Annex B – The Data protection impact assessment process

STEP 1 – PROJECT DETAILS

Project Name/Title	**Remote access to IT systems**
Description and Purpose of the Initiative Staff, at times, use NECS laptops to remotely access the clinical system.	
Details of any link to any wider initiative *(if applicable)*	Not applicable
Stakeholder Analysis *List those who may be affected (stakeholders have been consulted prior to project start), e.g., service users, clients, staff-managers and practitioners, trade unions, visitors, professional organisations, IT providers, regulators and inspectorial bodies, MPs, councillors, partner organisations, media, carers*	**Internal:** Staff who have to use laptops away from the surgery building to work from home **External:** **Patients only**

Does the initiative involve the use of existing personal and/or confidential data: • **For new purposes?** • **In different ways?** **If so, please explain** *(if not already covered above)*	Accessing patient data via the clinicial system but on a remote device
Are potential new purposes likely to be identified as the scope of the initiative expands?	None
What is already available? *(Any previous PIA, research or consultation undertaken)*	

STEP 2 – CONTACTS

Who is completing this assessment?

Name	Amanda Hall
Job Title	Business Manager
Department/Directorate name	
Contact Address	The Villages Medical Group 21 Gardiner Crescent Pelton Fell
Email Address	Mandy.hall8@nhs.net
Telephone Number	01913873558
Connection to Project	Organization manager

Other person(s) with responsibility for this initiative e.g., project manager/director, senior information risk owner (SIRO)	
Name	
Job title	
Department/directorate name	
Contact address	
Email address	
Telephone number	

Connection to project	

Technical lead(s) *(if relevant)*	
Name	
Email address	
Telephone number	

STEP 3 – SCREENING QUESTIONS

The purpose of these questions is to establish whether a full privacy impact assessment is necessary and to help to draw out privacy considerations					
		Yes	**No**	**Unsure**	**Comments** *(Document initial comments on privacy impacts or clarification for why this is not an issue or why you are unsure)*
i	Is the information about individuals likely to raise privacy concerns or expectations e.g., health records, criminal records or other information people would consider particularly private?	x			Dealing with health records off site
ii	Will the initiative involve the collection of new information about individuals?		X		No change to the purpose for accessing – health care related only
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		X		No change to the purpose for accessing – health care related only

iv	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		X		
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		X		
vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g., biometrics or facial recognition?		X		
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		X		
viii	Will the initiative compel individuals to provide information about themselves?		X		

If you answered **No** to <u>all</u> of the above screening questions and you can evidence/justify your answers in the comments box above, you do not need to continue with the DPIA.

Should the project at any point in the future use personal information you will need to revisit the screening questions and the DPIA.

If you answered or **Unsure** to any of the above, please continue with the DPIA.

[1] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

STEP 4 – DATA COLLECTION

Please mark all information to be collected

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Personal details		Only applicable if related to healthcare needs
Family, lifestyle and social circumstances	*Marital/partnership status* *Next of kin* *Carers/relatives* *Children/dependents* *Social status e.g., housing*	Only applicable if related to healthcare needs
Education and training details	Not applicable	Only applicable if related to healthcare needs
Employment details	Not applicable	Only applicable if related to healthcare needs
Financial details	Not Applicable	
Sensitive data: **Racial or ethnic origin**	*Racial/ethnic origin*	Only as relates to health care

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Sensitive data: **Physical or mental health or condition** *NB.* *Includes treatment if applicable.* *Include Mental health status e.g., whether detained or voluntary under the Mental Health Act if applicable.*	Health data	For health care
Sensitive data: **Sexual identity and life**	List the data items: Health data	For health care
Sensitive data: **Religious or other beliefs of a similar nature**	Not applicable	Only if relates to healthcare needs

Description	Specific data item (s)	Justification *(Reason that the data item(s) is/are needed)*
Sensitive data: **Trade union membership**	Not applicable □	
Sensitive data: **Offences including alleged offences**	List the data items: Information relevant to safeguarding only	For health care
Sensitive data: **Criminal proceedings, outcomes and sentences**	List the data items: Information relevant to safeguarding only	For health care

STEP 5 – THE INFORMATION ASSET

How will the data be obtained and from where?	**Data will come from clinical system which is held by TPP via a secure internet channel**
How will the data be used?	For completion of healthcare tasks
Will the data be used locally or nationally? *If national, list any available guidance*	Locally
Who will be the owner of the information? i.e., the Information Asset Owner (IAO) *This is usually the director or service lead under which this asset sits*	Dr Richard Hall, Lead GP
Who will be the Information Asset Administrator? (IAA) *This is usually the business manager or person with day-to-day access and control*	Business manager
Will a third party have access to the information? *If so, name the third party, the circumstances and details of how the data will be accessed*	No
Will the data be shared with any other team	Shared with other health care organisations only as necessary and under data sharing arrangements

or organisation? *If so, name the organisation and the circumstances* *If so, is there a data sharing agreement in place?*	

STEP 6 – DATA FLOWS

Please provide a process map or diagram if available, or complete the table below

The answer to most the questions for the data flows are the same, as described below.

Name of Flow	What is the purpose of the data flow?	Will you be receiving data or sending it or both?	Where will you be receiving it from and/or sending it to?	Is the data anonymised?	Is the data electronic or paper?	How is the data to be transferred? e.g., via a system, email, fax, post, by hand	How will the data be secured in transit? e.g., nhs.net to nhs.net	How often will data be transferred?	How many records in each transfer?	Where will the data be stored?	How will the data in storage be secured?
	Health care	Both	From / To Clinical system held by TPP	No	Electronic	Via the clinicial system & secure connection	Via logging into secure nhs .net connection	As necessary -	Depends on use of system by user	TPP	Via propietary TPP security

STEP 7 – DATA PROTECTION ACT COMPLIANCE

Name the data controller(s) *The data controller is the organisation which, alone or jointly or in common with other organisations, determines the purposes for which and the manner in which any personal data is, or is to be, processed.* *The data controller takes responsibility for complying with the GDPR.*	The Villages Medical Group
Name any data processors and provide contact details *A data processor means any organisation which processes the data on behalf of the data controller.*	The Villages Medical Group
What is the legal basis for processing the data? *e.g., consent, required by law, etc.*	For healthcare

DATA PROTECTION ACT PRINCIPLES

Principle	Response	Actions required
Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner		
Individuals affected by the project must be informed about the processing of their data. Has a fair processing notice been provided or is a new or revised communication needed?	Yes	None
What processes are in place to ensure that data required for secondary purposes is pseudonymised (or anonymised)?	Not applicable	
If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Implicit consent for the purpose of heatyhcare only	
Principle 2: Personal data shall be collected for specified, explicit and legitimate purposes		

Principle	Response	Actions required
What procedures are in place to ensure that privacy implications are considered prior to using data for a different purpose to that originally specified?	Data is to be used for healthcare purposes only	
Principle 3: Personal data shall be adequate, relevant and limited to what is necessary		
What procedures are in place for ensuring that data collection is adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Standard Information governance procedures & standards	
How will you ensure that the data you are using is likely to be of good enough quality for the purposes it is used for?	Standard Information governance procedures & standards	
Principle 4: Personal data shall be accurate and where necessary kept up to date.		
What procedures are in place for ensuring that data collection is accurate?	Standard Information governance procedures & standards	
What procedures are in place for ensuring that data collection is kept up to date?	Standard Information governance procedures & standards	

Principle	Response	Actions required
What procedures are in place to correct inaccurate data when requested to do so by a data subject?	Standard Information governance procedures & standards	
Principle 5: Personal data shall be kept in a form which permits identification of the data subject for no longer than is necessary		
How long is the data to be retained for?	As long as the patient is registered with out practice	
What procedures are in place for: • Archiving • Anonymisation • Deletion • Destruction of the data?	Standard Information governance procedures & standards	
Are there likely to be any exceptional circumstances for retaining certain data for longer than the normal period(s)?	The practice remains the data controller for electronic records after death	
What procedures are in place to provide data subjects access to their records?	Patients will be able to access records electronically by default from November 22. SAR requests can be made to access paper records at any time	

Principle	Response	Actions required
What procedures are in place to prevent the processing of data which may cause damage or distress?	Safeguarding / third party data to be redacted from record	Consult with Caldicott guardian to decide on action to take
What procedures are in place for data subjects who may require the rectification, blocking, erasure or destruction of inaccurate data?	Right to request process to be performed. Patients are to ask in writing to have specific data removed.	
Principle 6: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss destruction or damage		
What procedures are in place to ensure that all staff who have access to the data undertake information governance training?	Contractual requirement for annual completion	
What procedures are in place to ensure that data, whether at rest or in transit, is secured?	Technological – passwords / logging on via restricted network Signed undertaking that individuals will take	
What procedures are in place to prevent the unauthorised disclosure of data to third parties?	Confidentiality agreements – contractual and signed	

COMMON LAW DUTY OF CONFIDENTIALITY

Assessment of compliance	
Has the individual to whom the information relates given consent?	
Is the disclosure in the overriding public interest?	
Is there a legal duty to do so, for example a court order?	
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006?	

HUMAN RIGHTS ACT 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?

STEP 8 – PRIVACY ISSUES IDENTIFIED AND RISK ANALYSIS

Any privacy issues which have been identified during the DPIA process (for example: no legal basis for collecting and using the information; lack of security of the information in transit, etc.) should be documented in the risk register template embedded below. This risk register will enable you to analyse the risks in terms of impact and likelihood and document required action(s) and outcomes.

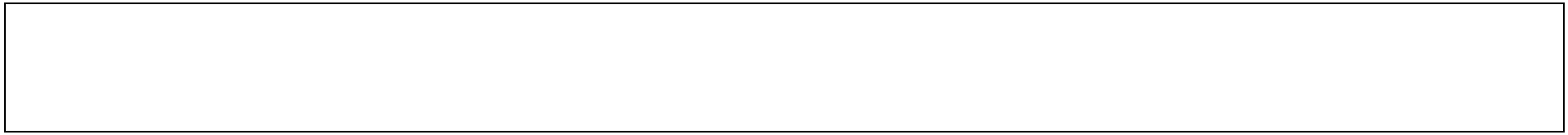
Note that where it is proposed that a privacy risk is to be 'accepted', approval for such acceptance should be sought from the Caldicott Guardian where patient data is concerned and the SIRO for all information risks.

STEP 9 – DATA PROTECTION PRINCIPLES COMPLIANCE AND AUTHORISATION

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

Information asset owner	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	

Data Protection Officer/Caldicott Guardian *(Caldicott Guardian only where the personal data is about patients)*	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	
Senior Information Risk Owner *(where the identified privacy risks are significant)*	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	
Information Governance Lead	**Name:**
	Date:
	Signature:
Reasoning behind the decision to accept or reject the identified privacy risks	



REFERENCES

- Data Protection Act 2018
- UK General Data Protection Regulations 2016
- The Caldicott Principles
- Common Law Duty of Confidentiality
- The Freedom of Information Act 2000
- The Mental Capacity Act 2005
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001)
- Public Health (Control of Disease) Act 1984
- Public Health (Infectious Diseases) Regulations 1988
- The Gender Recognition Act 2004
- Confidentiality: NHS Code of Practice 2003
- IGA Records Management Code of Practice for Health and Social Care 2016
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
- Abortion Regulations 1991
- Road Traffic Act 1988
- ICO Data Sharing Code of Practice
- Confidentiality and Disclosure of Information Directions 2013
- Health and Social Care Act 2012

- The Criminal Justice Act 2003
- The NHS Information Security Management Code of Practice 2007
- The Computer Misuse Act 1990
- The Electronic Communications Act 2000
- The Regulation of Investigatory Powers Act 2000
- The Prevention of Terrorism Act 2005
- The Copyright, Designs and Patents Act 1988
- The Re-Use of Public Sector Information Regulations 2005
- The Human Rights Act 1998
- The NHS Care Record Guarantee 2007
- Anonymisation Standard for Publishing Health and Social Care Data Code of Confidentiality