ESR Data Protection FAQs and Answers

Table of Contents

Table of Contents 1
Introduction 1
Data Warehouse 1
Consent 5
Overseas Transfer and Security 6
Data Security 8
Data Cleansing 8

Introduction

The Electronic Staff Record (ESR) solution will replace 29 payroll systems and 38 HR systems across the NHS with a single, national, integrated solution and will be used by all NHS organisations, in excess of 640 throughout England and Wales. The ESR solution enables Trusts to provide the core services required to manage the employment of their staff, and is based on the proven ORACLE HR Management System platform.

This set of Frequently Asked Questions with answers is designed to be read in conjunction with the NHS ESR Data Protection pack, which includes a template for providing Fair Collection information to Trust employees.

Data Warehouse

QUESTION: For the Data Warehouse, who is defined as the Data Controller and how are Data Protection Notifications managed ?

RESPONSE
The Data Warehouse is not a Controller in itself. Each entity with access to the Warehouse will be registered as a Data Controller. The Information Commissioner maintains a public register of all notifications via the website at http://www.ico.gov.uk/

For the ESR, each NHS Organisation is a Data Controller of its own employees' personal data. The Department of Health is also a data controller (having contractual liability and rights of enforcement).

For the Data Warehouse, given the large number of entities that are involved in the data warehouse element of the project, it is useful to categorise these entities into two main areas. Firstly there are those entities who have responsibility for the **transfer** of the information to the ESR and therefore by extension to the data warehouse. These have been classified as "**Transferring Controllers**" and are the same as for the ESR.

In addition, there are those entities that have responsibility for the **use** of the data in order to generate the requisite reports and so on. These entities can be considered as the end users of the warehouse and have been classified as the "**Reporting Controllers**". At present, they are

- NHS Employers organisation
- NHS Health and Social Care Information Centre

- All SHAs
- All Deaneries
- Health Solution Wales
- Welsh Assembly
- Department of Health (unlikely to need access as data will be provided to them by the Information Centre under SLA)

With regard to Data Notification for **Transferring Controllers**, a list of categories is available so that they can update existing notifications to ensure that the data is transferred to the ESR in a compliant manner.

Notification categories have not been drafted to cover the categories that are relevant to Reporting Controllers. Each controlling entity should itself determine given its knowledge of exactly how the personal data will be used within those entities and update their notifications accordingly.

QUESTION: Will individuals be notified of the exact nature of the data transferred to the Data Warehouse and is this data personally identifiable or generic?

RESPONSE – Non-sensitive personal data transferred to the Data Warehouse is broken down into the following key areas:

- Workforce Composition.

  FTE, headcount and time in post by care group, area of work, organisation, nature of contract, occupational code, grade, speciality, post, assignment, person and time.

- Workforce Movement.

  Joiners and levers, headcount and FTE, by area of work, occupation, person, workforce movement, organisation, staff group, census nature of contract, grade, speciality and time.

- Demonstrated Skills.

  Headcount and FTE of employees with skills, competencies and qualifications by skills profile, person, assignment, organisation, staff group, area of work, speciality, care group, nature of contract, occupation code and time

- Absence Management.

  Incidents, days lost and absence rate by absence type/absence details, area of work, staff group, organisation, person, care group, occupation code and time.

- Vacancies.

  Open vacancy FTE and duration by area of work, occupation code, organisation, staff group, vacancy, grade and time.

- Payroll and Earnings.

  Monthly earnings, basic pay, pay elements (grouped), hours/sessions worked/paid by assignment, staff group, person, organisation, grade, payroll frequency and time.

- Career Management

Headcount of employees with and without development and/or reviews by person, assignment, organisation, staff group, area of work, speciality, care group, nature of contract, occupation code and time.

- Training Attendance

  Headcount of employees attending training courses by person, training course, attendance status, organisation, staff group, area of work, speciality, assignment, nature of contract, care group, occupation code and time.

The only sensitive personal data transferred is ethnic origin and disability status, both of which are required to manage staff employment and ensure equal opportunities. The Fair Collection Notice gives general information about the purposes for the processing and the transfer to the Data Warehouse and it is not intended to give every member of staff a separate notification. However, in line with guidance in the Data Protection Toolkit, Trusts should consider what other information they provide to staff and how they provide this. Individuals will not be notified when their data is transferred to the Warehouse.

QUESTION: Who has ownership of the data in the Warehouse and what are the procedures for housekeeping, periods of retention etc. ?

RESPONSE

Ownership of the data lies with the NHS Trusts defined as Transferring Controllers. It is their data and they are responsible for its accuracy. However, users (Reporting Controllers) have access to the data for reporting purposes.

The period of retention is defined as the lifetime of the contract, up to 2014; historical data is held over this time to enable modelling and trend analysis. No automated housekeeping rules are currently in place; reports generated using Discoverer will be retained by the system for a fixed period, but are only accessible to their creator.

QUESTION: Do payroll extracts into the Warehouse required signed authorisation from the individuals concerned ?

RESPONSE

Data extracted to the Warehouse is not being used for new purposes; the processing is simply being conducted in a more efficient manner. Therefore specific consent of individuals is not required for the transfer of data to the Warehouse. Any organisation having access to your data will have a legal justification for access and will have to comply with the Data Protection Act. The legal rationale for not seeking explicit consent is covered in the main NHS ESR Data Protection pack.

The information extracted into the warehouse is for purposes such as completing the earnings survey and pay modelling for national pay review bodies. Within England, SHAs have restricted access to payroll and earnings sections of the warehouse to prevent people being identified.

QUESTION: Who can access the Data Warehouse ?

RESPONSE

At present, the list of organisations comprises:

- NHS Employers organisation
- NHS Health and Social Care Information Centre
- All SHAs
- All Deaneries
- Health Solution Wales
- Welsh Assembly
- Department of Health (unlikely to need access as data will be provided to them by the Information Centre under SLA)

However, this list is subject to change, if reviewed in the future; this is why the Fair Collection Notice template provided to Trusts cannot provide a definitive list of organisations with access. The above list will appear on the ESR website, and will be updated accordingly.

The NHS Prevention of Fraud unit have access to the core ESR system and are the only authority who can interrogate the system in this manner.

Consent

QUESTION: Does a Trust need consent from every employee for data to be held and processed on the ESR system? Can individual employees opt-out ?

RESPONSE

ESR uses the data provided by employees to provide an HR and payroll service; this does not represent any new purpose over existing systems and so consent to transfer data from legacy systems to ESR is not required. In addition, because the ESR service is required to manage employees and consent is not required, employees cannot opt-out from the service.

QUESTION: Does the processing of sensitive personal data within ESR require the explicit written consent of the individual ?

RESPONSE

There are a number of grounds within the Act that legitimise the processing of sensitive data; one of these is "explicit consent". However, under certain circumstances explicit consent is not required if, for example, the data is necessary for equal opportunities monitoring and employment law obligations. As processing is not for a new purpose, NHS Organisations are responsible for considering their own processing activities and the necessity of gaining any explicit consent from employees.

Overseas Transfer and Security

QUESTION: What is in place for ensuring the safety and protection of personal details against fraudulent use when some of the handling is to be carried in other countries. If by any chance someone did access such data, what would be the recourse?

RESPONSE

The Data Protection Act provides process and legal provision to protect data stored and processed within the European Economic Area (EEA). If data is to be processed outside the EEA, the assumption is that the organisation responsible for the transfer will make legal provision internally which is compatible with the Data Protection Act.

McKesson, as prime contractor, are responsible for fault diagnosis and rectification. Oracle act as a sub-contractor to fix application issues that McKesson cannot resolve.

Oracle US is a signatory to the Safe Harbour Principles, a scheme approved by the UK Information Commissioner as providing adequate protection to personal data made available in the US. This availability will then be deemed to be in line with the requirements under the Data Protection Act 1998. Currently, only Priority 1 issues would be dealt with in the US; none has yet arisen. All other issues will be worked on in the UK only, until a legal framework compliant with the Data Protection Act is demonstrably in operation..

The Electronic Staff Record project believes that a substantial benefit would be provided by the ability to fix any faults on a round-the-clock basis. This means that on some very rare occasions it may be necessary for Oracle staff based in countries outside the UK and US to view data screens in order for them to assess and fix technical problems**.** Consequently, we acknowledge that we need to work towards ensuring that any such data is secure and appropriately controlled. There are a number of factors, which we have been looking at to ensure that we can be confident that when this data does become available in India and Australia, it is within an appropriately secure framework and is in accordance with the Data Protection Act 1998. In particular, we are aware of the guidance from the Information Commissioner about overseas data issues. As part of this exercise, we are looking at the obligations which Oracle UK is to impose on its overseas group members as part of a binding corporate rules and intra-group transfer exercise.

QUESTION: Are UK jobs being outsourced to India and Australia ?

RESPONSE

We are NOT transferring staff data overseas to provide a payroll service for the NHS. The ESR service is provided within the UK; only a small minority of support calls may be handled overseas.

QUESTION: Will individuals and NHS Organisations be notified in those "rare and limited circumstances", in which staff based overseas are able to access personal data?

RESPONSE
No, such notifications will not normally be made. The potential for this remote data access for this has been raised in the Fair Collection Notice in order to make staff aware of the support model for ESR. Contractually and legally, the Department of Health and the NHS Central Team will not allow any overseas transfer outside the EEA unless security controls are in place that fully comply with the Act. By definition, it is likely that this access will occur outside normal office hours to fix any bugs on the system that may prevent someone being paid. Such access is only to fix faults and ensure that all employees receive the service that they require.

This area of service is one of the key benefits of ESR, in that the application is supported on a 24x7 basis.

QUESTION: Is it possible for individuals to exclude their records from those accessed from overseas ?

RESPONSE
No, individual exclusions cannot be made. However, it should be noted that data is not transferred abroad, it is simply viewable so as to provide 24 hour support for the system.

QUESTION: Can you confirm that advice has been sought nationally from the Information Commissioner with regards to the transfer of staff personal data outside the country?

RESPONSE
Yes, advice has been sought with regards to overseas access and support. Individuals and Trusts can be assured that all transfers and data processing will be conducted in accordance with the Act.

Data Security

QUESTION: What steps are being taken to ensure my details are not accessed to make inappropriate use of my identity and who will take responsibility should this happen ?

RESPONSE

ESR is built on industry-proven software, the Oracle HR Management System and uses secure technology. ESR is subject to appropriate security measures, defined by User Responsibility Profiles (URPs). The implementing Trust is responsible for ensuring that appropriate URPs are allocated to staff, in order to ensure the system is not compromised and access to personal data is only available to staff who require it. This is, in effect, no different to the measures that should exist with your present systems.

Access to the Data Warehouse is managed in a similar ways; users are granted certain privileges, specific to their role, when allocated log-in identifiers and passwords.

QUESTION: Where can a Trust find more information about the security conditions within the contract between the Department of Health and McKesson ?

RESPONSE

As part of the suite of documentation given to sites during implementation, a specific summary is being prepared to outline the security mechanisms within the system and the contract. This will be available shortly.

In practical terms, the NHS ESR Central Team and the Department of Health manage the contract on behalf of the NHS Trusts. Therefore, should a breach of security occur and an employee decide to take legal proceedings against a Trust, the case would be taken up by the Department and Central Team on behalf of the Trust, and redress sought from McKesson.

Data Cleansing

QUESTION: Are recommendations available on the data cleansing activities required as part of implementing ESR ?

RESPONSE

Data cleansing is clearly an on going activity which will be happening on legacy systems. However, we recommend that each organisation involved in the ESR project should ask employees to verify the information held on them prior to transfer into the ESR database.

When the information to be transferred to the ESR is provided to staff, they should be requested to notify any inaccuracies in the data by a given date. The ‘given date’ should provide them with a reasonable period in which to provide the requisite information. Six to eight weeks may for example be considered a reasonable time in which to ask people to update inaccuracies. This will account, for example, for annual leave and other eventualities. In addition, it is advisable to send reminders to staff. This could be done at the half way point, after say three weeks with a possible final follow up a week before the information is due to be returned. We have been advised that whilst one reminder is acceptable, two are preferable.

Some thought will have to be given as to how data subjects can provide updates to the data provided to them. For example, should information be updated via e-mail or a website or will all communications need to be in paper format? This also raises the issue of security, as it is vital that any system is secure and any communications are marked as confidential. For example, you may wish to provide secure return envelopes marked "strictly private & confidential". If electronic means of transmitting the data are to be permitted this will need to be carried out in a secure way involving the IT support. Consider whether risk can be minimised by removing information which is already known to be correct from any printout, e.g. salary. In addition, by organising the data to be sent by employee payroll number plus details rather than name plus details, the person to whom the data refers cannot be easily identified.

An individual cannot be forced to actually provide verification that his/her data is correct; therefore, if staff fail to respond, the Data Controller must provide reasonable, sufficient and practically achievable measures to individuals to ensure that the correct data is maintained. Organisations should also have processes in place to ensure that the accuracy of data continues to be maintained not only prior to its transfer to the ESR but also once the data cleansing process described above has been undertaken. This is very much an ongoing obligation of each Data Controller for all data being held and there should be responsibility taken within each organisation for ensuring that the Data Quality Principles are complied with at all times.

The data cleansing route, which would be most compliant with the Act, would be to ensure that data is accurate, cleansed and totally up to date before the data is transferred and before the ESR goes live. Not only does this lead to a more compliant approach in so far as the Data Protection Legislation is concerned but in addition there are the obvious practical benefits of having accurate information on the system before it starts to be used. If organisations were to do this at the later stage (after ESR go-live and therefore use ESR in order to generate a printout, which would, then be verified and "cleansed") then it simply means that the risk to the organisations is greater because non-compliance is prolonged. Whilst out of date or inaccurate information continues to be held, there is always a risk because this is essentially a breach of the Data Quality Principles.