Welcome to the NHSmail GDPR webinar

- The webinar will begin at 11am.
- Please synchronise your web and phone presence by inputting your **Attendee ID** into the phone.
- Participant lines will be muted during the presentation.
- The webinar will be recorded and published.
- You can use the chat messaging feature on the right of the screen to ask questions. Please only use this for questions, not general comments.
- Questions will be taken at the end of the session once the information has been delivered.

NHSmail GDPR webinar

Thursday 17 May 2018 at 11am

Agenda

- What is GDPR?
- What is NHSmail doing to comply with GDPR in England?

  The content of this webinar focuses on NHS Digital as the NHSmail Live Service Joint Controller. There will be some minor differences to users in Scotland, specifically in terms of points of contact and some of the data that is captured. National Services Scotland will be publishing their own guidance on the Portal help pages.
- Joint Controller arrangements
- Subject Access Requests (SARs)
- Communications and information you may find useful
- Next steps
- Questions

What is GDPR?

Emma Summers
NHSmail Product Owner

What is GDPR?

- General Data Protection Regulation (GDPR):

  "legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU)."

- Comes into force on 25 May 2018.
- Guidance on compliance is available via the Information Commissioner Office (ICO).
- 6 principles outline an organisation's responsibilities in relation to personal data.

GDPR terminology

Term	Description
Controller	Determines the purposes and means of processing personal data. Sometimes there are Joint Controllers as the responsibility is shared across multiple organisations.
Processor	Responsible for processing personal data on behalf of a Controller.
Data Subject	The identified or identifiable natural person to whom the data relates.
Data Protection Officer	Responsible for informing and advising on GDPR obligations; monitoring compliance with GDPR.
Transparency Information / Fair Processing Notice	Detailing how personal data is managed by the NHSmail Live Service.
Data Protection Impact Assessment (DPIA)	Documented process used to identify and minimise the data protection risks of the intended processing. Mandatory for high risk processing.

What is NHSmail doing to comply with GDPR in England?

Roles and responsibilities

Name	Role	Responsibility
NHSmail Live Service (NHS Digital)	Joint Controllers	Complying with GDPR. Demonstrating compliance with GDPR. GDPR compliance Controller checklist. Managing the contract with the Processor, Accenture
Organisations using NHSmail	Joint Controllers	Complying with GDPR. Demonstrating compliance with GDPR. GDPR compliance Controller checklist.
Accenture	Processor (process administration of accounts on behalf of Controller under their instruction)	Contracted to process NHSmail global and local administration level requests from the Controller on behalf of its users as part of its managed service responsibilities.

Data Protection Impact Assessment (DPIA)

The DPIA provides evidence to support NHS Digital's compliance with the data protection principles.

- Detailed information about data processing in relation to data flows, legal basis and what is captured and when.
- Data standards and quality of data.
- Individual rights and process for complaints.
- Where data is processed.
- Next steps for DPIA maintenance and improvement.

Transparency Information / Fair Processing

Local organisations that use NHSmail will NEED their own Transparency Information / Fair Processing Notice covering how personal data is managed at a local level. The NHSmail Live Service and local organisation Transparency Information / Fair Processing Notices should be read in conjunction with each other to understand the differing responsibilities. NHSmail Live Service Transparency Information includes:

- Who we (NHS Digital / NHSmail Live Service) are
- Our Data Protection Officer
- What information we collect about you
- The legal basis for using your personal data
- How we use your personal data
- Sharing your personal data
- Where your data is stored and processed
- How long we hold onto your personal data
- Your rights
- Where we get your information from

Transparency Information - content

Who we (NHS Digital / NHSmail Live Service) are:

- NHS Digital was set up by the Department of Health in April 2013.
- An executive non-departmental public body that provides national information, data and IT systems for health and care services.
- NHSmail Live Service is provided by NHS Digital under direction from the Secretary of State.
- Acts as the Joint Controller for NHSmail to manage the contract (on behalf of all Controllers) with Accenture (Processor) to run and maintain the NHSmail Live Service.
- Further information and contact details are available within the NHS Digital website.

Our Data Protection Officer:

- Responsible for assisting NHS Digital to monitor its compliance with Data Protection legislation and its own policies in relation to the protection of personal data.
- Can be contacted via nhsdigital.dpo@nhs.net.

Transparency Information - content

What information we collect about you

- Name, work address / postcode, date of birth, professional qualifications, email address, personal / work mobile number.
- Reason for collecting the data varies depending on your use of the service - account setup, data authentication prior to account provision, contact details in the NHS Directory, helpdesk quality assurance.

The legal basis for using your personal data

- NHS Digital has a legal obligation (a Direction issued by the Secretary of State for Health) that requires us to establish and operate informatics systems and to exercise systems delivery functions, including NHSmail as the national secure email service approved for sharing sensitive information. The Direction is available on the NHS Digital website.

How we use your personal data

- Personal data processing falls into two main categories:
  - Data processing that is used to run and maintain the NHSmail Live Service.
  - Data processing that takes place by local organisations using the NHSmail Live Service to securely send and receive sensitive or official data (including patient identifiable data) to support publicly funded healthcare.
- Other organisations, that have entered into a partnership agreement with NHS Digital to share calendar data where there is a business need, may also process NHSmail Live Service data.

Sharing your personal data

- **Your personal NHS Directory data and email data will be shared with:**
  - NHS and health and social care staff using NHSmail.
  - Organisations that have entered into a partnership agreement with the NHSmail Live Service.
  - The Processor (service supplier, Accenture) and approved (by NHS Digital) sub-contractors (Processors) for the purposes of supporting the NHSmail Live Service. Full details of sub-contractors are available via feedback@nhs.net.
  - NHS Directory information is available to anyone with an N3 / HSCN connection, since its purpose is to improve communication (except mobile numbers that have been hidden by the owner).
- **Your personal NHS authentication data will be shared with:**
  - NHSmail Live Service (NHS Digital) who oversee the NHSmail registration process.
  - The service supplier, Accenture, and other sub-contractors for the purpose of supporting the NHSmail Live Service.
- **Your personal email data will be shared with:**
  - Other contacts or organisations that you are permitted to email according to local organisation (Joint Controller) policies and procedures.

Transparency Information - content

Where your data is stored and processed

- **Personal data controlled by the NHSmail Live Service:**
  - Data controlled by the NHSmail Live Service is stored and processed within the United Kingdom.
  - Access and administration of the data can take place both within and outside the United Kingdom.
  - Access outside the United Kingdom is governed through the use of EU Model Clauses in the relevant contracts.
  - For some local organisations choosing to use the migration options provided by Accenture, data processing will be carried out outside of the EU. Further details are available via feedback@nhs.net.

- **Personal data exchanged via the NHSmail Live Service:**
  - Data exchange by individuals using NHSmail can take place between anyone in any location but should be in accordance with local governance and information management policies, to ensure personal or sensitive data is protected and health data is used in accordance with the duty of confidentiality.

How long we hold onto your personal data

- **Personal NHS Directory data:**
  - This information is kept indefinitely until contact details are deleted within the NHS Directory by the organisation employing the staff member.
- **Personal authentication data:**
  - This information is kept indefinitely for the lifetime of the NHSmail account.
- **Personal email data:**
  - Kept indefinitely until deleted by the individual. Central copies of email sent / received are retained for 180 days for forensic audit purposes. Message summaries (when and who an email is sent to / from) are kept for two years.

The NHSmail Data Retention Policy sets out the detailed data storage periods for the service.

Your rights

- Right to be informed - *Transparency Information.*
- Request a copy of your personal data - *Subject Access Request.*
- Correct your personal data errors or omissions (right to rectification) – *contact your Local Administrator.*
- Request us to restrict our use of your personal data – *contact your Local Administrator.*
- To be told whether there is a statutory or contractual need for your data and the possible consequences of not providing it – *if data is not captured as part of the registration process NHSmail cannot be used.*

Objections and complaints

- If you have a complaint about the way your personal data has been handled; believe it is inaccurate, held for too long or it is not secure you can contact the relevant Data Protection Officer (DPO) who will investigate the matter.
  - **Personal data controlled by the NHSmail Live Service:**
    Contact the Data Protection Officer at nhsdigital.dpo@nhs.net.
  - **Personal data exchanged via the NHSmail Live Service:**
    Contact your organisation's Data Protection Officer.

- If you are not satisfied with the response or believe your data is not being processed in accordance with the law, you can complain to the Information Commissioner's Office (ICO).

- The ICO is the regulator for Data Protection and upholds information rights. More information is available on the ICO website https://ico.org.uk/.

Joint Controller arrangements

Melanie James
Business and Operational Delivery Manager - NHSmail

Joint Controller arrangements

A document outlining the responsibilities of the Joint Controllers in respect to:

- data processing that is used to run and maintain the NHSmail Live Service in England
- data processing that takes place at local organisations using NHSmail to securely send and receive sensitive data (including patient identifiable data) in England

Going through final creation and will be cascaded via the IBC team to CIOs/CEOs and Primary Local Administrators in due course.

Summary of Joint Controller responsibilities

- Acting in accordance with the Data Protection Act 2018 which, will be enacted on 25 May 2018 and, supersedes all previous Data Protection Act legislation. General Data Protection Regulation (GDPR) guidance on compliance is available on the Information Commissioner's Office website.
- Acting as the joint controller to manage the NHSmail service.
- Processing data, for varying lengths of time, in line with NHSmail policy and process documentation including:
  - Access to Data policy
  - Data Retention policy
  - Information Management policy
- Working together to facilitate and process Subject Access Requests/Forensic Investigations
- Ensure those processing data are subject to a duty of confidence
- Ensuring data processing is carried out as per the details within the DPIA and the Transparency information

Summary of Local organisation Controller responsibilities

Informing your NHSmail users about how their personal data is managed via your organisation Transparency Information. The content of the Transparency Information must meet the guidelines stipulated by Information Commissioner's Office.

Owning and managing data that:

- controls the use of NHSmail accounts including content within the NHS Directory
- is exchanged via NHSmail by their users
- is provided as part of Subject Access Requests (SARs) to ensure inappropriate data is redacted prior to sharing with the SAR requestor. Clinical data will require clinician oversight / non-sensitive data will require senior Information Governance oversight.

Examples of the types of data to be managed can be seen in the DPIA.

Establishing local policies and procedures to:

- govern the use of the NHSmail service locally. This may entail the use of third-parties.
- review and maintain contacts within the NHS Directory and remove any that are no longer current.
- support requests for hiding an individual from the NHS Directory that will require permission from the owner or HR director to be forwarded to the NHSmail Live Service Operations Team (NHS Digital) via feedback@nhs.net before the NHSmail helpdesk (Accenture) can action. Urgent requests can be processed by logging the information with the NHSmail Operations Team while raising a service request in parallel.
- enable local staff to report NHSmail data breaches internally and to the Information Commissioner's Office (ICO) where necessary.
- enable individuals to exercise their rights based on the legal basis for processing
- managing data when a user leaves and archiving it locally (not using NHSmail as a document repository)

Summary of Local organisation Controller responsibilities

- Facilitating Subject Access Requests (SARs) and Forensic investigations
  - Authorising and authenticating request prior to sending to NHS Digital for processing
  - when completing Subject Access Requests (SARs) and sharing data with the requestor, a copy of the organisation's Transparency Information must also be included to conform with GDPR legislation.
- Agreeing to the content within the arrangements document and the transparency information published by the NHSmail Live Service in order to consume NHSmail. If any of the terms and conditions are not met, an organisation may be asked to leave the service.
- Managing NHSmail accounts in accordance with the expectations outlined by the NHSmail Live Service team e.g. having a Primary LA, making sure users have security questions/answers set and have accepted the AUP etc., familiarising themselves with the Portal help page, cascading communications to user.

Full details will be published in the arrangements document.

Summary of NHS Digital Controller responsibilities

- Reflecting the local organisation responsibilities in light of the NHSmail Live Service data controlled by NHS Digital.
- Responsible for managing the contract with Accenture, Processor, and the approval of their sub-contractors.
- Processing the data outlined within the Transparency Information and the DPIA when:
  - under instruction from other controllers unless required by law to act without instruction
  - Under instruction from organisations that have federated/partnered with NHSmail

  in accordance with the Data Retention Policy, Access to Data Policy, Information Management policy and other NHSmail policies and processes.
- NHS Digital may process the data request directly or pass it to the processor, Accenture, for completion. These requests may include Subject Access Requests (SARs) and/or Forensic investigations.
- Maintaining regular update on the NHS Directory via the ODS team.

Subject Access Requests (SARs)

Subject Access Request (SAR) process

- Process being finalised and will be published on the Portal help pages in due course.
- Individuals can request copies of data relating to themselves called a Subject Access Request (SAR).
- This is different to a Forensic Investigation Request.
- Due to difficulty in authentication, the SAR process requires the individual to make their request via their organisation's Local Administrator (LA), by completing a form outlining the data required.
- The LA will need to check the request and ensure it complies with local processing guidelines and send the completed form to feedback@nhs.net or nhsmail.scotland@nhs.net.
- The request will be sent to Accenture for processing.
- Data will be returned to the requesting organisation that made the SAR and they will need to ensure any data that is not related to the SAR is redacted, prior to sharing – please think about who this should be within your organisation i.e. clinician for clinical data.
  - Timeframe for completion of SAR process is 30 days (includes redaction).
  - If scale of request cannot be completed in the timeframe, Accenture may request the scope of data is reduced.

SAR – details required to proceed

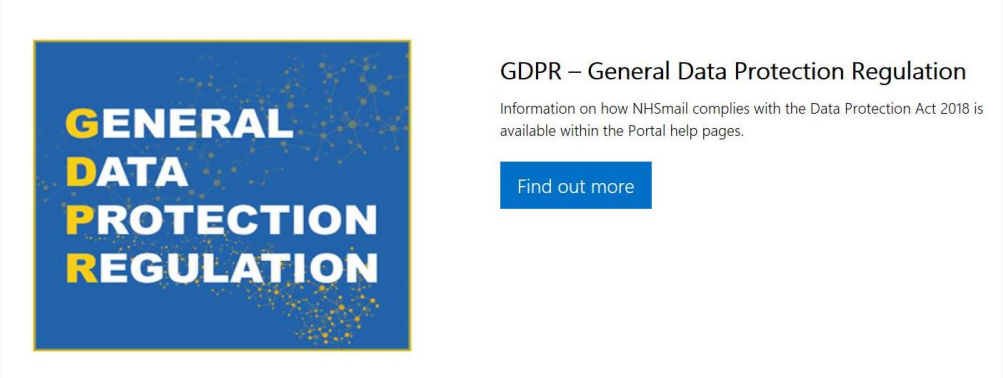
- Ensure any details supplied match existing NHSmail Live Service datasets for authentication purposes.
- The datasets that you wish to access, including details of:
  - Name of subject (surname, first name, former surname if applicable).
  - Contact details (phone number, email address).
  - Email address of subject access request i.e. mailbox names.
  - Date range i.e. start and end time.
  - Defined data fields required i.e. subject line, mailbox names.
  - Any further data minimisation information i.e. exclusions, details of other data subjects that may be linked to the SAR.
  - The reason for requesting the data i.e. any dependencies on court cases, disciplinary hearings.
  - The Joint Controller (organisation) of the data you are requesting i.e. organisation name that hosts the relevant NHSmail accounts.
- Confirmation of the person within the organisation that will be responsible for redacting any data that is not relevant to the SAR.
- Organisation details of those that will be responsible for redacting the supplied data and the location where this processing will happen.
- The location of where the data will be stored or shared, whilst redaction takes place.
- Any further evidence to support your application e.g. copies of consent letters.
- How long you intend to retain the data for.
- Confirmation of executive powers if you are acting on behalf of others.

Whilst the SAR process is being finalised continue sending Forensic investigations through to feedback@nhs.net in the usual way.

Communications and information you may find useful

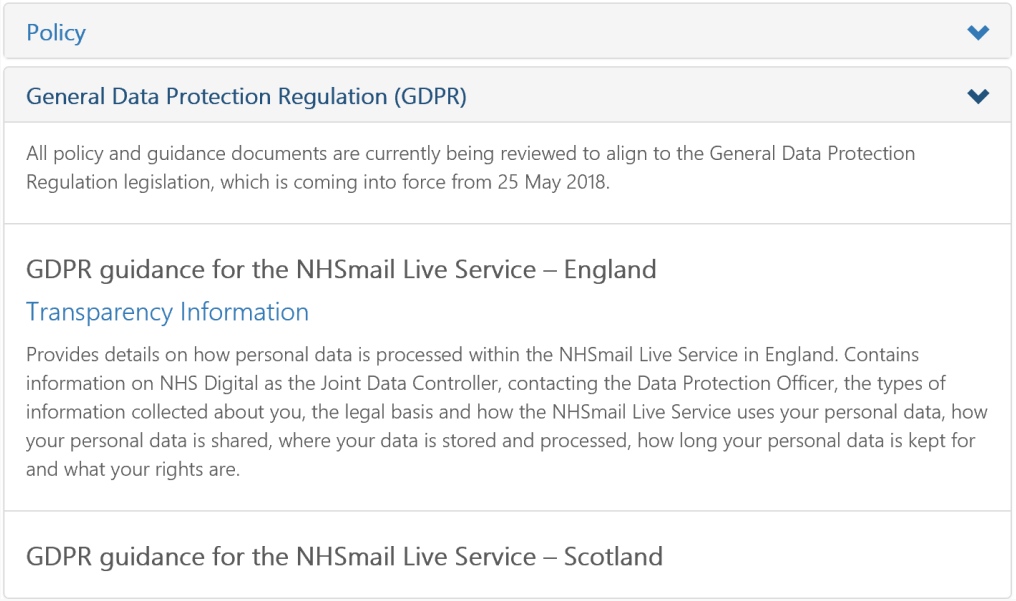
Communications activity

- Carousel on the Portal homepage - ‘Find out more’ button directing users to the new section on GDPR within the Portal help pages.
- Privacy Information (GDPR) link next to Acceptable Use Policy.



Communications activity

- Portal help pages have a new GDPR section that contains the core supporting documentation produced to inform users of what happens to their data



Communications activity

- Two webinars for Local Administrators (today / 23 May).
- Broadcast user communications scheduled w/c 21 May.
- FAQs to be published on the GDPR Portal help pages.
- NHS Digital website provides additional GDPR information.

Where to find information

Query	Document
Where can I find the GDPR Transparency Information for the NHSmail Live Service?	The Transparency Information is available via the Portal at www.nhs.net.
What are my rights under GDPR with respect to NHSmail? How does NHSmail protect my personal data? How can I have my personal data removed from NHSmail? How can I get information NHSmail hold about me corrected? Who is the Data Protection Officer? What information does NHSmail collect about me? How does NHSmail use my personal data? Who do NHSmail share my personal data with? How long does NHSmail hold my personal data? Where is my personal data held by NHSmail (e.g. what locations)? What is the legal basis for collecting my personal data? How can I raise a concern with regards how my personal data is being handled by NHSmail?	See the Transparency Information / Fair Processing Notice.

Where to find information

Query	Document / Response
How do I find out what certifications the NHSmail supplier holds?	See the NHSmail Portal help pages within the 'Policy' section.
Where can I find more information about GDPR?	ICO website - https://ico.org.uk/.
Can I opt-out?	Not applicable as NHS opt-out refers to patients only and the processing carried out by NHSmail does not relate to the use of patient data for secondary purposes.
How do I report a personal data or privacy breach?	This will need to be reported according to your local organisation Information Governance policies and processes. In the first instance, you should contact your Caldicott Guardian.
How do I make a Subject Access Request?	The process is still being finalised and will be published on the NHSmail Portal help pages as soon as it is available.

Above questions have been turned into a FAQ document which will be published within the GDPR section of the Portal help pages.

Other documents being reviewed

- Acceptable Use Policy
- Data Retention Policy
- Access to Data Policy and process
- Information Management Policy
- Forensic Investigations process
- Subject Access Requests process - new

Next steps

Next steps

Action	Date
Ongoing review and uplift of existing NHSmail policy and process documents	Now
Uplift DPIA and Transparency Information in light of legislation going live	Early June 2018
Receive feedback from NHSmail users and wider stakeholders to consider refinement or areas for clarification	July 2018
Review and uplift DPIA and Transparency Information prior to Microsoft O365 Hybrid implementation	September 2018
Annual review of DPIA and Transparency Information	April 2019
Annual review of DPIA and Transparency Information	April 2020
Contract closure and handover activity	January 2021

If you have any specific queries or would like to provide feedback on anything that isn't clear within the documentation published, or the contents presented today, please email feedback@nhs.net.

Questions?

NHS Digital

www.digital.nhs.uk

@nhsdigital

enquiries@nhsdigital.nhs.uk

0300 303 5678

Information and technology
for better health and care