Guide to inform your Data Protection Impact Assessment (DPIA) for NHS Jobs

Introduction

This document has been prepared to assist organisations who need to complete a Data Protection Impact Assessment (DPIA). If you require any further information direction is required, please direct your queries to your Data Protection Officer.

Information held by the NHS Jobs Service

The NHS Jobs service holds information pertaining to vacancies in organisations who hold an NHS Jobs account. It holds information from candidates who hold a personal account in NHS Jobs, used to apply for roles. The information held on candidates includes personal data as well as personal sensitive data and is requested to process the candidate for roles they apply for and is held in accordance with data protection legislation. The information held on candidates includes personal data as well as personal sensitive data which is legal required as part of offering someone a contract of employment or required to help make decisions about whether a candidate is suitable for the role.

The NHS Business Service Authority is registered with the ICO., as a data controller. For further information please check the ICO website - Information Commissioners - Data protection register - NHSBSA.

Data Protection

Both organisations and candidates are informed via our Terms and Conditions which explain the ways in which the service processes data and the responsibilties of all parties involved.

Employer - Terms and Conditions
Candidate - Terms and conditions

The terms and conditions outline:

- The data protection legislation that relates to the processing of personal data and privacy.
- Information relating to Freedom of Information requests.
- Further information relating to roles and responsibilities in appendix 2.

Who is the Data Controller?

The NHSBSA is a data controller for info in NHS Jobs up to the point when the candidate submits their application, at which point the vacancy holder becomes the data controller and NHSBSA becomes a processor.

Please refer to clause eight of our Terms and Conditions for further information. In addition, roles and responsibilities are available in Appendix 2 of the Term and Conditions.

Additional Background Information

Currently all potential candidates are required to register for an account in order to be able to apply for vacancies published on the website. Once an account has been created potential candidates have the ability to create a ‘profile’ application and have the option to use the data when applying for vacancies. The ‘profile’ data, if created,

is retained within their account for the life of NHS Jobs unless they request for their account to be deleted by the supplier.

Submitted application form data can be viewed by employers who have been given a user account within their organisation. The role assigned to each user will determine the data that they can see, and permissions they have to complete actions. Super Users, recruitment officers, recruitment team managers, and recruiting managers have the ability to view application data dependant on their allocated responsibilities in the system. Recruiting managers are not able to view the personal details section of the application form until after shortlisting has been finalised. This ensures that personal data is only accessible for those people who need to view the information in line with their responsibilities for processing applications.

Recruiting organisations have the ability to allow a potential candidate to copy their CV into the service. The content of the CV in its entirety can be viewed by the recruiting managers.

Application data can be downloaded for the following purposes:

- Shortlisting
- Interviews

Some NHS organisations transfer NHS Jobs data to the Electronic Staff Record (ESR) via an interface between the two systems. Organisations only have the ability to transfer successful candidate data.

Some organisations use a third party Applicant tracking System (ATS) provider to complete their recruitment processes. In cases such as this candidates are re-directed to apply via the third party provider and no application details are held in the NHS Jobs service.

The service is fully accesible and both organisations and candidates can read our Accessibility statements directly on the service.

Employers - Accessibility statement for NHS Jobs – Employers | NHSBSA
Candidates - Accessibility statement for NHS Jobs – Applicants | NHSBSA

Frequently Asked Questions

Legal Basis and Purpose of Processing Data (lawfulness, fairness, and transparency

1. What is the legal basis for processing the candidate personal / special category data?

    - Personal data
    - Performance of a contract
    - Special Category
    - Employment
    - Health

Candidate consent is also recorded, though is not the sole legal basis for processing.

2. Does the service inform employers and candidates of their responsibilities and obligations for processing data?

    - Employers who have been granted a user account and candidates who register with the site must agree to abide by the NHS Terms and Conditions before gaining access to their account and meets GDPR: Article 3 (b) and Article 9 (b) and (h).

3. Is data held in the NHS Jobs service processed outside of the UK?
    - All data held in the NHS Jobs service is processed and will not be transferred outside of the UK or the European Union.
    - This is compliant with Article 44 of the General Data Protection Regulations as well as other legislation which can be found in Article 8 of the Service's Terms and Conditions detailed above in answer to question 2.
4. Are personal sensitive data being separated from personal data?
    - Yes, both sets of data are only revealed at the appropriate stage of the recruitment journey and sensitive personal details relating to candidates are collected solely for reporting purposes.
    - Unless a candidate discloses their identify in their curriculum vitae, a recruiter will not be able to see the identity of the candidate until they need to. For example, after shortlisting and to invite candidates for interview.
    - Information relating to fitness to practice, and criminal records supplied by the applicant can be seen by all users who are named on the vacancy for any candidates who are invited to interview. Information relating to pre-employment checks are restricted and Recruiting Managers can only view the progress but not the detail relating to these checks.
5. Is the processing of personal data intrusive?
    - No, data is shared at the relevant point of the recruitment cycle.
    - When data is shared it is controlled by permissions and only where necessary.
6. Does the service allow for the possibility of disparate treatment of individuals?
    - The data provided by candidates is used by recruiting organisations to make decisions regarding offers of employment.
    - Such decisions are made according to criteria which is applied in a fair and balanced manner to all candidates.
7. How will confidentiality be maintained?
    - The system has role-based security measures which prevent access to information which is not appropriate to the recruitment activity being conducted. This ensure the appropriate level of confidentiality is maintained.
8. Does the NHS Jobs Service have a privacy policy?
    - Yes, this can be found here –
        - Employer - NHS Jobs Privacy Policy
        - Candidate - NHS Jobs Privacy Policy
9. Do we tell individuals about the use of cookies and other tracking technologies and are these changing?
    - Yes, the NHS Jobs Service has a cookie Policy in place Cookies (jobs.nhs.uk). There is also have in system pop up messaging asking users if they want to accept or decline cookies.
10. Does NHS Jobs process and share data with other organisations?
    - Statistical data is shared with the Department of Health and is anonymised.
11. Can candidate data be migrated to other systems by an electronic transfer?
    - Yes, to the Employee Staff Record (ESR).

12. What process is used to transfer data to ESR?

    - The transfer of data from the new NHS Jobs service to ESR is via a RESTFUL API, using password basic authentication, with an NHS Jobs endpoint which is secured to only allow access from the NHSBSA internal network, the end points of ESR are HTTPS.

13. Are any decisions affecting individuals made solely on processing by automatic means?

    - No.

Consent of Account Holders/Candidates

14. What consent is provided by account holders prior to sharing this information?

    - Informed and freely given.
    - Given by an affirmative action
    - Recorded as the condition for processing upon each application by the candidate.

15. Can an account holder delete their profile or account?

    - When a candidate registers for an account on NHS Jobs, they can create a profile which is effectively a draft application form. Once the profile is created, they can choose whether they wish to download the data from their profile into an application form when applying for a position. The data within the profile remains available for the life of their account.
    - If the candidate chooses to request to delete their account, all data relating to the profile will be deleted at the same time.

16. Can candidates withdraw their application?

    - The candidates can withdraw their application which removes the ability for employers to continue to view the details of their application.

17. Are Account holder's profiles subject to a retention period?

    - A candidate's profile is not subject to a retention period and this data will remain in the system until an account deletion is requested. No sensitive personal data is held on the candidate's profile only their name and email address.

18. Are account holders informed of how their data will be processed?

    - The process to open an employer account, includes a requirement for an employer to provide an organisational privacy notice and should reflect their processes accordingly. This is the responsibility of the employer to ensure its accuracy not the NHSBSA.
    - Candidates can read the privacy notice upon applying for a vacancy, but it is not mandatory.

19. Do candidates provide consent to information being requested as part of their pre-employment checks?

    - Yes, they provide details of their referees, registration and consent for information relating to any prior NHS service.

20. Is a candidate informed when they are redirected to any other provider that works in conjunction with NHS Jobs?

    - Yes, if an employer uses an ATS provider, the candidates is warned they are being re-directed to apply on another provider's service.

21. Are candidates informed and provide consent for their data to be migrated to the Employee Staff record (ESR), if an employer uses the service?

    - Candidates do not provide consent within the service but are warned that they are being re-directed to a third party. Any organisational privacy notice should detail this as applicable.
    - Information from a candidate's application will be transferred to ESR (if an employer uses it) upon acceptance of a final unconditional offer of employment. This information will relate to information submitted in accordance with maintaining records to meet:
        - Performance of a contract
        - Employment
        - Health
    - This is compliant with the ICO Data minimisation principle.

Use of Personal Data (Data purpose & minimisation principles)

22. What are the purposes of processing personal data?

    - Personal data is collected within the application form to match with the applicant in relation to their application so that they can be contacted and invited to interview if their application is successful and sent an offer letter/contract if they are successful following interview.
    - Some personal and sensitive personal data may also be transferred to Electronic Staff Record (NHS organisations) to create an employee record. This only applies to candidates who accept their contract of employment and for those organisations using ESR.

23. What type of personal data is processed?

    - Name and surname.
    - Email address.
    - Phone number.
    - Home address.
    - Date of birth.
    - Personal Identifiers
    - IP address.
    - Other - Information is also gathered regarding disciplinary hearings, alert notices and any other personal data which may have been disclosed in a CV.

24. What categories of sensitive personal data (Special Categories) are processed?

    - Racial or ethnic origin
    - Religious beliefs,
    - Health and disabilities
    - Gender, sex, and sexual orientation
    - Information relating to pregnancy
    - Offences and cautions.

25. How is a candidates data used?

    - A candidate's data (in relation to the application form they have submitted) will be reviewed in terms of ascertaining if they are suitable for the position for which they have applied. Candidate data will then be used to contact successful candidates so they can be invited to attend interview/assessments. If a candidate is identified as

appointable, this data is also used to send the candidate an offer, complete pre-employment checks and once these are successfully completed, send a contract.

- When a potential candidate registers for an account on NHS Jobs they can create a profile, which is effectively a draft application form. Once created they can choose whether they wish to download the data from their profile into an application form when applying for a position. The data within the profile remains available for the life of their account. If the account holder chooses to request that their account is deleted, all data within that account will be removed.

26. Is the identity of candidates masked so that their identity is only accessed when required?

    - Yes. When a candidate applies for a vacancy, they are given a unique application reference (AR) number when accessing the application form. This number is retained throughout the application process for that vacancy.

27. Does the system analyse data to assist in identifying previously unknown areas of note, concern, or pattern?

    - No, the personal details of candidates are protected early in the process to ensure that a fair selection process is followed.
    - After a short-listing decision is made some personal and sensitive personal data is shared with decision-makers. This includes:
        - Their name, email address and preferred telephone number.
        - Their immigration status and right to work details.
        - Fitness to practice information (where required for the role).
        - Previous criminal convictions and cautions (where required for the role).
        - If the candidate is 'at risk.'
        - If the candidate wishes to be part of the guaranteed interview scheme.
    - This information is restricted to the relevant roles on the vacancy who need to see this information.
    - Any equality and diversity data that a candidate discloses, cannot be seen by the organisation during the recruitment process and the data is for reporting purposes only as required by the Equality Act 2010 section 149.
    - Where an organisation uses ESR that is integrated with NHS Jobs, this data will migrate to ESR once the candidate accepts the contract in NHS Jobs.

28. Are any measures in place to ensure that further processing of applications and the associated data is compatible with the original purposes for which it was obtained?

    - The service only allows employers to download candidate details into ESR when they have accepted an offer of employment.
    - If the employer accepts the offer on behalf of the candidate, the candidate is informed by the service.
    - Applications can be downloaded from the service although no notification of this is provided to the candidate.
    - It is an organisation's responsibility to detail this in the privacy notice and have processes and audit procedures in place to monitor this.

29. Does NHS Jobs use personal data for new purposes?

    - No.

30. What other ways might an account holders' data or activity might be monitored?

- IP addresses are held in an audit log for the following reasons:
    - If an account holder reports suspicious activity on their account, we will use the IP address to see where requests may have come from.
    - In an investigation (e.g., anti-fraud) we will provide IP address to give geographical and /or telecoms provider info
    - to the investigator.
    - We may use it to investigate malicious activity (e.g., scraping adverts or automated application and can block this activity).

31. Are items of personal data held in every case which is only relevant to some customers?

- Each time a candidate applies for a vacancy they are required to complete an application form in full. Candidates can either upload the data contained in their profile or use a blank application form.
- Information is captured and only made accessible until such time as the service deems it relevant to share such data.
- Candidates agree to provide this data as part of their application.
- Recruiters choose which additional application questions are added to the standard application form to capture information they feel is relevant for that recruitment.

32. Are candidates compelled to provide the personal data to the NHS Jobs service and if so why?

- An absence of personal data would not allow successful candidates to be contacted if successfully shortlisted and to be invited for interview.

33. Are candidates compelled to provide the sensitive personal data to the NHS Jobs service and if so, why?

- No, candidates are required to submit a response to questions in relation to:
    - Criminal records
    - Fitness to practice and their registration.
    - Candidates are not required to provide detail in relation to these questions at application.
- These details are required to complete background checks and are:
    - Performance of a contract
    - Employment
    - Health

34. Can candidates withdraw applications and does the organisation still retain data relating to the application?

- Every application that gets submitted by a candidate is made available to them.
- Candidates can withdraw their application up until the offer stage whereupon they can decline the offer.
- Prior to the point of offer, candidates can withdraw their application which deletes their application from the organisation's account and data pertaining to their application.

Data Quality (accuracy principle)

35. What is the impact of the information being inaccurate or out of date on the individual and the NHSBSA?

    - The candidate is responsible for the data they input into their application form. Each time they apply, they must tick a declaration box confirming the information they have provided is accurate.
    - 'The information in this application form is true and complete. I agree that any deliberate omission, falsification, or misrepresentation in the application form will be grounds for rejecting this application or subsequent dismissal if employed by the organisation. Where applicable, I consent that the organisation can seek clarification regarding professional registration details.'

36. How are personal data checked for accuracy?

    - Personal data is not checked by the system, and it is reliant on candidates checking their data before submitting their application form.
    - There are fields in the service that have validation – i.e., National insurance numbers.

37. How do candidates correct information held in the service?

    - Candidates can amend information on draft applications.
    - Once a candidate has applied, they would need to correct any information directly with the organisation if it pertained to their email address or telephone number.
    - A candidate would need to contact the NHSBSA to update their details relating to their email address.

38. How frequently is the personal data updated or what would trigger the information being updated?

    - Once a candidate has registered an account on NHS Jobs the account is there for the life of the system or until a candidate contacts NHS Jobs and requests their account to be deleted.
    - The candidate is responsible for ensuring their personal data is up to date.
    - Candidates cannot amend their email address on the account.
    - Candidates cannot amend their personal details (email address or telephone number).

39. What action is taken to correct inaccurate personal data?

    - Only data relating to pre-employments checks can be updated by an employer.

40. Are the sources of the personal data recorded in the record?

    - Candidates must be logged into their account to submit their application and associated personal data.
    - Candidates are asked to confirm that their personal information is accurate prior to submission.
    - There is an audit trail which shows the origin of the input. Employers do not have access to an audit trail, but this can be requested from the NHSBSA.

41. Are there procedures to monitor the factual relevance, accuracy, and timeliness of free text/comments about individuals?

- There are free format comments on the application that can be entered by the recruitment team. At present, individual organisations are responsible for ensuring the validity of these comments.

42. Do we state the consequences to the individual of not providing certain information?

- Candidates declare and consent to the following statement – 'The information in this application form is true and complete. I agree that any deliberate omission, falsification, or misrepresentation in the application form will be grounds for rejecting this application or subsequent dismissal if employed by the organisation. Where applicable, I consent that the organisation can seek clarification regarding professional registration details.'

Personal Data Retention (Storage Limitation Principle)

43. How long is information held in the NHS Jobs service?

- The system will automatically delete candidate data from the employer account after a maximum of 460 days after the closing date of a vacancy.
- The system will automatically delete unsuccessful applications that have not proceeded to offer, 400 days after the closing date of a vacancy.

44. What is the justification for holding data for the agreed time?

- To complete recruitment processes and run annual reporting for national reporting for equality and diversity monitoring.

45. Who has agreed the retention period?

- The Department of Health.

46. What is the process for deleting information held in the system?

- An automated deletion process occurs every day.
- Account holders can request their accounts are entirely deleted from the system.
- Once data is deleted either manually or automatically the data is not retrievable.

Data Sharing and Disclosure (Integrity and Confidentiality Principle)

47. How are system users maintained and what is the frequency of this being audited for leavers / joiners / movers / escalated access?

- At an organisational level, it is the responsibility of the Super users to maintain who has access to the NHS Jobs service and that the role assigned to the user is commensurate with their responsibilities.
- This requirement can be accessed in the Acceptable Use Policy.

48. Which records/functions are restricted so that users only access the information they need to access for their role?

- Within the NHS Jobs service, there are various pre-defined roles which manage what the user can see and action. This changes throughout the recruitment journey.
- Support role permissions are based on a 'least privilege' basis to ensure that staff have the most restricted level of access that still permits them to perform their designated role.

49. Who is responsible for training employees in relation to unauthorised browsing and related privacy training?

- Organisations are responsible for the training of their Teams and users of the NHS Jobs service.

- Guidance documents are provided to support an employee's understanding of appropriate use of the service.

50. What interfaces are there to other systems?

- NHS Jobs interface with Electronic Staff Records where data transfers between the two systems.
- NHS Jobs has an interface with EE for SMS (text message) processing.
- Any data taken and uploaded to a third-party system is bound by the service's terms and conditions to provide us with an extract of the information taken to the third-party system.

51. Is any information held in the service supplied to third parties?

- Only aggregated information is shared with the Department of Health for statistical purposes.
- All personal data is anonymized and so an individual cannot be identified.