NHS
Counter Fraud Authority

Financial Information – Staff Data

Data Protection Impact Assessment

August 2021

V1:0 Published Version

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

Executive Summary

This document contains information in relation to staff data saved and used by Finance.

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

Document Control					
PM	**Ref**	**Document owner**	**Version No**	**Issue Date**	**Amendments**
Finance Business Partner	DPIA - Financial Information - Staff Data	DPO	V0.1	May 2021	Initial creation
Finance Business Partner	DPIA - Financial Information - Staff Data	DPO	V0.2	July 2021	Reviewed and amended
Finance Business Partner	DPIA - Financial Information - Staff Data	DPO	V0.3	August 2021	Final review and amendments
Finance Business Partner	DPIA - Financial Information - Staff Data	DPO	V1.0	August 2021	Final Approved

Prefix	
Reference:	**DPIA Financial Information Staff Data**
Date:	**August 2021**
Author:	**Finance Business Partner**
Data Owner:	**NHSCFA**
Version:	**1.0**
Supersedes	**0.3**

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

9. This DPIA is related to the NHSCFA Risk Assessments, which outline the threats and risks. The Risk Assessment document was developed in accordance with the requirements of NHSCFA and CESG HMG Infosec Standards 1 and 2.

Financial Information Staff Data - General Description

10. Staff data is extracted from the ESR system and sent to Corporate Performance as part of monthly MI. The data is then emailed to Finance and used calculate future year budgets (using salary and increment information) and to perform analysis on positions occupied by staff within the organisation. The report and associated working papers are stored within the finance drive and access is restricted to Finance staff.

11. The information is requested from BSA HR and is a standard system report ran from ESR. Information from other sources (e.g. NHS Employers pay award) is used to calculate future year expected salaries to assist with budget setting.

12. This is the first DPIA to be completed on the system and it has been carried out by the Information and Records Management Officer, in consultation with Finance Business Partner and the Information Governance and Risk Management Lead.

13. The use of staff data in addition to GDPR 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

14. To ensure the use of staff data by finance 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:

    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 ESR data is required to provide a starting point for salary costs in relation to budget setting. The need for a DPIA has been identified due to the nature of the information contained within the ESR report (identifiable employee information).

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. Data is provided via internal email from Corporate Performance. It is used to calculate future salaries/staff costs as part of the budget setting process. The information is stored on the finance Drive (F) and personal, identifiable information is deleted after processing is complete (circa 3 months after receipt).

2. ESR (Report ran from system) via Corporate Performance

3. Only shared amongst 4 members of staff in the NHSCFA finance team. Outcomes of the exercise are communicated in a format where individual staff information is not included.

4. Sensitive data

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. Staff data includes name, work location, date of birth/age, NI Number and salary information (no banking information).

2. Information is required for all NHSCFA staff to accurately calculate salary costs.

3. Annually

4. Personal/identifiable data will be deleted after processing (usually around 3 months)

5. This applies to all NHSCFA staff

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. Employer
2. Information is extracted from ESR (Control over information in ESR due to self service)
3. Usual process for Finance to calculate future year salary
4. No
5. No
6. No
7. ESR reporting does not have the functionality required to provide necessary outcome – manual calculations are required to base data via excel.
8. No
9. The NHSCFA has an ISO ISO27001:2013 certification on information security which covers information processed within the NHSCFA 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. Use ESR data to calculate expected salary payments for budget setting purposes
2. Nil – informs budget for NHSCFA by pay band
3. Accurate information that forms base of NHSCFA financial plan.

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. Not applicable
2. Corporate Governance
3. Requester of information and processer are the same individual
4. No

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. Public Task & Contract
2. Yes
3. No
4. Restricted access to folder & ensuring data is not used for any other purposes
5. Data to be kept in line with Data Retention Schedule.
6. None
7. Not Applicable
8. Not applicable
9. Not applicable

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
NHS CFA Privileged & Standard User – As a result of negligence or malicious intent, data could be stolen/modified.	Remote	Significant	Low
Accidental Screen & File sharing – Staff could share a file accidentally not intended to the recipient.	Remote	Significant	Medium

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
Continual monitoring of access rights given to staff and removal of access where it is no longer required. Password protection of document/folder. Accidental File Sharing – staff have been made aware not to share official sensitive documents, information request to HR is issued reference number so responses are tied to information requester	Reduced Reduced	Low Medium	

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 access, storage and subsequent retention of person identifiable data obtained from ESR has been carried out. Access and the use of the data will be limited to only that required to achieve the stated purposes, with access restricted to the Finance Team only. 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 - 5th August 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)	Finance and Performance Manager
Senior Information Risk Owner (SIRO)	Head of Intelligence and Fraud Prevention
Application/Database Owner	Finance Business Partner
Data Protection Officer	Trevor Duplessis Information Governance and Risk Management Lead

2. DPIA Report

Section 1: Overview of Data Collection and Maintenance

1. Staff data is extracted from the ESR system for Finance to calculate future year budgets (using salary and increment information) and to perform analysis on positions occupied by staff within the organisation.

2. Data includes name, work location, date of birth/age, NI Number and salary information (no banking information).

3. The impact level of the ESR data was assessed as OFFICIAL SENSITIVE and it can only be accessed internally.
4. The following measures briefly describe what controls have been implemented to protect the staff data - Finance and the personal data recorded:
    a. The data is accessed by approximately 4 members of staff from NHSCFA.
    b. The data does not have any direct interconnections with other NHSCFA systems and applications
    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 finance team.
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. Data is extracted from the ESR system for the calculation of future year budgets (using salary and increment information) and to perform analysis on positions occupied by staff within the organisation.

8. The Finance Business Partner has responsibility for the processing/administration of the staff data.

9. Information in the report could include; name, work location, date of birth/age, NI Number and salary information

10. There is no sensitive information contained within the data.

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 staff data is subject to NHSCFA Data Handling and Storage Policy. The information is stored digitally and will be deleted in line with the data retention schedule (no physical/paper information is kept).

13. The IAO is required to review the retention period and any requirement to change must be submitted to the Senior Information Risk Owner.

Section 4: Internal Sharing and Disclosure of Data

14. The data is accessed by approximately 4 members of staff from NHSCFA.

Section 5: External Sharing and Disclosure of Data

15. The information is used for internal use only. As the information we receive is an extract of an existing system, any information requests would be directed to the ESR.

Section 6: Notice/Signage

16. 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.

17. The use of signage or other notifications to notify the public of the gathering and use of personal data is not relevant and therefore outside the scope of this DPIA.

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 existing data currently stored with ESR.

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 and member of the public have the right to access, redress and correct personal data recorded about them.

Section 8: Technical Access and Security

22. The security and technical access architecture of the Database/System is as explained in this DPIA:

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

23. Access is restricted to internal staff only.

24. The technical controls to protect the database 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.

Section 9: Technology

25. The staff data holds personal information obtained electronically and is located in the NHS Counter Fraud Authority data centre.

3. Compliance Checks

DPA 2018 Compliance Check

1. The DPO must ensure that the report, and the personal data that it records, and its business activities, are compliant and maintain compliance with:

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 information does not contain any sensitive personal data. 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.

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 recorded in the data. 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 Finance
Project	Financial Information – Staff Data

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.

Staff data is extracted from the ESR system for Finance to calculate future year budgets (using salary and increment information) and to perform analysis on positions occupied by staff within the organisation. The report and associated working papers are stored within the finance drive and access is restricted to Finance staff

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

NHSCFA leads on a wide range of work to protect NHS staff from economic crime.

The purpose of the information is to enable the finance function to accurate calculate expected costs for staff in future years.

Access is restricted to 4 members of staff within NHSCFA.

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 ESR report 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 information.

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