NHS Counter Fraud Authority

Workforce Management Information

Data Protection Impact Assessment

June 2021

V1.0 Published Version

NHS fraud.
Spot it. Report it.
Together we stop it.

Executive Summary

This document contains information in relation to ***Workforce Information.***

The document is deemed OFFICIAL and any information viewed/obtained within it should be treated in the appropriate manner as advised and set out in the Government Security Classifications (May 2018).

More information in relation to this data classification, including the requirements for working with these assets can be found here:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

In particular please note that:

ALL routine public sector business, operations and services should be treated as OFFICIAL - many departments and agencies will operate exclusively at this level. There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

Table of contents

Executive Summary **2**

Links & Dependencies **5**

1. Data Protection Impact Assessment Requirement & Process **6**

Introduction 6

Data Protection Impact Assessment 8

Ownership 20

2. DPIA Report **20**

Section 1: Overview of Data Collection and Maintenance 20

Section 2: Uses of the Application and the Data 21

Section 3: Data Retention 21

Section 4: Internal Sharing and Disclosure of Data 22

Section 5: External Sharing and Disclosure of Data 22

Section 6: Notice/Signage 22

Section 7: Rights of Individuals to Access, Redress and Correct Data 22

Section 8: Technical Access and Security 22

Section 9: Technology 23

3. Compliance Checks **23**

DPA 2018 Compliance Check 23

The Privacy and Electronic Communications Regulations 23

The Human Rights Act 23

The Freedom of Information Act 23

Conclusion 24

Annex A - Definition of Protected Personal Data **25**

Annex B - Data Protection Compliance Check Sheet **26**

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Performance, Analytics & Improvement PMO Manager	DPIA Workforce Management Information	DPO	V0.1	Nov 2020	Initial creation
Performance, Analytics & Improvement PMO Manager	DPIA Workforce Management Information	DPO	V0.2	March 2021	Reviewed and amended
Performance, Analytics & Improvement PMO Manager	DPIA Workforce Management Information	DPO	V1.0	June 2021	Final Approved

Prefix	
Reference:	**DPIA (Workforce Management Information)**
Date:	**June 2021**
Author:	**Performance, Analytics & Improvement PMO Manager**
Data Owner:	**NHSCFA**
Version:	**1.0**
Supersedes	**0.2**

Links & Dependencies

Document	Title	Reference	Date	POC
DPA	Data Protection Act	All	2018	HMG
EU GDPR	EU General Data Protection Regulation	All	2016	GDPR
FOI	Freedom of Information Act	All	2000	HMG
Government Security Classifications	Government Security Classifications	All	May 2018	Cabinet Office
HRA	Human Rights Act	All	1998	HMG
ISO/IEC 27000	Information security management systems Standards	ISO/IEC 27001:2013	Oct 2010	ISO
IS1P1 & P2	HM Government Infosec Standard No. 1, Part 1 – Risk Assessment and Treatment	P1 - Issue 3.5 P2 – Issue 3.5	October 2009 October 2009	CESG
IS2	InfoSec Standard 2	Issue 3.2	January 2010	CESG
PECR	The Privacy and Electronic Communications Regulations	All	2003	HMG

1. Data Protection Impact Assessment Requirement & Process

Introduction

1. The General Data Protection Regulation (GDPR) 2016 introduces a new obligation to undertake Data Protection Impact Assessments (DPIAs), before carrying out types of processing **'likely to result in high risk(s) to individuals' interests'**. DPIAs are now mandatory for certain types of processing and there are specific legal requirements for content and process. Where a DPIA identifies a 'high risk' that cannot be mitigated, the Information Commissioner's Office (ICO) must be consulted.

2. DPIAs provide a way to systematically and comprehensively analyse the intended processing and help to identify and minimise data protection risks. In addition to considering compliance risks, they should also consider broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm to individuals or to society at large, whether it is physical, material or non-material.

3. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It does not have to eradicate the risks altogether, but should help to minimise them and assess whether or not remaining risks are justified. A DPIA may cover a single processing operation or a group of similar processing operations. For new technologies you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

4. A DPIA must consider 'risks to the rights and freedoms of natural persons'. While this includes risks to privacy and data protection rights, it can also affect other fundamental rights and interests:

    a. "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead **to physical, material or non-material damage**, in particular: where the processing **may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy**, **unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage**; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data[1]…"

5. Under GDPR you must carry out a DPIA where for example you plan to:

    a. process special category or criminal offence data on a large scale.

6. The ICO also requires a DPIA to be undertaken for example, where you plan to:

    a. use new technologies;

    b. match data or combine datasets from different sources;

    c. collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');

7. DPIAs are an essential part of the organisation's accountability obligations under GDPR and an integral part of the 'data protection by default and design approach'. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur.
8. Conducting a DPIA is a legal requirement for any type of processing. Failure to carry out a DPIA in required cases may leave the organisation open to enforcement action, including a **fine of up to €10 million**.

[1] GDPR - Recital 75

General Description

9. Workforce Management Information is a core business requirement for NHSCFA to report and manage key information from across NHSCFA, specifically relating to the organisation people, absence monitoring and other core information such as headcount and FTE. Electronic Staff Record (ESR) system is effectively the NHS HR system that is segmented to specific business groupings at the organisation level. It is anticipated that the data contained within ESR will be used in core business activity that will support the accurate and timely reporting of management information. Initially the data will be extracted and reported/processed by NHSCFA Performance Team and presented in a flat report with integration into a SAS portal once firm analytical processes for data controls have been established these will include names persons processing staff data and reporting organisation managers using SAS data processing tools. The extraction required from NHSBSA is the only method where the appropriate calculation can be applied to the data that account for working days instead of calendar days, in addition we also need to calculate the total operational hours available to NHSCFA to calculate operational time lost as a direct result of absence. Currently only the Chief Executive Officer has access to the organisation within their ESR dashboard, however this will still not show the operational time/days available to the organisation or the distribution of long/short term absence. The required calculations to the data are not available within ESR a flat report/xls/csv is the only method available where calculation can be applied that meet our requirements. Workforce Management Information will be controlled by the Performance Team with the data being stored in a secure location, this data is stored in a restricted drive within the performance function, should this move to a SAS portal then the data will be stored securely and process by a senior analyst with the appropriate permissions applied the any visual analytical product, the second phase will include the integration in a SAS platform with control plans around the sight of raw data files, including the protection of that data within a restricted SAS library.

10. At this stage it is envisaged that the core data required to produce meaningful management information will be extracted from ESR and processed within NHSCFA by using analytical techniques and tools. The data collection element is already done as part of routine updating from managers within NHSCFA into ESR. We intend to make use of this valuable data by simply reporting in aggerate on a routine basis, the data is extracted from ESR then reported in aggregate. Only if presented in SAS VA would an extract be available and even then, only the data that is shown in the chart e.g. numbers and percentage values

11. This is the first DPIA to be completed and it has been carried out by the Information and Records Management Officer, in consultation with Performance and Improvement Lead and the Information Governance and Risk Management Lead. This relates to the collation, processing and reporting of data used for management information and organisation health monitoring.

12. Management information and raw data from ESR is compliant with our GDPR requirements it is also required to comply with other relevant HMG legislation including where applicable the Data Protection Act 2018, Human Rights Act 1998 and Freedom of Information Act 2000.

Data Protection Impact Assessment

13. To ensure data received from NHSBSA meets all legal requirements and the risks to personal data are identified and understood it is necessary to undertake a DPIA. This DPIA is based on the ICO's recommended template[2] comprised of seven steps, this is to ensure that the data that will be used in the analysis complies with the organisation governance principles:

    Step 1 - Identify the need for a DPIA

    Step 2 - Describe the processing

    Step 3 - Consultation process

    Step 4 - Assess necessity and proportionality

    Step 5 - Identify and assess risks

    Step 6 - Identify measures to reduce risk

    Step 7 - Sign off and record outcomes

[2] Version 0.3 (20180209)

STEP 1: Identify the need for a DPIA

Explain broadly what the system/project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The project aims are to have the ability to report meaningful management information to organisational leaders. This information will be used to support the development of policy, processes and procedures within NHSCFA. In addition, this information will be a core data source that will enable to accurate and timely reporting of specific metrics in the future. The processing of this data is to simply report meaningful management information that is easily digestible and usable by the organisation, currently NHSCFA does not have access to this centrally or even make use of workforce information. The use or formula, counts, calculation, sums, lookups will be used in the processing of this data to calculate days lost, resource available, resource impact and resource cost of absence. In addition, the sum/count of reasons behind absence and cost will also be undertaken using the methods discussed, however, analysis for patterns in the data will also be undertaken. The requirement to conduct a DPIA has been identified within the initial project plan and ToR to ensure the highest levels of governance and protection are applied to this data prior to processing. At this point in time, we hold a vast amount of data within ESR that is not tapped that will deliver information that will be used to support decision making. At this point in time, our intention is to extract this core data on a routine basis and analyse for patterns, behaviours and for key statistics. It is the protection of this data in its raw format that has mainly prompted the DPIA. In addition, we want to provide assurance to the organisation people that we are processing this data in a safe, legal and ethical way that supports the business. See the scope of processing for fields and range of data.    Organisation Health Indicators 20

STEP 2: Describe the processing

Describe the nature of the processing:

1. How will you collect, use, store and delete data?

2. What is the source of the data?

3. Will you be sharing data with anyone (consider using a flow diagram or other way of describing data flow)?

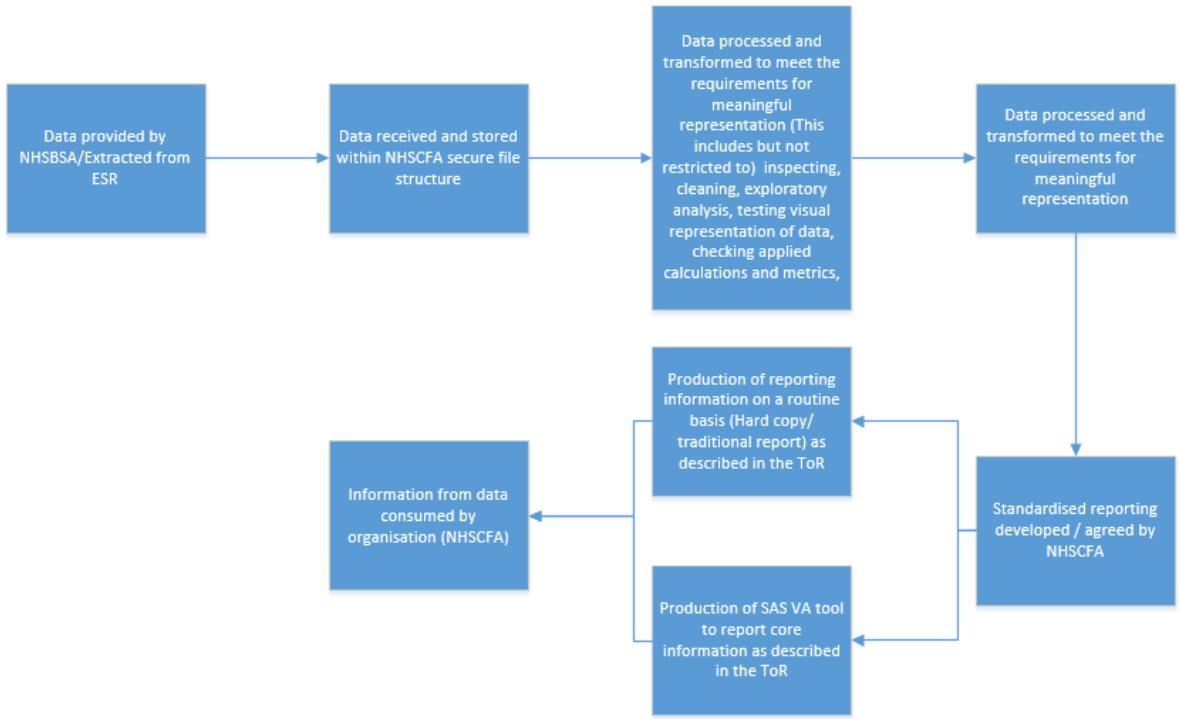
4. Why types of processing identified as 'likely high risk' are involved?

1: The data will be either extracted from ESR or provided in a series of static reports from NHSBSA to a central hub for processing. The data will be processed to meet management information requirements to inform decision making within NHSCFA as directed in the ToR. Currently this is not available or provided by NHSBSA, there is an organisational request to add this information (aggregated) to visualisation software for wider scale distribution using the SAS VA platform. Therefore, the security protocols and processes will be implemented by the IA team. This will operate in a similar fashion to that of benchmarking data, where information is restricted based on assigned permissions. Physical touch points of the data will also be minimised after the initial data exploration and transformation phases of the data have been complete. Therefore, the actual design & development of the visual tool will be restricted to anonymised data in the first instance to prepare for the routine addition of data. The implementation and addition of SAS will be considered a final step once the use and reporting structure of "written/hard copy/pdf" reporting has been adopted. This is to ensure accuracy and consistency of reporting. The report will be shared to management within NHSCFA in pdf/word versions with no embedded data and moving towards SAS VA via a reporting portal.

2: The data will be stored within a secure file structure within NHSCFA's own network that will be configured by NHSCFA systems, this is currently secured within the Performance file structure and restricted to the Performance and Improvement Lead and Performance and Improvement Director. The retention of this data will be retained for a specified period of time for statistical purposes, given that the intention is to report routinely, it is envisaged that aggregate datasets are requested to cover late data entries and account for changes, advice on this specific retention will be sought from Governance, however, we are recommending that core statistics from processing be retained indefinitely but underpinning datasets be reduced after six years (this is due to the proposed approach of appending data) . It must be acknowledged that this is data held within NHSBSA ESR business system and therefore under the same governance the retention of flat files/raw data will be taken under advice from governance. It is envisaged that a record of destruction process will be implemented, however, statistical reporting will be retained within NHSCFA archives for reference and trend analysis. If we were to follow advice provided by the CIPD we would apply the this as best practice given this data is HR related, we envisage this being no longer than six years once reported:

3: The Statutory Sick Pay (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) abolished the former obligation on employers to keep these records. Although there is no longer a specific statutory retention period, employers must still keep sickness records to best suit their business needs. It's advisable to keep records for at least 6 months after the end of the period of sick leave in case of a disability discrimination claim. However, if there's a personal injury claim, the limitation is 3 years. If there's a contractual claim for breach of an employment contract, it may be safer to keep records for 6 years after the employment ceases. (https://www.cipd.co.uk/knowledge/fundamentals/people/hr/keeping-records-factsheet) The information held will only be for reporting purposes.

The high-level data flows will look like:



The risks involved in this project include:

Potential data breaches of staff data, uncontrolled distribution of raw data files and miss representation of the analysis presented.

Uncontrolled distribution has been minimised by introducing a single point of entry into NHSCFA for this data, therefore preventing the multiple distributions that currently exist now. This is considered a significant improvement to business process.

Describe the scope of the processing:

1. What is the nature of the data and does it include special category or criminal offence data?

2. How much data will you be collecting and using?

3. How often?

4. How long will you keep it?

5. How many individuals are affected?

6. What geographical area does it cover?

1. Yes: Protected characteristics will be included for Equality, Diversity and Inclusion monitoring: personal data revealing racial or ethnic origin. Data includes: staff sickness, ED&I, Staff lists, start/end dates, incremental progression dates, grade, grade point, salary (raw), gender, office locations, team, age/DoB to calculate age and all other protected characteristics applicable to the production of core management information.

2. All staff data, this data will be used by the Performance Team and Information Analytics to interpret the results for management consumption. This is not a data collection but a use of "collected" data.

3. Monthly or as applicable to support key workforce development and planning

4. Under guidance from governance (suggested 6 years) for analytical purposes

5. This applies to all NHSCFA staff & Board

6. It will cover England

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

2. How much control will they have?

3. Would they expect you to use their data in this way

4. Do they include children or other vulnerable groups?

5. Are there any prior concerns over this type of processing or security flaws?

6. Is it novel in any way?

7. What is the current state to technology in this area?

8. Are they any current issues of public concern that you should factor in?

9. Are you signed up to any approved code of conduct or certification scheme (once any are approved)?

1. Relationship is professional – processing NHSCFA data on behalf of NHSCFA

2. Employees will have no control on the production of management information, this is standard reporting of key information collected on behalf of NHSCFA by NHSBSA from ESR. However, employees will have the ability to amend their ESR records relating to protected characteristics, managers can and should maintain sickness absence records correctly.

3. Yes – this is standard business reporting across the NHS

4. No – employees only

5. Yes, security of processing raw data outside of ESR business system and data processing into SAS VA – these areas are under review to ensure the appropriate security measures are in place. Secure storage has already been arranged the NHSCFA network adheres to the relevant security standards required for the organisation to function ISO 27001. Single point of data entry into the organisation has also been arranged to further reduce the risk of breach.

6. The actual approach is not novel in other organisations, but it will be for NHSCFA. We are not applying any novel insight that will include the application of specialist approaches to this data. This is predominantly counting and summing.

7. Technological solutions are currently not available for this reporting, hence the reason we intend to apply analytical techniques and routine reporting of this data. At this stage, it looks like ESR will not produce the required outcomes required for NHSCFA purposes. However, NHSCFA has the tools and experience to process this data to become meaningful.

8. NHSCFA's people are our main concern, however, this project will satisfy the need to respond to FoI's for specific but limited questions relating to staff numbers, FTE, sickness cost, amount (FTE days lost) and main reasons for absence. It will also support the production of this key information for the annual report.

9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA network. This does not relate to DPIA but is an accreditation of our own security protocols and will be held within a network that is ISO27001 compliant. This information is within the information asset register. We are not implementing a system we are analysing ESR data that will be stored on a secure drive within the organisation network.

Describe the purposes of the processing:

1. What do you intend to achieve?

2. What is the intended effect on individuals?

3. What are the benefits of the processing, for you and more broadly?

1. Production of quality management information

2. No impact on individuals, but this may support the development of appropriate policies and procedures that support the organisation people and business from an evidence base.

3. No benefit to me personally, Benefit to NHSCFA has already been discussed within this document and in point 1 & 2.

STEP 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views or justify why it's not appropriate to do so?

2. Who else do you need to involve within your organisation?

3. Do you need to ask your processors to assist?

4. Do you plan to consult information security experts or any other experts?

1. This will be done by NHSCFA OD and from NHSCFA management tiers. However, this is management information the communications of this has already been highlighted in the recent people agenda article shared on Go2: However, workforce information is there to support policy development and safeguarding of the organisation people. People will not be given any opt outs or views on how to prepare workforce information, however, we will communicate with the organisation that this overarching analysis and reporting is taking place.

2. "The Performance Management Office continues to strengthen organisational performance processes to monitor and track performance against strategic and operational targets. This has included ongoing development of NHSCFA's management reporting tool, work to develop management information and strengthened reporting not only to the Board and Executive Team but to everyone. The drive to develop more outcome-based measures and KPIs for next year and beyond continues".

3. OD, ISA, IA, Performance, LT & SMT, NHSBSA

4. Yes, processors will be from the Performance and IA team under the Performance and Improvement Director.

5. Yes, we will be discussing and arranging very specific security arrangements to securely store the raw data with ISA and Database Administrators. In addition, we have asked for secure drive to be established within the restricted "performance drive".

STEP 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

2. Does the processing actually achieve your purpose?

3. Is there another way to achieve the same outcome?

4. How will you prevent function creep?

5. How will you ensure data quality and data minimisation?

6. What information will you give individuals?

7. How will you help to support their rights?

8. What measures do you take to ensure processors comply?

9. How do you safeguard any international transfers?

1. (Maintenance of Records) (Revocation) Regulations 2014 (SI 2014/55) / DPA

- The lawful bases for processing are set out in Article 6 of the GDPR is:
    - Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

2. Yes

3. Potentially, these are currently being explored with NHSBSA for some elements, specifically overarching reporting of sickness absence. However, calculating operational time available may not be a core element of the ESR business system.

4. The initial plan for this data is to incorporate “core” management information and introduce additional metrics where necessary and when required for a specific business need.

5. Data quality will be enforced by ESR as we are processing business system data, however, exception reporting and notification including requires up to date personal records may be adopted but not enforced by this project. However, any significant data quality issues will be raised with SMT for organisation action. Lighter data quality issues will be addressed with unit managers e.g. personal allocated to wrong teams, open sickness absence dates that area significant.

6. It must be stipulated that corporate reporting of this information will not be at the individual level unless this is deemed necessary by SMT and will be controlled by user access to SAS VA at manager level.

7. Ensure compliance with the DPA, protecting personal data and its integrity, ensuring governance is applied at key stages without minimising the operational need to change specific reporting criteria.

8. Any processors will ensure that SoP’s are developed and reviewed, the Analytical Lead & Performance and Improvement Lead will develop and implement to account for the two different approaches to produce management information based on the tools used.

9. There is no requirement to conduct international transfer this data

STEP 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant, or Severe	**Overall risk** Low, Medium or High
Data Breach	Possible	significant – potentially sensitive data i.e. sickness/protected characteristic	Low
Application of strong analytical techniques (ML/DL) and profiling	Possible	Significant	Low – analysis is designed in a very specific and limited way according to the business and ethical needs of the business the application of these techniques is not in use within NHSCFA on this particular data type.

STEP 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.	**Effect on risk** Eliminated, Reduced, Accepted	**Residual risk** Low, Medium, High	**Measure approved** Yes/No

STEP 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before proceeding.
DPO advice provided		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice: Having reviewed the DPIA I am satisfied that a comprehensive assessment of the extraction, access, storage and subsequent retention of person identifiable data from ESR has been carried out. Access to and the use of raw personal ESR data will be limited to only that required to achieve the stated purposes. Initial access to the information will be controlled and by IT administrators and overseen with limited permissions-based access approved by the Director of Performance & Improvement and the Performance, Analytics & Improvement PMO Manager. Access will be fully auditable. All data will be held and governed in accordance with current legislative requirements and handled in accordance with organisational best practice and its data retention policy. I am therefore satisfied with the with the organisational security measures employed.		
DPO advice accepted or overruled by:	Trevor Duplessis - 18th June 2021	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' view, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Ownership

The following table describes the roles and responsibilities

Table 1 - Roles and Responsibilities

Role	Responsibility
Information Asset Owner (IAO)	Performance, Analytics & Improvement PMO Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Performance, Analytics & Improvement PMO Manager (for the duration of this project) Analytical Intelligence Lead (Routine processing within SAS VA)
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. Workforce Management Information is a core business requirement for NHSCFA to report and manage key information from across NHSCFA, specifically relating to the organisation people, absence monitoring and other core information such as headcount and FTE. Electronic Staff Record (ESR) system is effectively the NHS HR system that is segmented to specific business groupings at the organisation level. It is anticipated that the data contained within ESR will be used in core business activity that will support the accurate and timely reporting of management information. Initially the data will be extracted and reported/processed by NHSCFA Performance Team and presented in a flat report with integration into a SAS portal once firm processes have been established. Workforce Management Information will be controlled by the Performance Team with the data being stored in a secure location, the second phase will include the integration in a SAS platform with control plans around the sight of raw data files, including the protection of that data within a restricted SAS library. This is to support the production of workforce management information

2. Brief overview of the data contained within: This will be workforce information/data extracted from ESR for formal and routine business reporting.

3. The impact level of the Workforce Management Information reporting is assessed as OFFICIAL SENSITIVE and it can only be accessed internally or reported in aggregate in documents such as the annual report.

4. The following measures briefly describe what controls have been security implemented to protect the Workforce Management Information reporting and the personal data recorded

    a. The Workforce Management Information will be accessed by managers from NHSCFA, which includes the database administrators this is not a system but a series of ongoing analysis and reporting requirements to inform the organisation of specific and limited health indicators that impact on organisations ability to operate.

b. The is reporting of data contained within ESR that is currently not visible to the origination, The reporting does not have any direct interconnections with other NHSCFA systems and applications this is a series of reporting and analysis where data is used from ESR to present meaningful information. The tool used may vary e.g. excel, SAS but the application of techniques will not

c. The Data Custodian must comply with the data protection requirements Examples include: regularly reviewing the business requirement to record the personal data; ensuring that the data is not excessive; it is being used for the purpose intended; that there is a deletion and disposal policy; that the application is registered on the NHSCFA register and the NHSCFA DPO is aware of its existence.

5. It is assessed that there are no residual privacy risks to the personal data used by the Workforce Management Information this is standard reporting that is going to be developed using information extracted from ESR.

6. This DPIA must be reviewed if any changes are made to the personal information if used by the database or any other changes are made that affect the privacy of an individual.

Section 2: Uses of the Application and the Data

7. Describe the purpose: The analysis is to produce high quality workforce information for monitoring purposes, specifically for trend, and ~~,~~ resource impact, this is a fundamental in any organisation to support the workforce and manager to be effective and financially aware of the cost of absence management.

8. Who has responsibility for the administration of the reporting: All NHSCFA line managers are responsible for the quality of the information held within ESR. However, the core data required to produce meaningful management information will be extracted from ESR and processed within NHSCFA by using analytical techniques and tools. The data collection element is already done as part of routine updating from managers within NHSCFA into ESR. We intend to make use of this valuable data. The initial data processing will be undertaken by the Performance and Improvement Lead.

9. Information in the Database/System could include; ED&I monitoring: personal data revealing racial or ethnic origin. Data includes: staff sickness, ED&I, Staff lists, start/end dates, incremental progression dates, grade, grade point, salary (raw), gender, office locations, team, age/DoB to calculate age and all other protected characteristics applicable to the production of core management information.

10. The processing of sensitive data is as described in points 8 and 9 above.

11. The IAO must comply with data protection requirements. Examples include: regularly reviewing the business requirement to use the personal data; ensuring that the data is not excessive, it is being used for the purpose intended; that there is a deleting and disposal policy; that the application is registered and the DPO is aware of its existence.

Section 3: Data Retention

12. The Workforce Management Information is subject to NHSCFA Data Handling and Storage Policy. No data deletion process in place, however this will be implemented once the flat files are received. This is subject to our own data retention recommendation of six years for raw data.

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner. This asset will be reviewed and planned for upon receipt of the first dataset and recorded.

Section 4: Internal Sharing and Disclosure of Data

14. Initially this will be a paper based report, however, when the time is right we will implement dynamic reporting. This will be dependent on access requirements, currently this will be Exec/SMT/LT by business unit and not for general consumption by staff, row level permissions will also be applied to protect information so only appropriate managers can view their own units records. SMT & Exec will have greater permissions to view reporting outputs (visually)

Section 5: External Sharing and Disclosure of Data

15. The only reason information of this type would be shared externally is by FoI and presented in a summary statistical format and presented in aggregate. No personal inform will be shared or dataset requests.

Section 6: Notice/Signage

16. This data is extracted from ESR that NHSCFA's people have access to.

NHSCFA's privacy policy on its website hosts separate sections in relation to data collection, retention and storage. This broadly covers all elements of the NHSCFA usage of data, in a nonspecific manner.

Section 7: Rights of Individuals to Access, Redress and Correct Data

18. Individuals subject to certain exemptions, have the right to gain access to their own personal data. In the event an access request is directly or indirectly received by NHSCFA, we are required to provide the individual who has made the request with details of the personal data recorded about them.

19. It is unlikely that many access requests will be received as the personal data recorded is all in relation to for current employees, this information is available to them via their ESR access. For former colleagues, this will be via the BSA HR service

20. In the unlikely event that information is identified as being incorrect, NHSCFA staff will take appropriate steps to correct the record where permissible.

21. All NHS employees have the right to redress and correct personal data recorded about them. This is available within their own access to ESR or via their line manager.

Section 8: Technical Access and Security

22. The security and technical access architecture of the network where the data is stored is as explained in this DPIA:

The application and the hosting infrastructure was assessed at **Official-Sensitive** and the hosting infrastructure is subject to the ISO27001

23. Access is restricted to internal staff only.

24. The technical controls to protect the system include:

a. Anti-virus protection;

b. Permission based access controls to shared drive.

c. Logging, audit and monitoring controls.

d. Vulnerability Patching Policy for the underlying infrastructure.

e. Secure access to folders when raw data is stored

f. Single point of entry to NHSCFA for workforce data.

Section 9: Technology

25. The system holds personal information extracted electronically from (Electronic Staff Records) the extracted will be located in the NHS Counter Fraud Authority secure file structure upon receipt from BSA partners, this secure folder has already been configured and single routes into CFA have been established.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the System, and the personal data that it records, and its business activities, are compliant and maintain compliance with: This is not a system development but the analysis of data contained within ESR for management information purposes.

a. The GDPR and the Data Protection Act in general;

b. The Data Protection Principles;

c. The interpretations of the Principles.

2. **This is not a recommendation but a requirement of law.**

3. The roles and responsibilities for the protection of personal data are described in the NHSCFA security policy.

4. The system processes sensitive personal data and so a Data Protection Compliance Check Sheet has been completed (see Annex B) describing how the requirements of GDPR and the Data Protection Act 2018 have been complied with, See; also Annex A Category C

The Privacy and Electronic Communications Regulations

5. The Privacy and Electronic Communications Regulations is not applicable as personal data is not exchanged with external organisations for commercial purposes.

The Human Rights Act

6. The decisions and activities of the organisation are undertaken in compliance with the Human Rights Act, having due regard to appropriateness and proportionality to ensure compatibility with Convention rights.

The Freedom of Information Act

7. As a public authority we are compliant with the provisions of the Freedom of Information Act, in proactively publishing and making available upon request, certain recorded information held by the organisation subject to any relevant exemption(s). However, no personal information would be disclosed under the Freedom of Information Act as this would breach the data protection principles.

Conclusion

8. There are no residual privacy risks to the personal data that will be used in the production of management information. The controls described in this DPIA explain in detail how the data is protected and managed in accordance with the GDPR and Data Protection Act 2018. The DPO is responsible for ensuring that the controls are implemented through the life cycle of the system.

Annex A - Definition of Protected Personal Data

Personal data includes all data falling into Categories A, B or C below:-

A. Information that can be used to identify a living person, including:

Name;
Address;
Date of birth;
Telephone number;
Photograph, etc.

Note: this is not an exhaustive list.

B. Information which, if subject to unauthorised release, could cause harm or distress to an individual, including:

Financial details e.g. bank account or credit card details;
National Insurance number;
Passport number;
Tax, benefit or pension records;
DNA or fingerprints;
Travel details (for example, at immigration control or oyster records);
Place of work;
School attendance/records;
Material related to social services (including child protection) or housing casework.

Note: this is not an exhaustive list.

C. Sensitive personal data relating to an identifiable living individual, consisting of:

Racial or ethnic origin;
Political opinions;
Religious or other beliefs;
Trade union membership;
Physical or mental health or condition;
Sexual life
Commission or alleged commission of offences;
Proceedings relating to an actual or alleged offence.

Any data set containing this information must be processed in accordance with the GDPR and the Data Protection Act 2018 (DPA 2018).

Particular care must be taken with data in Category B and with any large data set. Information on smaller numbers of individuals may justify additional protection because of the nature of the individuals, source of the information, or extent of information.

There are additional, specific constraints within the provisions of GDPR and the DPA (2018) on the processing of data in Category C.

Annex B - Data Protection Compliance Check Sheet

PART 1: BASIC INFORMATION - New or existing Project, System, Technology or Legislation

1. Organisation and project.

Organisation	NHSCFA
Branch / Division	NHSCFA Performance, Projects and Analytics.
Project	Workforce Management Information

2. Contact position and/or name, telephone number and e-mail address.
(This should be the name of the individual most qualified to respond to questions regarding the DPIA)

Name, Title	Trevor Duplessis
Branch / Division	Finance and Corporate Governance, NHSCFA
Phone Number	020 7895 4642
E-Mail	Trevor.Duplessis@nhscfa.gov.uk

3. Description of the programme / system / technology / legislation (initiative) being assessed.
(Please note here if the initiative does not collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

This is to support the production of internal workforce management information for reporting, monitoring.

4. Purpose / objectives of the initiative (if statutory, provide citation).

NHSCFA leads on a wide range of work to support organisation decision making and formal reporting of core measures and workforce monitoring.

1. Workforce Management Information is a core business requirement for NHSCFA to record and manage key information from across NHSCFA, specifically relating to the organisation people, absence monitoring and other core information such as headcount and FTE. ESR system is effectively the NHS HR system that is segmented to specific business groupings at the organisation level. It is anticipated that the data contained within ESR will be used in core business activity that will support the accurate and timely reporting of management information. Initially the data will be extracted and reported/processed by NHSCFA Performance Team and presented in a flat report with integration into a SAS portal once firm processes have been established. Therefore, initial of the Workforce Management Information System/Portal will be the Performance Team (currently 1 FTE) with the data being stored in a secure location, the second phase will include the integration in a SAS platform with control plans around the sight of raw data files, including the protection of that data within a restricted SAS library.

.

5. What are the potential privacy impacts of this proposal?

Data Protection Impact Assessments (DPIA) have been considered in the light of personal data gathered, and the data in the Workforce Management Information System has been gathered for a specific, justifiable and proportional purpose and found to be mitigated by the steps put in place to minimise the possibility of unauthorised access or use (see Compliance Checks in section 3 of this document)

6. Provide details of any previous DPIA or other form of personal data* assessment done on this initiative (in whole or in part).

This is the first DPIA carried out on the system.

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO PART 3: DPA COMPLIANCE - CONCLUSIONS

*IMPORTANT NOTE:
'Personal data' means data which relate to a living individual who can be identified:
(a) from those data, or

(b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Page left intentionally blank.

NHSCFA offices

Coventry

Earlsdon Park
55 Butts Road
Coventry
West Midlands
CV1 3BH

London

4th Floor
Skipton House
80 London Road
London
SE1 6LH

Newcastle

1st Floor
Citygate
Gallowgate
Newcastle upon Tyne
NE1 4WH