Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
OPAS-G2 – Electronic Staff Occupational Health Record	

Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) to meet its legal/compliance obligations with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

The Data Protection Impact Assessment (DPIA) ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed, as required under ISO/IEC: 27001:2017. It is important that the DPIA is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation. Data Protection Impact Assessment are an integral part of the "privacy by design" approach as identified by the Information Commissioner's Office.

Document Completion

A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the Information Asset Owner, a representative from NHIS, Information Governance/Data Protection Officer and a customer representative (if applicable) and through the appropriate governance structure of the implementing organisation. Sign off and acceptance of the document does not close the privacy risks related to this project. It is important that the risks are revisited during the life of the project and any additional privacy risks identified are appropriately reviewed and mitigated.

PLEASE NOTE:
The Information Asset Owner (implementer) undertaking the Data Protection Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with the Trust procedures.
Assessment Process Stages

Activity	IAO	Governance
Complete Title Bar and include Ref Number	x	
Complete Project Details and check the Initial Screening Questions	x	x

Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – DPIA (Full) is to be undertaken	x	x
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded	x	x

If a Data Protection Impact Assessment **IS NOT** required		
Activity	**IAO**	**Governance**
Complete Assessment Summary & Recommendations for Action	x	x
Assessment to be passed to Implementer		x
Ensure Sign Off is completed	x	x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**IAO/IAA**	**Governance**
When a new system is being implemented and the supplier provides a completed DPIA on a suppliers template, the information will need to be transferred to the Trust's template to ensure there are no omissions	**x**	
Complete Stage 2 – Data Protection Impact Assessment (Full)	**x**	
Complete Stage - 3 Identified Risks and Mitigating Action	**x**	
Complete Stage – 4 Legal Compliance		x
Complete Assessment Summary & Recommendations for Action	x	
Account access management Standard Operating Procedure to be completed prior to the implementation of the project	x	
Closure meeting for final agreement	x	
Ensure Sign Off is completed		x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

This document is intended to be completed by the Trust and external organisations the *Governance* section will be completed by the IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	**OPAS-G2 – Electronic Staff Occupational Health Record**

Project Description: Describe in sufficient detail for the proposal to be understood
Joint Occupational Health Service system with Nottinghamshire Healthcare NHS Foundation Trust, separate instances of the application, OPAS-G2, per Trust ensuring access to data is available to the correct occupational health team only. OPAS-G2 is the upgrade of the current OPAS system which has been used by the Trust for 28 years which is now at end of life being over 30 years old. The outdated system will no longer receive security and system updates and will not be secure in line with UK GDPR. Using the same occupational health system as Nottinghamshire Healthcare NHS Foundation Trust will provide the ability to benchmark and share best practice. The OPAS-G2 application also has an interface with the Trac recruitment software used by the Trust which will streamline the onboarding process for the recruitment and Occupational Health teams and provide a superior end user experience to applicants.

Overview of the proposal: What the project aims to achieve
Create efficiencies for the Occupational Health and recruitment teams and provide a better service to employees, managers, HR and applicants and income generating clients. Ensure data is kept in line with UK GDPR. The outdated system will no longer receive security and system updates and will not be secure in line with UK GDPR.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Jo Friar, Civica jo.friar@civica.co.uk Lisa Welham, Office Manager Neil Waring, Project Manager Victoria Kirkbride, Deputy Head of Occupational Health

	Adam Grundy, Head of Occupational Health

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Robert Symcox	Director of People	Sherwood Forest Hospitals NHS Foundation Trust	9th June 2022
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	8th June 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	26th May 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	9th June 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	3rd August 2022
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	9th June 2022

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:

Summary:
Legislative Compliance:

Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity)

Article 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities

Summary of Risks:
Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.

Risks

1. Loss of system access - Full system back-up process in place
2. Loss of system data - Full system back-up process in place
3. Leavers' access not removed – Occupational Health team notified of leavers by HR
4. Data is accessed inappropriately – individual username and passwords are provided, Active Directory to be explored post go-live
5. OPAS-G2 will need to be added to the divisional information asset register and recorded as part of the annual IAO returns to the SIRO
6. Interface between TRAC and OPAS G2 causing delays in clearance data

being updated on TRAC - Occupational Health to have a process in place to inform Recruitment of clearance status during any downtime

7. Data is lost during the migration from old system to new system requiring Occupational Health team to access paper records for historical information - Occupational Health team to review records transferred to confirm integrity.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure OPAS-G2 is added to the information asset register	IAA	30th April 2022
Single sign on – This can be implemented but was not in the original scope of the project and would require additional resources and costs	IAA	Post go-live
Occupational Health to have a process in place to inform Recruitment of clearance status during any TRAC downtime		
Occupational Health team to review records transferred to confirm integrity		

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full DPIA will be undertaken on a case-by-case basis by IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Information will be collected from individuals who attend the Occupational Health department and from those who go through the recruitment process. This is required for health screening of individuals and forms part of the recruitment process
2	Will the project compel individuals to provide information about themselves?	Y	The information individuals must provide is the same using the OPAS-G2 software as is currently required whilst using the current OPAS system.
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	The same data as is currently gathered and processed will be used.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	OPAS-G2 will assist the occupational health department to ensure that data is relevant and up to date.
6	Are there security arrangements in place while the information is held?	Y	Civica, the supplier of the OPAS-G2 application hold ISO 27001 and Cyber Essentials. IBM who provide the Cloud infrastructure hold various ISO certifications including 27001 and Cyber Essentials.
7	Does the project	Y	Currently Occupational Health data is held and

Q	Screening question	Y/N	Justification for response
	involve using new technology to the organisation?		processed in a desk-based system, OPAS, which is over 30 years old and at end of life. OPAS-G2 is the most up to date version of the OPAS suite of occupational health solutions. OPAS-G2 is around 3 years old and is used by many organisations including other Trusts in the UK and Ireland. The OPAS-G2 applications has an interface with the Trac recruitment software used by the Trust's recruitment team and will streamline the onboarding process.
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	N	07.02.2022 - the software's focus is on employees of the trust and not as staff as 'patients'. The legislation is clear that this applies to patient systems. In addition, the intended use of the system is to make referrals to specialists and not used solely to base clinical decisions on. The systems are also used within councils etc so are not exclusively a clinical system.
10	Is a Quality Impact/Technical Security Review required?	Y	• Civica has carried out robust reviews of third parties used to deliver the OPAS-G2 service. Third parties used are IBM for the UK Cloud Infrastructure who have many accreditations including ISO 27001 details can be viewed here: https://www.ibm.com/support/pages/ibm-iso-management-system-certifications • The optional calendar synchronisation is provided by Cronofy details of their ISO etc. can be found here: https://www.cronofy.com/privacy/ • The optional SMS text messaging service is supplied by Twilio, details of their certifications

Q	Screening question	Y/N	Justification for response
			can be found here: https://www.twilio.com/legal/data-protection-addendum • https://www.twilio.com/gdpr • https://www.twilio.com/legal/privacy/shield • Removable media - Civica do not use removable media to transfer data rather SFTP sites are used and set up for specific tasks as required. • Remote working - Many Civica employees work remotely and access to Civica systems is via strictly controlled VPN. • The Trust can allow the OPAS-G2 application to be accessed from any internet enabled device alternatively access can be restricted to being accessible through the Trusts Single Sign On. Logged as a recommendation. NHIS have reviewed the supplier assurance framework and have not identified any concerns or recommendations

Please ensure that on completion this is returned to Information Governance lead to agree how to proceed.

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☐	Other?	☒
	If Other please specify.		Migration of Occupational Health data from end-of-life desk-based software to SaaS Cloud OPAS-G2.			

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☒
	DOB	☒	Gender	☒	Address	☒
	Post Code	☒	NHS No	☐	Hospital No	☐
	Other unique identifier (please specify)		OPAS number, NI number			
	Sensitive Personal Data (special categories):					
	Children					☐
	Vulnerable groups					☐
	Racial or ethnic origin					☒
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐
	Other data (please specify)					

2.2.2	Is the data?					
	Identifiable?	☒	Pseudonymised?	☐	Anonymised?	☐
	If the data is pseudonymised please describe the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust. Also describe how the data will be transferred ie using HL7					
	The data is sent encrypted from our server to the Civica server. OPAS-G2 is secured using an SHA-256 signature with a 2048-bit public key HTTPS (TLS 1.2) certificate. This ensures all communication between the Trust devices and the cloud solution is encrypted and protected from interception. All underlying physical disk storage is encrypted using industry standard AES-256. Additionally, all user passwords are encrypted/hashed within the database using bcrypt with individual salts. The Management Consoles used by Civica IT and Civica Development to manage the application and database services are also accessed over HTTPS to ensure configuration details are secure.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Data is required to ensure an employee's health and safety to carry out tasks required for their role. The data required is processed currently the only difference will be that it will be processed in OPAS-G2 rather than OPAS.
2.3.1	How will you collect, use, store and delete data?	
	Data subject (employee). Employees will complete a range of online questionnaires aimed at ensuring that they are safe to carry out the role for which they are employed. Managers will be able to complete online referrals and applicants will complete Pre-placement questionnaires online. Once submitted to the Occupational Health team the data will be available to clinicians to access online to triage and arrange next step actions. occupational health clinicians will complete their notes directly in to OPAS-G2. OPAS-G2 has inbuilt record retention functionality. The Trust specifies the criteria and OPAS-G2 dashboards let the Occupational Health team know when data should be deleted according to the Trust's policies. Data can then be deleted either by a clinician with the appropriate administration rights (super user) or by raising a ticket with the Civica support team.	
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)	
	Data subject (employee), applicant, HR or manager completing online	

	questionnaires. Occupational Health employees completing cases using OPAS-G2. ESR daily feed to OPAS- G2 – NHIS development team will extract from ESR and send to OPAS-G2 and create the daily data feed. The data is then sent encrypted from our server to the Civica server. Trac is compatible with OPAS-G2. The Trust uses Trac for recruitment purposes by the Trust and this is a free integration tool provided as a bolt on with OPAS-G2.
2.3.3	How much data will you be collecting and using?
	All data that is collected from the patient is the minimum amount of information required in order to provide a service to the individual. The data is already being collected and used but in OPAS rather than OPAS-G2
2.3.4	How often? (for example monthly, weekly)
	Daily
2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf
	OPAS-G2 has built in record retention functionality which allows the Trust to specify the retention criteria. Dashboards alert the occupational health system administrator when records or part(s) of records should be deleted.
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage
	IBM Public Cloud platform utilising their UK based data centres for all components.
2.3.7	How many individuals are affected?
	All employees and applicants.
2.3.8	What geographical area does it cover?
	This will depend on the home address of all staff, UK wide.

2.4	Who are the Organisations involved in processing (sharing) the data?

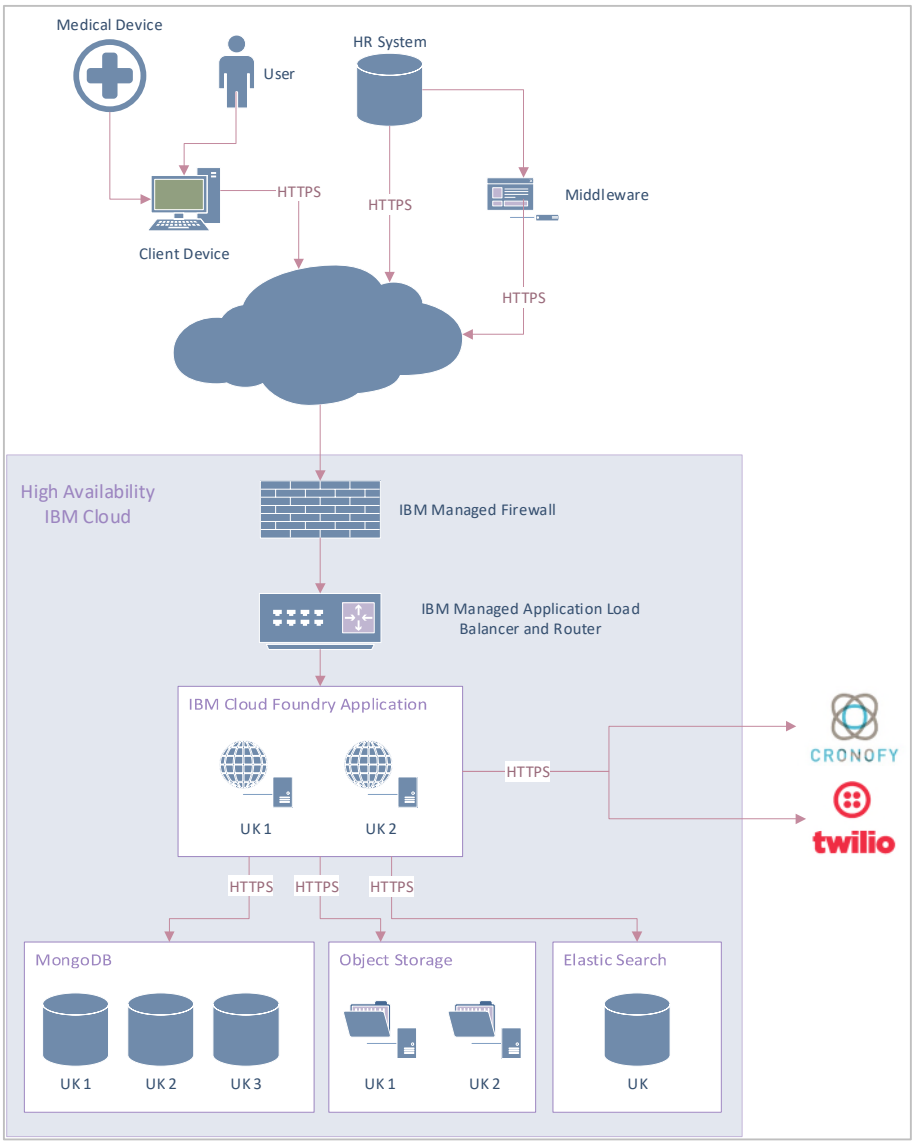
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	Civica	Data Processor

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below**  NHIS - Supplier Assurance Framework  Supplier Assurance Framework - Example
		 Civica OPAS-G2 data-protection-imp  05. SAF - OPAS G2 - Electronic Staff Occup
2.5.1	Please describe access and controls in place https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf https://www.sfh-tr.nhs.uk/media/12008/ig-0121-account-management-sop-template-sept-21.pdf  Account ManagementSOP OP/	
	Granting User Access – Access to the application and data is tightly controlled to ensure it is	

	only available to the relevant people, at the required times, for only the duration it is required. OPAS-G2 is a role-based application. The standard authentication method for the application is by email address and password. When a user is initially created in OPAS-G2, they are sent a link to verify their email address and set a password. The user will be created by the System Administrator at the Trust. All users of the OPAS-G2 application will require a unique user in the system to enable them to access the application and the data they are allowed to view. Civica will create and maintain the initial System Administrator level user, and a System Administrator level user will be created for the Trust to manage access. The Trust will not have access to the underlying database or infrastructure. This is reserved for the Civica IT team to manage the system as required. Access to the infrastructure management area is via login to the IBM Cloud Portal and is restricted to those within the Civica IT team only. Database access is also restricted to Civica IT and is accessed using credentials obtained from the IBM Cloud Portal. Civica Support will not have any access to the system on a day-to-day basis. If they require access to the application to investigate an issue, this must be requested via Civica IT. At this point a username and password will be issued to allow access to the application. This will be logged in an internal Access Request system and access granted only for the required duration. Additional users are added by the Trust, and we will create their username, along with the level of access. The new user will then request a password reset which will email them their initial password. Employees and applicants are requested to complete online questionnaires and provide consent by invitation and do not require an account. The Trust is not currently using Active Directory to access the system therefore the default password policy in the system requires: • Passwords must be changed every 31 days • Minimum length of 10 characters • Unable to have 3 identical consecutive characters • 2 categories of character (upper, lower, numerical, symbol) must be used

	• Credentials are always transmitted within a secure HTTPS tunnel. Additionally, all user passwords are encrypted/hashed within the database using bcrypt with individual salts.			
2.5.2	Please provide a copy of the contract in place			
	 Sherwood Forest Hospitals NHS Founda			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Civica IBM have policies and procedures in place to ensure any storage media involved in the provision of its Cloud services are destroyed physically at the end of their life. Civica also have a Media Handling Policy which details how Civica will handle any media at the end of it usable life. If the Trust no longer wishes to continue with the use of the OPAS-G2 service, the underlying data will be delivered to the Trust as a Mongo Database via either SFTP or Courier as arranged with the Trust.			
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes		
		Z5268164		
2.5.5	Has the supplier received ICO Enforcement? Please check the register	Yes	No	
			x	
2.5.6	Has the supplier received ICO Decision Notice? Please check the register	Yes	No	
			x	
2.5.7	Has the supplier received an ICO Audit? Please check the register	Yes	No	
			x	
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes - 8HC47	17th February	Standards Met

	check the register and provide the following details		2022	
2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates			
		Yes	No	
	Cyber Essentials Plus		Cyber Essentials Certificate - Civica UK	
	ISO 15489 Records Management		No	
	ISO 27001 Information Security Standards	27001 - Civica HQ with Annex (1).pdf		
	ISO 9001 Quality Management Systems	9001 - Civica HQ with Annex (1).pdf		
2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country			
	Yes	No		
		x		
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier			
	Not applicable			
2.6	Will this information be shared outside the organisations listed above?			
	Y/N	if answered **Yes** please describe organisation/s and geographic location		
	N			
2.7	Does the work involve employing contractors external to the Organisation?			
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?		

	Y	Contract in place with Civica and the Trust
2.8	Has a data flow mapping exercise been undertaken?	
	Y/N	If **Yes**, please provide a copy here. If No, please explain why
	Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If No, please explain why	
	Y. Civica – Training documents demonstrate information flow, provided.  The Trust's data flows	

	 OH Data Flows 2022.xlsm					
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Yes	OPAS-G2 has comprehensive audit records that show details of what has changed on records and by who. These can be accessed from within the application by a user with the System Admin role. Modifications are tracked at a field, record and user level making it possible to easily see all changes to a specific field over time.

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	Y	Current Occupational Health data is held in a paper record system. Once OPAS-G2 is live the Occupational Health department will stop creating paper records and will proceed to use OPAS-G2. Where current paper notes are still used by the Occupational Health department for active staff members the intention would be to use them for information only and scan and upload the paper notes to OPAS-G2 in order that paper copies can be phased out.

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?
	Staff demographics held on OPAS-G2 will be updated directly regularly from ESR on a daily basis to ensure contact details (address, mobile) are up to date. Occupational Health Department staff will also do a verbal check to confirm staff details are accurate when staff attend the Occupational Health department.

2.13	Who will have access to the information? (list individuals or staff groups)	
	All Occupational Health Department staff will have access to the OPAS-G2 system following training **Civica Access** Customers will not have access to the underlying database or infrastructure. This is reserved for the Civica IT team to manage the system as required. Access to the infrastructure management area is via login to the IBM Cloud Portal and is restricted to those within the Civica IT team only. Database access is also restricted to Civica IT and is accessed using credentials obtained from the IBM Cloud Portal. The Network Admins always need to retain the ability to login with the Domain Admin/Database Admin level in order to maintain the systems. This is only done as required and is not used on a daily basis. Civica Support will not have any access to the system on a day-to-day basis. If they require access to the application to investigate an issue, this must be requested via Civica IT. At this point a username and password will be issued to allow access to the application. This will be logged in an internal Access Request system and access granted only for the require duration. Membership of Civica Support Staff to the support accounts is recorded on the Access Request system. Civica IT check regularly if the open access is still required and close it on completion of the work.	
2.14.1	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☐
	Username and password	☒
	Smartcard	☐
	Key locked filing cabinet/room	☐
	Hard/soft Token (VPN) Access	☐
	Restricted Access to Network Files (shared drive)	☐
	Has information been anonymised?	☐

	Has information been pseudonymised?	☐		
	Is information fully identifiable?	☒		
	Other (provide detail below)	☐		
	Access to the system can be linked to Active Directory (single sign on), however this was not scoped as part of the project but can be undertaken at a future date if required. Added as a recommendation.			
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	Each of IBMs Data Centres may contain multiple server rooms which are designed to house around 5000 servers each. These server rooms allow IBM to optimise space, power, network, personnel and internal infrastructure as required. Physical access is controlled by key card proximity systems for access to the Data Centre and individual server rooms. Access throughout each facility, and to sensitive areas such as generators, batteries, UPS and air con is restricted and only allowed for authorised personnel. All UK facilities require two factor authentication (biometric and key card) for access. All sites are covered by CCTV cameras and security personnel monitor these, along with alarms from the access control systems to maintain the security of the site. Failed access attempts are logged and available for follow up with the Site Manager as necessary. Individuals requiring access to a Data Centre that do not have access cards etc. are required to sign in at the security desk, provide photo ID and are escorted around the facility at all times. Temporary ID is issued to identify them at all times. This access will only be granted to Civica Staff when required for audit assurance purposes where supplied documentation does not cover the audit requirement.			
2.15	Will the data be stored on Trust servers			
	Yes	No		
		x		
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐

	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Other	☐	please specify below	☐

2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually. **Civica** Backups of the data required for the OPAS-G2 system are taken on a daily basis, and can also be triggered on an ad-hoc basis as required (for example prior to an upgrade). These backups are stored on the IBM Infrastructure that houses the database, and are replicated to several UK locations to ensure recovery is possible if the primary data centre is unavailable. The application and all its underlying services are already running redundant systems which work from multiple UK datacentres, so failure at one of the locations should allow the service to resume at another without intervention. In a full disaster scenario it would be possible to download the database backup and deploy it elsewhere with relative ease.

		The backups taken can only be accessed by Civica IT.
2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**
		Train the trainer
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	There may be occasion where reports run from OPAS-G2 contain personal information if the report is required for a recall exercise for example to confirm vaccination status of groups of staff.
	Who will be able to run reports?	Access to reports will be limited to senior Occupational Health team members
	Who will receive the reports and will they be published?	Management Referral reports will be accessible by the manager (and HR if included by the manager) online by logging in to OPAS-G2.

2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	**Civica** IBM have policies and procedures in place to ensure any storage media involved in the provision of its Cloud services are destroyed physically at the end of their life. Civica also have a Media Handling Policy which details how Civica will handle any media at the end of it usable life. If the customer no longer wishes to continue with the OPAS-G2 service, the underlying data will be delivered to the customer as a Mongo Database via either SFTP or Courier as arranged with the customer.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
		Part of our statutory duties under GDPR 6(1)(e) public interest or public duty
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		The Trust's privacy notice is here Sherwood Forest Hospitals (sfh-tr.nhs.uk) The Trust's Privacy Notice can be accessed by users directly through the application. When employees are invited to complete online forms they are able to access the Trust's privacy notice via a hyperlink within the form. Civica privacy notice is here Data Privacy Notice | Civica

2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Civica – An occupational health System Administrator can delete a personnel record (in line with the Records Management Code of Practice 2021) from OPAS-G2 if required. It is also possible for the occupational health System Administrator to classify a record within OPAS-G2 as restricted processing if required.
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The purpose of OPAS-G2 is to enable to Occupational Health department to provide an efficient Occupational Health service to Trust staff and other groups who access our services. The Occupational Health department currently uses an older version of OPAS and the new version will be used in a similar way and should not change the expectation of clients with regards to the way their data is processed through the Occupational Health system
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		The Trust has a policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk) Track and process Subject Access Requests (SARs) easily in the application. Record who made the request, what evidence was provided, timescales for responding and importantly, what the response was. This dedicated feature also collates all the information about a Data Subject into a

		single PDF along with the associated documents for easy redaction.
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Robert Symcox, Director of People
	IAA	Adam Grundy, Head of Occupational Health
	System Administrators	Lisa Welham, Office Manager Demi Scales, Occupational Health
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	OPAS-G2 is secured using an SHA-256 signature with a 2048-bit public key HTTPS (TLS 1.2) certificate. This ensures all communication between the client device and the cloud solution is encrypted and protected from interception. All underlying physical disk storage is encrypted using industry standard AES-256. Additionally, all user passwords are encrypted/hashed within the database using bcrypt with individual salts. The Management Consoles used by Civica IT and Civica Development to manage the application and database services are also accessed over HTTPS to ensure configuration details are secure.	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
		A patient safety case is not required. The supplier assurance framework has been reviewed by NHIS. No risks or recommendations identified.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	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?
	To improve the management of staff members using the Occupational Health department services. This will include managing health surveillance programmes to ensure timely access to screening where required. The implementation of this project is anticipated to improve the recruitment processes for staff joining the Trust. There will also be improvements to the experience of managers through changes to the management referral process.
2.31	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?
	Adam Gundy, Head of Occupational Health presented this DPIA to the Information Governance working group for consultation and Information Governance Committee for approval.

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting,

	quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	The Trust's lawful basis for processing personal and special categories of personal data are: 1. Article 6(1)(e) public interest or public duty 2. Article 9(2)(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject 3. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Supplier 1. Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. 2. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	This DPIA will be published once finalised. The Trust's privacy notice has been updated.

2.34	What measures do you take to ensure processors comply?
	The Trust and Civica have a contract in place, and this will be reviewed on a regular basis. Civica have a contract in place with IBM.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Civica will only ever process the Trust's data as per explicit agreement with the Trust The Trust and Civica have a contract in place where roles and responsibilities are defined. To prevent function creep, processing activity will be carried out on behalf of the Trust by Civica that is agreed to. The Civica Service Agreement provides explicit information on processing activity provided by Civica as part of offering the OPAS-G2 System. As such, there is limited scope to utilise the platform for other functions within the Trust. As data controller, the Trust has full responsibility for ensuring health care professionals accessing the system utilise it appropriately.

Stage - 3 Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

Completed by: Adam Grundy	Role: Head of Occupational Health	Date completed: 11th March 2022

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Loss of system access due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be patient harm, financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place	2	2	4	System back-up not present	2	2	4	Manual input, business continuity plan to be used
Loss of system data due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable.	Full system back-up processes and ISO 27001 accreditation in place	3	1	3	System back-up not present	2	2	4	Manual input, business continuity plan to be used

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
The consequences of this could be patient harm, financial penalties and reputational damage to the Trust									
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Account Management and access procedure completed. Appropriate access according to role. Segregation of duties. Occupational Health team notified of leavers by HR monthly report Changes to user roles reviewed monthly via a Trust e-form report	2	2	4	There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records. The system will only allow one generic account and individual users cannot be tracked or audited	2	1	**2**	Ensure access is managed and leavers list is received and actioned. Routine audits.
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually via existing paper records or verbally with the patient/employee	2	2	4	OPAS-G2 will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	OPAS-G2 will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Issue with interface between TRAC and OPAS G2 causing delays in clearance data being updated on TRAC	Regular updates from TRAC team to advise users of any planned updates and process to contact all main users for support during any unplanned downtime – during any extended downtime Occupational Health team would manually advise Recruitment of clearance status	2	2	4	Timely clearance information sent to recruitment	2	1	**2**	Occupational Health to have a process in place to inform Recruitment of clearance status during any downtime
Data is lost during the migration from old system to new system requiring Occupational Health team to access paper records for historical information	Following migration of data the Occupational Health team will conduct a review of a selection of records to ensure the integrity of data transferred	3	2	6	Work would need to be undertaken with Civica to establish why the data did not migrate and what actions can be taken to rectify	3	1	**3**	Occupational Health team to review records transferred to confirm integrity

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

Compliance to be determined by IG team from the responses provided in the previous stages, delete as appropriate:

Data Protection Act 2018	Compliance and Comment
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest, and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals. • If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. • We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We

	have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • We implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.