Privacy Notice & NHS Digital Smartcard / Authorised Device Terms & Conditions – GDPR compliant Version 2.0

Privacy Notice to Smartcard / Authorised Device users on the use of your personal data

These terms and conditions cover all access to the NHS Care Records Service applications

Definitions:

- NHS Smartcards means an approved physical card, supplied by the authorised supplier(s) of cards to NHS Digital, are similar-to chip and PIN bank cards and enable healthcare professionals to access clinical and personal information appropriate to their role. A smartcard used in conjunction with a passcode, known only to the smartcard holder, gives secure and auditable access to national and local Spine enabled health record systems
- Authorised Devices[1] means an alternative to smartcards, a device as approved by FIDO 2 Consortium that provides Assured Level 3 Authentication.

NHS Digital will collect personal data on you, some of which you provide in your application, and some of which is collected by cookies when you access NHS Care Records Service applications[2].

NHS Digital is the data controller for this data, under powers arising from Directions [3].

This data will be processed:

- by local and other Registration Authorities for the purposes of validating your identity, managing your Smartcard / Authorised Device and ensuring that you are given appropriate access to NHS Care Records Service applications, or applications that utilise the NHS Care Records Service authentication. Every organisation that has a Registration Authority (RA) that must adhere to the NHS RA Policy at all times[4].
- by NHS Digital to record your use of the NHS Care Records Service applications.
- in accordance with General Data Protection Regulation (GDPR) data protection law.
- for disclosure and auditing of access to systems as part of our commitment to patients within the Care Record Guarantee, such as to the Summary Care Record (SCR) https://digital.nhs.uk/services/summary-care-records-scr and in accordance with any complaint, investigation or as required by appropriate legislation.

Your data will:

- be held throughout your time as an active user and will be retained for up to 40 years after your Smartcard / Authorised Device user profile has been closed, at which point it will be subject to review.

- not be transferred out of the European Economic Area.
- not be used for any automated decision making.

The above details the personal data processed in relation to the NHS Digital Smartcard / other Authorised Device registration itself. For details of how other NHS Digital programmes use data (that you may access using your Smartcard / other Authorised Device) please see https://digital.nhs.uk.

Your rights

You have the right to access your data. As an active Smartcard / Authorised Device holder, you can view your data in My Profile within CIS. If you can no longer access CIS for any reason, please contact your local Registration Authority. Once you are no longer working in healthcare, you can make a subject access request to NHS Digital (see contact details below).

You have the right to rectify inaccuracies in your data. You should update your own contact details within My Profile in CIS. In case of difficulties, if your personal details have changed or you need to make other amendments please contact your local Registration Authority.

You have the right to complain (see the contact details below).

You do not have the right to erase your data, object to it being recorded, transport it elsewhere, withdraw consent to its capture or use, or restrict its processing. This is because the capture and processing of this data is necessary for a statutory requirement and the provision of the service. NHS Digital is also legally bound to record this data. Once you leave health and social care, your local Registration Authority will close your user profile. This may be reopened if you return to working within health and social care.

Contacts

For all operational enquiries, including Smartcard / other Authorised Device and access assignment, always contact your local Registration Authority.

See how NHS Digital looks after your information at https://digital.nhs.uk

To ask any question or make a complaint about how your data is used, you can contact NHS Digital on 0300 303 5678 (9am to 5pm Monday to Friday excluding bank holidays) or email enquiries@nhsdigital.nhs.uk

You can also write to:

Data Protection Officer
NHS Digital
1 Trevelyan Square
Boar Lane
Leeds
LS1 6AE

If you have concerns or complaints about NHS Digital's information right's practices, you can report them to the Information Commissioner's Office on 0303 123 1133 (9am to 5pm Monday to Friday excluding bank holidays) or use live chat at: https://ico.org.uk/concerns/

You can also write to:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

By clicking on the 'Accept Terms and Conditions' button at the bottom of this declaration, you the applicant confirm that you:

1. understand and accept that your personal data will be used as described in the "Notice to Smartcard / Authorised Device users on the use of your personal data" above. Furthermore, you agree to provide any additional information and documentation required by the Registration Authority to verify your identity. Each user must have their identity assured and verified to the relevant standard applicable at the time of registration[5]. This requirement may be refreshed from time to time;
2. confirm that the information which you provide in the process of your application is accurate. You agree to notify your local Registration Authority immediately of any changes to this information;
3. understand and accept that the Smartcard / Authorised Devices issued to you is the property of the NHS Digital, and you agree to use it only in the normal course of your employment or contract arrangement;
4. agree that you will check the operation of your Smartcard / Authorised Device promptly after you receive it. This will ensure that you have been granted the correct access profiles. You also agree to notify your local Registration Authority promptly if you become aware of any problem with your Smartcard / Authorised Device or your access profiles;
5. agree that you will keep your Smartcard / Authorised Device private and secure and that you will not permit anybody else to use it or to establish any session with the NHS Care Records Service applications. You will not share your Passcode with any other user. You will not write your Passcode down, nor use any kind of electronic storage (media or otherwise) to store it, for example by using a programmable function key on a keyboard. You will take all reasonable steps to ensure that you always leave your workstation secure when you are not using it by removing your Smartcard / locking your Authorised Device. If you lose your Smartcard / Authorised Device or if you suspect that it has been stolen or used by a third party, you will report this to your local Registration Authority as soon as possible;
6. agree that you will only access the NHS Care Records Service application by using a Smartcard or Authorised Device. You agree that you will only use your Smartcard / Authorised Device, the NHS Care Records Service applications

and all patient data in accordance with the NHS Confidentiality Code of Practice (www.dh.gov.uk) and (where applicable) in accordance with your contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to you;

7. agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate your Smartcard / Authorised Device, NHS Care Records Service applications components or any access profiles given to you;
8. agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes, but is not limited to, the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality;
9. understand and accept that your Smartcard / Authorised Device may be revoked, or your access profiles changed at any time without notice if you breach this Agreement; if you breach any guidance or instructions notified to you for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. You also understand and accept that if you breach this Agreement this may be brought to the attention of your employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);
10. understand and accept that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Smartcard / Authorised Device for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or applications which use NHS Care Records Service authentication or the accuracy of any patient data;
11. understand and accept that you, or your employer, shall notify your local Registration Authority at any time should either wish to terminate this Agreement and to have your Smartcard / Authorised Device revoked e.g. on cessation of your employment or contractual arrangement with health care organisations or other relevant change in your job role;
12. understand and accept that NHS Digital may unilaterally change the terms of this Agreement[6] from time to time, and unless otherwise stated these will be effective from publication; and
13. understand and accept that these terms and conditions form a binding Agreement between yourself and those organisations who have sponsored your role(s). You also understand and accept that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.

References:

1. These additional authentication methods must meet the National Institute of Systems and Technology (NIST SP800 – 63 Digital Identity Guidelines, available at https://pages.nist.gov/800-63-3/), this describes the cryptographic strength of authentication methods that is required to access sensitive data. In addition, devices and authentication methods need to meet FIDO 2 standards for how devices utilise the required cryptography (available at https://fidoalliance.org/) and must be accredited by the FIDO alliance.

2. NHS Care Records Service applications includes the following: EPS, GP to GP, GPES, GPSoC, NHS e-RS, SCR, SUS+, Spine CIS, Spine NHS Identity. See https://digital.nhs.uk/services/

3. Directions mean “the Health and Social Care Information Centre (Spine Services) (No.2) Directions 2014”, and the “Novation of Information and Technology Contracts from DH to NHS Digital: “Electronic Prescription Service, Health and Social Care Network, N3, NHS Choices, NHS e-Referral Service, Secondary Uses Service (SUS), Spine (Named Programmes) Directions 2016”. These can be found at: https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/spine-services-no-2-2014-direction

4. The current National Registration Authority RA Policy can be found at: https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities The NRA RA Policy is subject to revision from time to time.

5. Good Practice Guide GPG45 (or recognised successor) on the identity proofing and verification of an individual to a minimum of Level 3. See Government publication at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

6. The Smartcard Terms and Conditions can be found at: https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities.