

## Recruitment privacy notice

### How we process your personal data

Telstra Health UK process your personal data when you apply to work for us. You will be the source of most of this data but we will receive data from other sources including former employers.

We use this to make hiring decisions and to complete necessary checks when we have made an offer of employment. These include checks on your right to work in the UK, your qualifications and your previous work history.

This notice explains how and why we process personal data for recruitment purposes and will be updated from time to time, so please check our website for the latest version.

### What information we collect about you

We collect and use information about you when you apply to work for Telstra Health UK. We also process personal information to complete necessary checks when we have made an offer of employment. This includes your CV, proof of qualifications and any references or other checks, such as for eligibility to work in the UK. Broad categories and examples of the information we may hold about you through the recruitment process are given below.

**Applicant related data:** your title, forename, middle name(s) and surname, birth name, preferred name, any additional names, gender, nationality, second nationality, civil/marital status, date of birth, age, home contact details (e.g. address, telephone number, e-mail), driving licence, passport details or national ID number, residency status, immigration and eligibility to work data/visa, languages spoken.

**Recruitment data:** employment history, education, qualifications, professional licenses, referee details, CV and application, interview records, vetting and verification information.

**Regulatory data:** records of your registration with any applicable regulatory authority, your regulated status and any regulatory references.

**Information collected at the offer stage:** bank account details, National Insurance number, tax information, third party benefit recipient information, next-of-kin/dependent and emergency contact information, references, Disclosure and Barring Services (DBS) checks and credit checks (where necessary for the role).

**Sensitive personal information:** We may collect personal information about you which may be considered sensitive or protected under applicable laws. For example, we may collect information about your:

- health in connection with leave entitlements, workplace safety and support;
- criminal record checks where necessary to assess your suitability for a role.

### How we use your information

We may collect and record your personal information from a variety of sources, but mainly directly from you. You will usually provide this information directly to the hiring manager or Human Resources or enter it into our systems (for example, during the recruitment process, your participation in HR processes, emails you send, documents you create or through verbal information which may be recorded).

We may also obtain some information from publicly available sources (e.g. social media) as well as from third parties, for example, references from a previous employer, tax authorities, benefit providers or where we employ a third party to carry out a background check (where permitted by applicable law).

Where we ask you to provide personal information to us on a mandatory basis, we will inform you of this at the time of collection and in the event that particular information is required by contract or statute this will be indicated. Failure to provide any mandatory information will mean that we cannot

carry out certain HR processes. For example, if you are made an offer of employment and do not provide us with proof of your right to work in the UK, we will not be able to employ you.

You may sometimes provide information about other individuals to us (e.g. your referees, emergency contacts, dependents, or work colleagues). If you do so, you must have first:

- obtained consent from those individuals for us to collect that information (if required under applicable laws);
- informed those individuals that you are providing that information to us and the purposes for which you are providing that information; and
- advised them of the relevant parts of this privacy notice.

The other individuals may provide information about you to us, where necessary and permitted by applicable laws. As a general rule you should avoid providing sensitive information about other individuals unless absolutely necessary.

The legal reasons, under data protection law, for processing your information are that it is necessary:

- for a contract or to enter into a contract;
- to comply with a legal obligation;
- to comply with employment law;
- for purposes of legitimate interests.

In some cases we may ask for your consent to process your personal information. Consent must be freely given, for specific purposes, informed and clearly indicated. You have the right to refuse or withdraw your consent.

Purpose for processing	Lawful basis
Recruitment and selection.	<p>This processing is <u>necessary to take steps at the applicant's request to enter a contract of employment</u>.</p> <p>This processing is also necessary for the purpose of the <u>legitimate interests</u> pursued by Telstra Health UK. Telstra Health UK considers that it has a legitimate interest in fully assessing applications for employment to ensure that only suitable and appropriate candidates are both assessed and selected.</p>
Appropriate vetting for recruitment and team allocation including, where relevant and appropriate credit checks, right to work verification, identity fraud checks, criminal record checks (if and to the extent permitted by applicable laws), relevant employment history, relevant regulatory status and professional qualifications.	<p>This processing is <u>necessary for the compliance with legal obligations</u> to which Telstra Health UK is subject.</p> <p>This processing is also necessary for the purpose of the <u>legitimate interests</u> pursued by Telstra Health UK. Telstra Health UK considers that it has a legitimate interest in managing its business operations in the most effective way and wishes to maintain its reputation and continue to attract high calibre employees.</p> <p>Telstra Health UK has a legitimate interest in the proper vetting of its employees and in being able to provide assurance to NHS Digital and to customers that the checks are proportionate to the risks. Information relating to criminal records, including checks through the Disclosure and Barring Service (DBS), will be processed on the basis of these legitimate interests and on the <u>condition of the right for employers to ask</u>.</p>
Complying with applicable laws and regulation (for example maternity or	This processing is <u>necessary for the compliance with legal obligations</u> to which Telstra Health UK is subject.

Purpose for processing	Lawful basis
parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulation).	
Complying with data protection laws and responding to requests from individuals as data subjects or from the Information Commissioner's Office (ICO) or other authorities.	This processing is <u>necessary for the compliance with legal obligations</u> to which Telstra Health UK is subject.

### Information we may share with other organisations and where it is processed

In some cases, we may need to disclose your personal information to related entities, partners and other organisations, both within and outside the UK, for purposes related to your application for employment or engagement with Telstra Health UK. Unless specific consent is required, please take this as notice that your information may be transferred or used as described in this section, without the need for further consent or notification to you. In general your information may be disclosed:

- to third parties who provide services to us so that such organisations and contractors can assist us with the purposes for which we may use your information. These services include training and conference providers, mailing, information technology, network, legal, business consulting, banking, payment, data processing, data analysis, document management, information broking, research, investigation, insurance, auditing, surveillance, payroll, human resources, superannuation and staff benefits services;
- to your authorised representatives;
- to third parties who provide business IT support services to us;
- to law enforcement and national security agencies, and other government and regulatory authorities, as required or authorised by law; and
- to any other party for any other purpose related to your application for employment at Telstra Health UK.

Below are some examples of which other organisations may process your information and if it is transferred outside of the UK. In many cases the transfer of data overseas is due to the use of Cloud services. This list is not exhaustive.

Organisation	Purpose	Processing location
BioCity	For interviews in Nottingham, BioCity facilities management require your name for building access and vehicle registration for visitor parking.  BioCity operate CCTV as data controllers separate to Telstra Health UK.	<a href="#">United Kingdom, EEA, unless necessary to transfer overseas</a>
Microsoft	Microsoft 365, including Outlook for emails relating to your application	<a href="#">Australia through Telstra Health</a>
The Referencing Agency	Vetting and reference checks, this will include contact with your referees and, where applicable, the DBS.	<a href="#">United Kingdom and Republic of Ireland, except where requested to make checks in a third country</a>
TrustID	Identity and right to work in the UK checks	<a href="#">United Kingdom</a>

### How long we keep your information

For unsuccessful candidates we keep copies of application information, such as CVs and covering letters, for up to one year after the end of the recruitment process for the advertised vacancy. The information is retained to provide assurance that the process is run fairly. It is also retained so that we can consider applicants for similar vacancies during that time.

We keep anonymised statistics about candidates to inform and improve our recruitment process. We will not be able to identify individuals from these statistics.

Information relating to successful candidates will be transferred to an employee file once they start work with us.

We do not record details from basic DBS checks, but we do note if it has been satisfactory or not.

We aim to keep your information accurate and up to date. When personal information is no longer required it will be deleted securely.

### Your rights

<b>Informed</b>	✓	This notice and details at <a href="https://telstrahealth.co.uk/privacy">https://telstrahealth.co.uk/privacy</a> inform you about how we use your data.
<b>Access</b>	✓	You can request a copy of personal data we hold about you.
<b>Objection</b>	✓	You can object to your data being processed on the basis of legitimate interests.
<b>Portability</b>	✗	Not applicable.
<b>Correction or change</b>	✓	Request that the information we hold about you is corrected or changed.
<b>Erasure</b>	✓	This is your 'right to be forgotten'. You can request that we erase your personal data.
<b>Restriction</b>	✓	You can request that the use of your personal information is limited to storage only.
<b>Informed of automated decision making</b>	✗	We do not use your data to produce decisions made solely by computers rather than people.
<b>Withdraw consent</b>	✓	Where you have consented to us processing your personal data you can withdraw this at any time.

We will respond to rights requests within a month of receipt. Contact our Data Protection Officer for more information. Find out more about your personal data rights at the [Information Commissioner's Office \(ICO\) website](#).

### Data Protection Officer

Our Data Protection Officer can be contacted by email on [DrFoster-InfoGovInbox@health.telstra.com](mailto:DrFoster-InfoGovInbox@health.telstra.com).

### How to complain

If you feel that we have let you down in relation to your information rights then please contact our Data Protection Officer using the details above.

You can also make complaints directly to the Information Commissioner's Office (ICO). The ICO is the independent authority upholding information rights for the UK. Their website is [ico.org.uk](http://ico.org.uk) and their telephone helpline number is 0303 123 1113.