*Will personal data be transferred to a third country or international organisation outside the EU?* *If yes, what safeguards and Chapter V GDPR measures are in place?*	
3.20	*Detail any other factors or information that can assist in this Privacy Impact Assessment.*	

3.3 IDENTIFY THE RISKS AND PRIVACY ISSUES

Using the responses obtained from answering the assessment questions, we are now able to identify the privacy issues and associated risks and record who these risks will impact. Risks will usually fall into one of three categories: -

- ***Risks to Individuals*** - Any risk that affects a data subject, their data, their privacy or their rights is classed as a risk to an individual. Inadequate disclosure controls, consent issues, processing purposes and surveillance methods are just a few of the issues that may result in risks to individuals.

- ***Compliance Risks*** - These can arise where the assessment response indicates that a breach of laws, legislation and/or regulations will occur if the processing goes ahead. This can include non-compliance with the GDPR, PECR or human rights legislation.

- ***Corporate Risks*** - Risks that will affect the business, including reputation, revenue, fines and sanctions. These will mainly arise where the initial collection, consent, disclosures, sharing and storage of the personal information have not been complied with or where record keeping is ineffective.

Once the risks have been identified, the below risk matrix is used to give the risk a rating based on the severity of the impact and the likelihood of the risk occurring. This rating provides an easy to see colour code for how severe the risk could be to the privacy of individual and therefore the necessity of putting mitigating actions into place, or reassessing using the processing activity.

The risk rating table below uses the common *'Red, Amber, Green (RAG)'* matrix, where each risk is given a RAG score based on the likelihood versus the impact.

LIKELIHOOD	IMPACT					
		Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	Almost Certain (5)	Low Med	Medium	High	Very High	Very High
	Likely (4)	Low	Low Med	Med High	High	Very High
	Possible (3)	Low	Low Med	Medium	Med High	High
	Unlikely (2)	Low	Low Med	Low Med	Medium	Med High
	Rare (1)	Low	Low	Low Med	Medium	Medium
Impact Score x Likelihood Score = Risk Rating						

- **GREEN** - Where an assessment outcome is Green, we still work to see if we can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk is still to be added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.

- **AMBER** - Where an assessment outcome is Amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (*acceptable)* level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible.

- **RED** - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable, and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some processing activities are eliminated at this point as the impact to individuals is considered to high risk to proceed.

However, in instances where the activity is essential or is a legal requirement, the proposed solutions and mitigating actions are applied and a further DPIA to see if the subsequent DPIA results in a Green and/or acceptable level of risk. If a high risk still exists and the processing activity is authorised, we always consult the Supervisory Authority (SA) prior to processing and advise that the DPIA indicates that the processing would result in a high risk and there is an absence of measures that can be taken mitigate the risk. We then await written advice from the SA and provide all information requested by them during this period.

The above process enables us to devise ways to reduce or eliminate privacy risks and assess the costs and benefits of each approach, as well as looking at the impact on an individual's privacy and the effect on the processing activity outcomes. This enables us to document our identification and assessment of the risk, the solutions and mitigating actions used to reduce or eliminate the risk and records privacy risks which have been accepted as necessary for the project to continue.

IDENTIFIED PRIVACY ISSUES AND ASSOCIATED RISKS					
REF	**PRIVACY ISSUE**	**RAG**	**RISKS TO INDIVIDUAL(S)**	**COMPLIANCE RISK**	**CORPORATE RISK**
#	*Use assessment response to detail the privacy factor resulting in risk*	*Risk Rating*	*Complete if risk impacts data subject(s) or put N/A if not applicable*	*Complete if risk causes non-compliance or put N/A if not applicable*	*Complete if risk impacts business or put N/A if not applicable*
PR1	*E.g. Processing relies solely on using automated systems*	*8*	*Affects rights under Article 22(1)* *Could result in biased results*	*Breaches Article 22(1)*	*Sanctions & fines for breaching GDPR*
PR2	*E.g. Processing makes it difficult to withdraw consent once given*	*6*	*Affects right to withdraw consent* *Unlawful processing*	*Breaches Article 7(3)* *Unlawful processing*	*Breach fines* *Reputational damage*

3.4 IDENTIFY AND EVALUATE PRIVACY SOLUTIONS

Once all privacy issues and risks have been identified and rated, we begin identifying and evaluating solutions and mitigating actions. We address each issue and document measure and controls that will reduce the risk impact. It is not possible to eliminate all risks, but we aim to reduce them to an acceptable level. Where unable to reduce risks to this level, we decide on cancelling the project or, accepting the risk if there is a legal/best interests' requirement.

Our aim is always to assess whether the impact on privacy is proportionate to the objectives of the project and to ensure that individuals and their privacy remains our priority. We consider any solution that may reduce risk and balance the aims with the impact.

When applying the solutions to the template, we use the risk rating obtained in the ***Risk Identification*** process to ensure that we know the current risk and what an acceptable level would be. Once all solutions have been added, we are then able to repeat the assessment of the risk and ascertain its eliminated, reduced or accepted result. The new risk rating is then added to the template.

Some of the steps we may use or consider reducing risks include: -

- Changing the personal information collected to reduce the privacy level when processing
- Carry out all processing in-house to avoid transfers or data sharing
- Utilise systems/technology to make the processing more accessible
- Creating new procedures for areas such as retention, destruction methods, exercising rights
- Developing new security measures for a specific project that align with its aims
- Ensuring that adequate and effective training is provided to staff of the data protection regulations and the project processing
- Publishing guidance manuals and supporting documents for use by those involved in the project
- Creating new materials and website content to enable us to better communicate with individuals
- Carrying out higher level of due diligence on any processors used for the project
- Producing data sharing agreements and transfer contracts
- All staff have signed a confidentiality agreement as part of their Contract of Employment

We also assess the costs and benefits associated with all solutions to ensure that they are viable, feasible and proportionate to the privacy impact. All solutions also involve a review and input from the Data Protection Officer, who reviews them against the GDPR and any codes of conduct that we follow in accordance with data protection laws.

PROPOSED RISK SOLUTIONS AND MITIGATING ACTIONS						
REF	**RISK**	**RAG**	**SOLUTION/MITIGATING ACTIONS**	**RESULT**	**OUTCOME**	**RAG**
#	*Risk to be mitigated*	*Current rating*	*Detail corrective actions, solutions and mitigating controls that address the risk*	*Reduced, Eliminated or Accepted*	*Has the solution(s) reduced the risk enough to proceed with processing?*	*New risk rating*
PR1	*E.g. Processing relies solely on using automated systems*	*8*	*1. After processing completes, add human intervention stage to assess results for bias.* *2. Add system trigger to wait for human sign off*	*Risk Eliminated*	*Processing no longer relies solely on automated system as human intervention added, so risk is eliminated*	*1*
PR2	*E.g. Difficult to withdraw consent once given*	*6*	*Create communication to be sent to individual(s) with guidance for withdrawing consent in writing.*	*Withdrawal possible, but only in 1 format - Reduced*	*Due to type/location of processing, withdrawal of consent can only be done in writing. Can't offer opt-out or automated withdrawal options at this time*	*6*

3.5 INTEGRATE OUTCOMES

Once all risks and privacy issues have been identified and mitigating actions and solutions applied to reduce, eliminate or accept the risks, making the project viable, we then integrate the outcomes back into the project and create an action plan for developing and implementing the solutions.

The integrated outcomes template enables us to record what actions must now be taken to put the solutions identified above, into place. We also detail who has overall responsibility for ensuring that the actions are on track and completed, an estimated completion date and the status of the progress, so that any delays can be recorded and other parties can see how far along we are in the process.

The action plan also allows us to ensure that all risks and solutions have been accounted for and are being mitigated against and that no actions are missed or stall. If at any point in the project, the objectives or processing operations change or need to be amended, we repeat the screening questions to ascertain if any new risks or privacy issues have been identified and then add these to the DPIA and provide solutions and action plan for them also.

The screening questions and assessment questions are revisited after all actions are complete to ensure that they are still appropriate and that solutions have reduced or eliminated the risks.

INTEGRATING OUTCOMES INTO PROJECT PLAN				
REF	**ACTION(S) TO BE TAKEN**	**RESPONSIBILITY**	**COMPLETION DATE**	**PROGRESS/STATUS**
#	*Details what actions must happen for the solutions in the evaluation plan to be developed and implemented*	*Who is responsible for overseeing the actions and updating the project plan*	*What is the expected date that the actions will be completed*	*Current progress and/or action status*

4 AUTHORISATION & RECORDING

All stages and aspects of a Data Protection Impact Assessment are recorded and retained for 6 years after the project implementation date. These are also used again should a similar project or technology be utilised in the future.

The stages in the DPIA aim to demonstrate that we are carrying out effective assessments when high risks to privacy are involved and that the security and privacy of personal data is one of our main priorities. Keeping records of all stages enables us to evidence that we have identified, assessed and mitigated at every stage and that all risks have been evaluated.

Where there is a requirement for us to send a copy of the DPIA report to the Supervisory Authority, we do this within the deadlines and await their authorisation to proceed before going ahead with any processing. Such disclosures include the full report, along with a summary of the project, risks and proposed solutions.

The finalised DPIA is authorised by the Data Protection Officer, and a member of the Director/Senior Management team.

DATA PROTECTION OFFICER:

Print Name: Sherrie Kelly **Date:**

PIA Authorised: **Signed:**

DIRECTOR/SENIOR MANAGER:

Print Name: **Date:**

PIA Authorised: **Signed:**