NHS Smartcard
Terms and Conditions

NHS Smartcards 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.

You must read and accept the terms and conditions related to the use of your personal Smartcard.
You will be asked to sign to confirm upon collection of your Smartcard from the RA (Registered Authority) Team:

1. You understand and accept that your personal data will be used by us as described in the privacy notice for users of NHS Identity and CIS https://digital.nhs.uk/services/registration-authorities-and-smartcards/privacy-notice-to-smartcard-authorised-device-users-on-the-use-of-your-personal-data. Each user must have their identity assured and verified to the relevant standard applicable at the time of registration. This is currently 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 This requirement may be refreshed from time to time.

2. You 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. You understand and accept that the Authentication Token, (with the exception of personal devices) issued to you is the property of / licensed to the health and social care bodies providing it to you, and you agree to use it only in the normal course of your employment or contract arrangement.

4. You agree that you will check the operation of your Authentication Token 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 Authentication Token or your access profiles.

5. You understand that the suppliers of some Virtual Smartcards, Authorised Devices, and iPad Devices may process personal data about you as an independent Controller, and may have applicable privacy policies and terms and conditions. You will be presented with these as part of download/registration and are responsible for reviewing and abiding by these.

6. You agree that you will keep your Authentication Token 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 physical Smartcard, ensuring your virtual Smartcard has disconnected or locking your Authorised Device or iPad Device. If you lose your Smartcard, Authorised Device or iPad Device or if you suspect that your Authentication Token has been stolen or used by a third party, you will report this to your local Registration Authority as soon as possible.

7. You agree that you will only access the NHS Care Records Service application by using an Authentication Token approved by NHS Digital. You agree that your use of the Authentication Token, the NHS Care Records Service applications and all patient data shall be 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.

8. You agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate your Authentication Token, NHS Care Records Service applications components or any access profiles given to you.

9. You 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.

10. You acknowledge that your access may be audited. You understand and accept that your Authentication Token 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).

11. You understand and accept that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Authentication Token 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.

12. You 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 Authentication Token revoked e.g. on cessation of your employment or contractual arrangement with health care organisations or other relevant change in your job role.

13. You understand and accept that we may unilaterally change these terms and conditions from time to time, and unless otherwise stated these will be effective from publication. The latest version of these terms and conditions will be accessible at https://digital.nhs.uk/services/registration-authorities-and-smartcards/privacy-notice-to-smartcard-authorised-device-users-on-the-use-of-your-personal-data and in your NHS Identity / CIS account. We will inform you through your NHS Identity / CIS

account if we make any material changes to these terms and conditions, and will also send an email notification to all RA managers.

14. You understand and accept that these terms and conditions form a binding Agreement between yourself and all Registration Authorities who provide Registration Authority services to you. Non-compliance may also be treated as a disciplinary matter by your employer.

15. You 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 information. 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.

NHS
East Kent Hospitals University
NHS Foundation Trust