***eCredential* PRIVACY COLLECTION STATEMENT**
11 September 2019

We are required by law (in Australia and New Zealand) to provide information to you about how we collect, use, store and disclose your personal information. This document provides you with the details in relation to this. Particulars of our identity and contact details are at the end of this notice.

We collect, use, store and disclose your personal information for two separate and distinct functions:

1. *where you are a doctor, health practitioner, nurse or other qualified member of medical staff (generically, a "**Clinician**"), to let you create and maintain your self-managed centralised clinical profile which can be shared with hospitals and other health service providers (each an "**HSP**"); and*

2. *where you are an officer, employee or agent of an HSP (generically, an "**Administrator**"), to identify you to allow access to the HSP's portal on behalf of that HSP (including any copy of a Clinician's profile, where consented to by that Clinician for that HSP).*

*If you are a Clinician located in the European Union when you provide your personal information or data to us, and the General Data Protection Regulation ("**GDPR**") applies to that data, we will process your personal data in accordance with the collection notice set out at Schedule 1.*

Where, as a Clinician, you:

(a) *create a profile, the data contained in your profile (as may be updated by you from time to time), will be held by us in a database controlled by us (the "**Clinician Portal**"); and*

(b) *subsequently consent to a copy of your profile being made available to an HSP, the HSP will store a one-off copy of that profile in its own separate database as also provided and supported by us (an "**HSP Portal**").*

*The HSP will be able to add and annotate whatever further information it wishes, which may include reasons for acceptance or rejection from roles, role details and reporting lines, length of time of employment, job description and authorisations, performance observations, gross annual income, base pay, pay period details, entitlements and similar information, including other personal information relating to you (collectively, "**Employment Records**"), to the records in its HSP Portal.*

COLLECTION FOR CLINICIANS:

Why we collect your personal information

Where you are a Clinician, we collect your personal information:

(a) *to enable us to provide data services for you, to let you create your account, establish your username and password and create and maintain your self-managed centralised clinical profile which can be shared, at your election, with an HSP;*

(b) *to enable you, at your election, to procure and maintain professional indemnity insurance ("**PII**") from a third-party provider;*

(c) *where you have consented to a copy of your profile being made available to an HSP, to enable that HSP to create and maintain such data fields, including Employment Records, as it considers appropriate consistent with its own privacy policies and internal procedures; and*

(d) *to deidentify that information, to develop and offer multi-data insights, reports and market benchmarking analyses for HSP customers or other parties.*

What personal information do we collect?

The personal information we collect about you as a Clinician includes (or may include) your name, photo', contact details, date and place of birth, gender, current and past place of work and position title, current and previous residential address(es) and other data relating to your employment history or résumé.

Where you have consented to a copy of your profile being made available to an HSP, we may also collect Employment Records, as part of the records created by that HSP and held in its HSP Portal.

How we collect your personal information

We usually collect your personal information directly from you, to let you create and maintain your self-managed centralised clinical profile in your Clinician Portal. We may also initially collect your personal information from Employment Data entered by a current HSP employer when it creates its HSP Portal as our customer. In this case, you will be notified that a profile has been created for you in your Clinician Portal, and you will be able to log in, take control of, update and maintain any such personal information as your own self-managed centralised clinical profile from that time.

*We may also, through our services, obtain personal information about you from entities involved in the registration and accreditation of various health professions in Australia, such as the Australian Health Practitioner Regulation Agency ("**AHPRA**"), and from your PII insurer.*

Where you have consented to a copy of your profile being made available to an HSP, we may also collect personal information comprising Employment Data from your HSP employer as our customer, but only for retention in its HSP Portal.

You may choose what personal information you provide to us

It is up to you what personal information you provide to us for purposes of your Clinician Portal. However, if you choose not to provide certain information, it may affect the way an HSP can interact with you or whether we can enable that interaction at all in providing our services. For example, if you do not:

(a) provide sufficient information, or we are otherwise not able to satisfy ourselves as to your identity, we may refuse to supply you with our information services;

(b) provide us with your AHPRA number, after identifying that you are registered with that body, you will be unable to proceed to set up your Clinician Portal; or

(c) manually update your PII information, notwithstanding its renewal through a third-party provider (and any upload of a new Certificate of Currency, as relevant), the information presented on your Clinician Portal will be out-of-date and present incorrectly to any HSP you may elect to share with.

It is up to the HSP as to what Employment Records or other personal information about you it may provide to us for purposes of its HSP Portal.

How we use your personal information

In providing our information services for your Clinician Portal, you accept that:

(a) the primary purpose for collecting your personal information is to host and allow you to create and maintain your self-managed centralised clinical profile which can be shared, at your election, with an HSP;

(b) an account will be created for you using your personal information when you access our information services, with relevant information also disclosed to one or more related companies for invoicing or report purposes;

(c) we are only likely to provide your personal information to an overseas recipient where:

- *you access your Clinician Portal from outside Australia;*
- *you choose to provide a copy of your profile to an HSP which is a foreign entity (for example, where the HSP is located in NZ or Malaysia), is a branch of a foreign entity, or which otherwise has a foreign activity (such as a processing centre) or presence (in which case, the recipients are likely to be in those relevant jurisdictions in which that entity is established or the activity operates); or*
- *that personal information is accessed by our Parent in providing us with technical, security and data validation support for personal information stored by us in order to provide our services, in which case the Parent is contractually obliged to access and handle any such information in accordance with the Australian Privacy Principles set out in the Privacy Act 1988 (Cth);*

(d) where you provide an identity document to us, you may have your identity information verified with the document issuer or Official Record Holder;

(e) we may make your personal information available, including a document provided by you, to a relevant government authority or an issuing body (or, with your consent, to a designated person that can certify an identity declaration for the purposes of identity proofing), if we are not satisfied as to your claimed identity or the legitimacy of the identity documents supplied for purposes of an authorisation code application; and

(f) we and our related companies may, at any time, use and disclose your personal information to:

- *monitor traffic on our website;*
- *undertake data management for quality or operational purposes (and, where any such data contains sensitive information, that data will be de-identified to protect you, and this functionality is within your reasonable expectations);*
- *diagnose data collection issues (with any technical navigation information required for that purpose purged immediately after a problem (if any) has been remedied); and*
- *investigate any complaint made by you or on your behalf, either privately or by a relevant regulator or law enforcement agency.*

Our Privacy Policy also contains information about how we handle personal information and is available at www.equifax.com.au/hrsolutions/pdf/privacy.pdf.

We may also de-identify your data to develop and offer multi-data insights, reports and market benchmarking analyses for HSP customers or other parties.

How we store, use and disclose your personal information

As outlined in the description of our use of your personal information, we may use or disclose your personal information:

(a) to create your Clinician Portal;

(b) to maintain your profile on the Clinician Portal and enable you to share, at your election, a point-in-time copy of your profile with an HSP of your choice or otherwise share that profile to an HSP with your permission; and

(c) to other companies related to us, in particular those which provide services to us.

When your personal information is used for data analytics, it will always be de-identified.

Where we receive Employment Records input by an HSP against any copy of your profile which you have elected to make available to that HSP, those records and related data are visible only to that HSP and the HSP is the owner of that data. To the extent that we access, use or disclose any such personal information, you agree that data constitutes evaluative information generated within our information service as agent of that HSP in connection with commercially sensitive decision-making processes conducted by that HSP, and so is not subject to disclosure by us to or at your direction or request. Any requests for access to such data must be directed to the HSP and will be governed by its privacy statement and policies.

We supply your personal information to an HSP through download from our website. When you communicate with an HSP, receive or share an authorisation code, or choose to provide or receive personal information by e-mail, you acknowledge that e-mail is not a secure form for transmitting information and that any communications transmitted over it may be intercepted or accessed by unauthorised or unintended parties, may not arrive at the intended destination or may not arrive in the form transmitted. In such circumstances, we take no responsibility for communications transmitted over the internet and give no assurance that such communications will remain confidential or intact. Any such communications are at your sole risk, as are any communications between you and the HCP or other party you choose to deal with.

Where our information services are accessed through means or in formats other than by use of our app and on-line as originally intended and provided by us, you remain responsible for reviewing all pertinent portions of our services, including any relevant disclosures and disclaimers.

Other than where personal information is shared with an off-shore third party as is reasonably necessary for one or more of the functions or activities covered by this Statement, we store, use and process your personal information in Australia on our secure information technology servers, which may include hosting through our Virtual Private Cloud using servers located in Australia under a managed services/SaaS model (where the vendor does not access or process Data).

COLLECTION FOR ADMINISTRATORS:

Why we collect your personal information

Where you are an Administrator, we collect your personal information to satisfy ourselves that you are an accredited representative of the HSP that we provide services for.

What personal information do we collect?

The personal information we collect about you includes (or may include):

(a) your name, contact details, date and place of birth, gender, place of work and position title, current and previous residential address(es) and other data as may be required to conduct alternative proof of identity checks; and

(b) such other Employment Data as may be made available by your employer HSP.

How we collect your personal information

We initially collect your personal information and Employment Data from your employer as our customer. We may also collect personal information directly from you, to verify your identity as Administrator.

You may choose what personal information you provide to us

It is up to you what personal information you provide to us in addition to records supplied by your HSP employer. However, if you choose not to provide certain information, it may affect the way we can interact with you or whether we can interact at all in providing our services. For example, if you do not provide sufficient information, or we are otherwise not able to satisfy ourselves as to your identity, we may refuse to supply you and your employer (as relevant) with our information services.

How we use your personal information

In providing our information services, you accept that:

(a) the primary purpose for collecting your personal information is to create your Administrator status, for the benefit of your employer in respect of its HSP Portal;

(b) an account will be created for you using your personal information when you access the HSP Portal information services, with relevant information also disclosed to one or more related companies for invoicing or report purposes;

(c) we are only likely to provide your personal information to overseas recipients where:

- *the HSP to which the HSP Portal is licensed is a foreign entity (for example, domiciled in NZ or Malaysia), is a branch of a foreign entity, or which otherwise has a foreign activity (such as a processing centre) or presence (in which case, the recipients are likely to be in those relevant jurisdictions in which that entity is established or the activity operates); or*
- *that personal information is accessed by our Parent in providing us with technical, security and data validation support for personal information stored by us in order to provide our services, in which case the Parent is contractually obliged to access and handle any such information in accordance with the Australian Privacy Principles set out in the Privacy Act 1988 (Cth);*

(d) we may make your personal information available, including a document provided by you, to a relevant government authority or an issuing body (or, with your consent, to a designated person that can certify an identity declaration for the purposes of identity proofing), if we are not satisfied as to your claimed identity or the legitimacy of the identity documents supplied for purposes of an authorisation code application; and

(e) we and our related companies may, at any time, use and disclose your personal information to:

- *monitor traffic on our website;*
- *undertake data management for quality or operational purposes (and, where any such data contains sensitive information, that data will be de-identified to protect you, and this functionality is within your reasonable expectations);*
- *diagnose data collection issues (with any technical navigation information required for that purpose purged immediately after a problem (if any) has been remedied); and*
- *investigate any complaint made by you or on your behalf, either privately or by a relevant regulator or law enforcement agency.*

Our Privacy Policy also contains information about how we handle personal information and is available at www.equifax.com.au/hrsolutions/pdf/privacy.pdf.

We may also de-identify your data to develop and offer multi-data insights, reports and market benchmarking analyses to your employer and other third parties.

How we store, use and disclose your personal information

As outlined in the description of our use of your personal information, we may use or disclose your personal information:

(a) in creating and maintaining your Administrator account and related rights for purposes of the HSP Portal; and

(b) to other companies related to us, in particular those which provide services to us.

When your personal information is used for data analytics, it will always be de-identified.

Other than where personal information is shared with an off-shore third party as is reasonably necessary for one or more of the functions or activities covered by this Statement, we store, use and process your personal information in Australia on our secure information technology servers, including hosting through our Virtual Private Cloud using servers located in Australia under a managed services/SaaS model (where the vendor does not access or process Data).

GENERAL:

Privacy Policy, identity and contact details

Our Privacy Policy contains information about how you may access and seek correction of your personal information held by us, or make a privacy complaint, and how we will deal with such a complaint. Our Privacy Policy and contact details are available at: www.equifax.com.au/hrsolutions/pdf/privacy.pdf.

Interpretation

Terms defined by:

(a) our Terms of Supply (accessible at www.equifax.com.au/hrsolutions/pdf/terms-of-supply.pdf); or

(b) the eCredential™ SOW (accessible at www.equifax.com.au/hrsolutions/pdf/ecredentialsow.pdf),

*have the same meaning where used in this statement, unless the context otherwise requires. "**Parent**" means Equifax, Inc (NYSE: EFX), our ultimate parent company headquartered in Atlanta, Georgia, and any other related body corporate of Equifax, Inc located in the United States of America operating under the same Group policies as us, including under the EFX Global Security Policies, Standards and External Security Standards.*

This Collection Statement is governed by the law of New South Wales, and the parties submit to the non-exclusive jurisdiction of the courts of New South Wales and any courts hearing appeals therefrom.

SCHEDULE 1: GDPR COLLECTION NOTICE IN RESPECT OF eCREDENTIAL

*This Schedule applies only in respect of personal data that is subject to the General Data Protection Regulation (**GDPR**). By acknowledging and accepting the eCredential Privacy Collection Statement, you consent to your personal data being collected and processed for the specific purposes set out in, and in accordance with, the eCredential Privacy Collection Statement including (without limitation) this Schedule.*

*Your personal data is being collected and processed by Equifax Australasia Workforce Solutions Pty Ltd ABN 86 080 799 720 (**we**, **us** or **our**).*

We can be contacted by post at Equifax, PO BOX 964, North Sydney NSW 2059 or by phone on 138 332.

Manner and details of collection and source of personal data

Your personal data is collected directly from you by us for purpose of providing the eCredential service.

In addition, your personal data is collected by us from:

- *your HSP employer or an HSP that you have elected to provide a copy of your profile to from your Clinician Portal; and*
- *suppliers forming part of the support services for our eCredential service.*

We collect that information in connection with our suppliers' assistance in the provision of services for you and to provide services to either or both you and an actual or prospective HSP employer, respectively.

*The personal data that we collect about you consists of information as summarised in the eCredential Privacy Collection Statement under **What personal information do we collect?***

Processing activities and lawful basis

We process the personal data that we collect about you for the purposes and on the applicable lawful basis set out in the table below:

Purpose of processing	***Lawful basis***
To provide our services to you or to an HSP (as applicable).	*For our legitimate interests in being able to provide our services as requested.*
To enable our related entity to generate and provide you or an HSP with invoices related to our services.	*For our legitimate interests in being able to provide our services as requested.*
To provide information services to an HSP customer.	*Your consent (if given to us).*
To enable you to access and use our website.	*Your consent (if given to us).* *Performance of a contract with you.*
To operate, protect, improve and optimise our website and services business and our users' experience, such as to perform analytics, conduct research and for advertising and marketing.	*For our legitimate interests in operating our business efficiently and effectively.*

Purpose of processing	*Lawful basis*
To comply with our legal obligations, resolve any disputes that we may have with any of our users, and enforce our agreements with third parties.	*Compliance with our legal obligations.* *For our legitimate interests in enforcing our contractual and legal rights.*
To send you marketing and promotional messages and other information that may be of interest to you, including information sent by, or on behalf of, our business partners that we think you may find interesting.	*Your consent (if given to us).*
To provide a related company with personal data for the purposes of data-matching to support other product offerings, where those products do not disclose any of your personal data to a third party.	*Your consent (if given to us).*

We collect personal data about you in order to provide our services to you or to your actual or prospective HSP employer (as applicable). If you do not provide that personal data to us, we may not be able to provide our services or perform our services to the same standard.

Third party recipients

As part of processing your personal data, we may disclose personal data for the purposes described in this collection notice to:

- *our employees and to our related bodies corporate in Australia;*
- *third party suppliers, our related bodies corporate overseas and service providers (including suppliers and providers who assist us to operate our business or in connection with providing our products and services to you or your employer);*
- *payment systems operators (e.g. merchants receiving card payments); and*
- *our professional advisers, dealers, business partners and agents.*

we may hold and disclose your personal data outside of the European Union. In particular, our Australian companies may receive personal information that is originally collected by or disclosed to EU-located suppliers. Personal data transferred by such companies to our Australian entities will be undertaken where necessary with your consent under this Collection Notice.

Overseas recipients

In addition, we are likely to disclose your personal information to overseas recipients where:

- *you access your Clinician Portal from outside Australia;*
- *you choose to provide a copy of your profile to an HSP which is a foreign entity (for example, where the HSP is located in NZ or Malaysia), is a branch of a foreign entity, or which otherwise has a foreign activity (such as a processing centre) or presence (in which case, the recipients are likely to be in those relevant jurisdictions in which that entity is established or the activity operates); or*
- *that personal information is accessed by our Parent in providing us with technical, security and data validation support for Data stored on the Verification Exchange™, in which case the Parent is contractually obliged to access and handle any such information in accordance with the Australian Privacy Principles set out in the Privacy Act 1988 (Cth).*

Where:

(a) our eCredential services require disclosure of your personal data to persons located in another country outside the EU; and

(b) the EU Commission has not determined that such country has in place 'adequate' privacy protection laws for purposes of the GDPR,

you give us explicit consent to the proposed transfer, being aware that you may not be able to enforce your data subject rights or rely on effective legal remedies where such rights are not made available to you. The possible risks associated with the transfer due to a lack of such 'adequate' privacy protection laws in that country include identity theft, your loss of privacy, governmental misuse, inability to access your data subject rights, and a loss of due process and other legal protections.

Storage of personal data

We will store your personal data for so long as we continue to provide our services to you or to a HCP you have provided your data to (as applicable). After this time, we will continue to store your personal data to the extent required by any law applicable to our business or for compliance and risk management purposes. We will delete or de-identify your personal data when it is no longer necessary or required to be kept consistent with our Statement of Work (accessible at: www.equifax.com.au/hrsolutions/pdf/eCredentialworksow.pdf).

Your rights

Where we process any personal data about you based on a consent given by you, you have the right to withdraw your consent at any time by giving notice to us (which you can do using our contact details set out above). We will give effect to your withdrawal of consent promptly and will cease any processing that you no longer consent to, unless we have another lawful basis for that processing. The withdrawal of your consent will not affect the lawfulness of any processing that occurred prior to the date that you notified us that you were withdrawing your consent.

You have the right to request access to a copy of the personal data that we hold about you in the eCredential service and to request that we correct or rectify any inaccurate personal data that we hold about you, other than where that data is held on an HSP Portal. You also have a right to data portability, which is the right in certain circumstances to request a copy of your personal data in in a structured, commonly used and machine-readable format and to transmit this data to another data controller. You may also request that we erase any personal data that we hold about you which is no longer necessary for any of the purposes that we collected it for, which you have withdrawn your consent in respect of or processing which you are allowed under the GDPR to object to. We will comply with such requests unless we are permitted or required by law to retain that information. You also have the right to object to our processing of personal data in certain circumstances, including where we process personal data based on our legitimate interests. You can also request that we restrict our processing activities in some circumstances. If you make such a request in those circumstances, then we will continue to store your personal data but will not otherwise process your personal data without your consent or as otherwise permitted by law.

You have a right to lodge a complaint in respect of our processing of your personal data with the data protection supervisory authority in the member state of the European Union that you ordinarily reside or work in.

For more information on our processing of your personal data, please see our Privacy Policy, which is available at www.equifax.com.au/hrsolutions/pdf/privacy.pdf.