Data Protection Impact Assessment

eConsult Online Consultations for Primary Care

Template Version number: 5a

Prepared by: Corporate Information Governance

Classification: OFFICIAL

Data Protection Impact Assessment
eConsult Online Consultations for Primary Care

Administrative information

NHS England	
Your name	Jon Shingleton
Your team and directorate	Senior Lead – IG Assurance and Planning Corporate Information Governance
Your location	Quarry House, Leeds
Your telephone number	
Your email address	england.igpolicyteam@nhs.net

Purposes

Fully describe what is the purpose of the project and how is the processing of information necessary to that work?	**Online consultations provide opportunities for patients to engage with the NHS remotely, in some cases through automated clinical algorithms that reduce the need for contact with clinicians, thus reducing burden on clinical staff and enabling patients to seek real-time clinical support.** **NHSX and NHS England have been promoting the use of online consultation solutions across the health service, particularly in primary care settings. Efforts to widen uptake of virtual alternatives to face to face appointments have been accelerated considering Covid-19.** **eConsult is one such solution that has already been commissioned independently in a number of GPs across the country, although there are inconsistencies in the contracts, agreements and data protection impact assessments in place between the supplier and different NHS customers. To ensure provision of a consistent approach across the NHS, NHS England will undertake a national DPIA and establish a comprehensive contractual solution with the supplier on behalf of and in conjunction with GPs.** **It is important to note that these arrangements have been made to facilitate rollout of the eConsult solution at pace, while ensuring the provision of robust information governance controls. These will be reviewed in six months' time and do not constitute a change in precedent as to the provision of IT systems on behalf of the NHS.** **Background:** eConsult is widely used across primary care providers already, and NHS Digital have been piloting its integration into the NHS App. eConsult provides a text-based clinical consultation service which guides patients through a consultation algorithm to assess their symptoms and recommend appropriate next steps, which may include arranging a GP appointment, self-care advice or signposting to other services (e.g. NHS111, pharmacies etc.). It does not facilitate real-time consultations between patients and GPs

	but does make GPs aware of all assessments undertaken on their patients. The solution is provided by the UK-based eConsult Health Limited. Where GPs require their patients to access the service via the NHS App, the integration will be provided by NHS Digital. For the purposes of data protection in relation to the provision of online consultations to patients, eConsult Health Limited and NHS Digital are data processors on behalf of NHS England and the primary care provider, who are joint controllers. NHS England will enter into and maintain a Data Processing Agreement with eConsult. Copies of the following agreements are attached: • Data Processing Agreement between NHS England and eConsult • Joint Data Controller Agreement between NHS England and the primary care providers • Data Connection Agreement between eConsult and NHS Digital (to enable integration with NHS Login and NHS App) • Data Processing Agreement between NHS England and NHS Digital  eConsult Joint Data Controller Agreement  eConsult Data Processing Agreemen  NHS Digital Data Processing Agreemen  eConsult connection agreement FINAL_sigr For context, several additional processing activities are described in this DPIA that have touch points with the eConsult service, such as: • NHS Login, provided by NHS Digital, to verify patient identity • Account management of the NHS App • Auditing of the NHS App's effectiveness and stability • Continuous improvement of the NHS App These processing activities have already been extensively documented and previously received IG approval, thus are outside scope of this DPIA.

Nature of the data

Will the processing involve anonymised information[1]?	No
Will the processing involve pseudonymised personal data?	No
Will the processing involve fully identifiable personal data?	Yes

Assets

Does the proposal involve creating a new information asset?	Yes, NHS England will register the eConsult solution as a national information asset and primary care providers using the solution will also log the solution on local asset registers.
Does the proposal involve processing data held on an existing information asset or assets?	No
Is/are the asset owner(s) aware of the proposal	Yes, within NHS England. Primary care providers will be informed through dedicated communications.

What is the timeframe for the project/programme/initiative?

Imminent rollout as an ongoing solution, with IG arrangements to be formally reviewed after 6 months.

Controllers[2]

NHS England	Yes, jointly with primary care providers. NHS England it determines the means of the processing.
TDA	No
Monitor	No
NHS Digital	No
Other (Please do not include any third party that we are contracting with to	Primary care providers using the solution, jointly with NHS England.

[1] anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

[2] 'controller' means NHSE, alone or jointly with others, determines the purposes and means of the processing of personal data

process personal data for us as a processor.)	Primary care providers determine the purpose of the processing.

Screening questions

Does the proposal involve any of the following – drop down list to include: • NCDR • Pseudonymised by NHS Digital • Aggregate data • Anonymised data	No
Has processing of this nature already been captured and considered within a previous DPIA? If so, link to reference number	Yes, online consultation solutions in general have been assessed within the NHS App DPIA, attached. This was approved by NHS Digital.  NHS App Data Protection Impact As eConsult have also undertaken their own DPIAs to demonstrate the platform's integration with NHS Login and Docman. These were approved internally within eConsult.  DPIA - NHS Login integration.pdf  DPIA - Docman integration.pdf
Will the processing involve a large amount of personal data (including pseudonymised personal data) and affect a large number of data subjects?	Yes
Will the project involve the use of a new technology(ies) which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition, Artificial Intelligence or tracking (such as tracking an individual's geolocation or behaviour)?	No
Will the processing introduce or make use of a new platform not currently in use?	Yes
In the absence of proper controls is there the risk that the processing may give rise to discrimination, identity theft	Yes

or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?	
Does the proposal introduce difficulties in ensuring that individuals are informed or able to exercise their information rights?	No
Will there be processing of genetic data, data concerning health, sex life, racial or ethnic origin, biometric data, political opinions, religion or philosophical beliefs, or trade union membership?	Yes
Will there be processing of data concerning criminal convictions and offences or related security measures?	No
Will the project involve the targeting of children or other vulnerable individuals for marketing purposes, profiling or other automated decision making?	No
Will the processing result in you making decisions or taking actions against individuals in ways which can have a significant impact on them? e.g. decisions about an individual's access to a product, service, opportunity or benefit, or recruitment aptitude test based on automated decision making (including profiling)?	Yes
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	No
Will the processing include any data matching e.g. the combining, comparing or linking of personal data obtained from multiple sources?	Yes, when verifying patient ID, information provided by the data subject will be matched with the NHS number via NHS Login and other information provided by GP systems. This is described in the NHS Login DPIA.
Will personal data about individuals be shared with other organisations or people who have not previously had routine access to the data?	Yes

Will the project/proposal use personal data about individuals for a purpose it is not currently used for or in a new way?	No
Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	No
Are you using a Data Processor/third party supplier or is a service/processing activity being transferred to a new supplier/organisation (or re-contracted) at the end of an existing contract?	Yes

NB. If the answer to any of the above questions is Y, please complete the rest of the form. If all of the screening questions are answered N, the local IG team must still sign off the DPIA.

Where the information will include the processing of personal data, please continue.

Personal data[3]

Why would it not be possible to do without personal data?	Online consultations require patients to provide personal data for the purpose of identifying them and diagnosing their symptoms.
What are the required personal data? Please itemise them or supply a dummy sample, blank forms, screenshots from the prototype system etc.	• NHS Number • Name • Address • Date of Birth • Sex • Session ID • Data concerning health (symptoms, conditions etc.)
Please confirm that this is the minimum amount of personal data that is necessary.	This is the minimum data required to confirm the identity of the patient and undertake their consultation.
Would it be possible for NHSE to use pseudonymised personal data for any element of the processing?	NHS England will not receive personal data associated with this processing. For primary care providers, pseudonymising the personal data would render it unusable for the purposes described above.
If Y, please specify the element(s) and describe the pseudonymisation technique(s) that we are proposing to use.	Not applicable.

Scale and constituency(ies)

What is the scale of the processing (i.e. (approximately) how many people will be the subject of the processing)?	Within a primary care provider, the online consultation solution could span the entirety of the practice list, which varies significantly by provider. Nationally, the scope will span the practice lists of all primary care providers using the solution under these arrangements.
Please describe the constituency(ies).	Patients.

[3] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Outcomes

What will be the effects of the processing (i.e. what actions/decisions will result from the processing)?	The processing will determine appropriate courses of action for the patient in managing their symptoms, which could include seeking a GP appointment, undertaking self-care or accessing other NHS services (e.g. NHS111, pharmacies). It is important to note that the patient will not be obliged by the advice provided by the online consultation solution and will be free to request a GP appointment at any time.

Purpose(s) and legal basis(es) of the processing

Is the processing necessary for a task that is within the organisations' remit as public authorities?
Yes **NHS England and Primary Care Providers:** GDPR Article 6(1)(e), which permits us to process personal information that is necessary to provide a service which is in the public interest.

Is NHSE under a legal obligation to carry out the processing?
No

Is the processing necessary for the arrangement or fulfilment of a contract between NHSE and the subject(s) of the personal data?
No

Will we be seeking, and recording, freely given, specific and informed consent[4] to the processing? If so, please supply a copy of the draft consent form.
No

Is the processing necessary in an emergency situation to protect the life or safety of any person? (NB This basis should be used only where the processing cannot be based on another legal basis.)
No

[4] 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her – this must be demonstrable by NHSE

Is the processing necessary in the legitimate interests of NHSE or a third party?
No

Special categories of personal data

Will the processing involve personal data about:	
• racial or ethnic origin	No
• political opinions	No
• religious or philosophical beliefs	No
• trade union membership	No
• genetic data[5]	No
• biometric data[6]	No
• data concerning health[7]	Yes
• data concerning the sex life or sexual orientation of the data subjects	Yes

Legal basis(es) for special category personal data

Legal basis	Personal data to which this legal basis relates: Data concerning health transmitted as part of the online consultation process.
• explicit consent	No
• required in the field of employment, social security or social protection law	No
• necessary in an emergency situation to protect the life or	No

[5] 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

[6] 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

[7] 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

safety of any person where the data subject cannot consent	
• data subject has put the personal data in the public domain	No
• necessary for legal claims or to the Courts	No
• necessary for reasons of substantial public interest	No
• necessary for health or social care purposes (please specify below)	Yes **NHS England and Primary Care Providers:** GDPR Article 9(2)(h), which permits us to process personal information to provide and manage a health care system.
• necessary for public health	No
• necessary for archiving in the public interest, scientific or historical research purposes or statistical purposes	No

Common law duty of confidentiality

Are any of the data subject to a duty of confidentiality (e.g. clinical records, OH details, payroll information)? If so, please specify them.	Yes
Where it is planned to disclose such data, what are the grounds for doing so?	The disclosure of confidential data directly from patients is required for the provision of their direct care, therefore implied consent provides grounds for meeting GPs duty of confidence. No personal data is shared with NHS England.
If the processing is of data concerning health or social care, is it for a purpose other than direct care[8]?	No

[8] direct care: a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

Consultation

Would it be appropriate to seek the views of data subjects or their representatives on the proposed processing?	Yes
If Y, how will this be done?	A cohort of patients were invited to consult on the eConsult and NHS App solutions before they went live.
If N, why is this the case?	Not applicable
Would it be helpful to seek advice from independent experts (clinicians, security experts, ethicists etc.) where their specialist knowledge would be useful in understanding and managing privacy risks?	Yes
If Y, how will this be done?	Opinions have been sought from digital and IG specialists in NHSX, NHS England and NHS Digital
Will any other stakeholder(s) (whether internal or external) need to be consulted about the proposed processing (e.g. NHSE Central team, Public Health England, NHS Digital, the Office for National Statistics)?	No
What was/were the outcomes(s) of such consultation?	The solution has deemed to be secure from a data protection and information security perspective.

Datasets and access

Purpose / process	**Required data items**	**Accessed by (Roles)**	**Storage location**
Verifying patient identity (via NHS Login)	• Verifying patient ID is undertaken via NHS Login, which has been subject to IG scrutiny separately and has received approval		
Provision of online consultation service	• NHS Number • Name • Address • Date of Birth • Sex • Session ID • Data concerning health (symptoms, conditions etc.)	• Primary care provider • eConsult • Docman • NHS Digital	• UK • Some data may be transferred via EEA servers during transit through the NHS App,

			though it is not stored offshore

Data processor[9]

Will the processing be wholly or partly performed on our behalf by a data processor(s)?	Yes
If Y please give details	eConsult will be the primary data processor providing the online consultation service. NHS Digital will be an additional processor for providers using the eConsult solution via the NHS App.
Where is the data to be processed by the data processor?	eConsult store and process all data in the UK for providing online consultation services and audit and improvements. During transit through the NHS App, NHS Digital may process some personal data via EEA servers, though it is not stored offshore. Organisation-wide agreements between NHS Digital and their sub-processor (Akamai) are in place with full organisational and technical controls. Contractual arrangements between NHS Digital and Akamai will be reviewed in accordance with the review date of the eConsult arrangements.

If the processing is not completed by a data processor, please ignore the following questions and proceed to the 'Collection of personal data' section …

What assurance has been/will be sought about the/each processor's compliance with the GDPR?	eConsult has completed NHS England's data processor assurance checklist as part of this DPIA. IG specialists in NHS England, NHS Digital and NHSX have worked closely with eConsult on this project and have assured their capability. One issue remains with challenges that eConsult continue to face replicating the terms of our Data Processing Agreement with a sub-processor, Docman. However, Docman is an

[9] 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

	approved supplier under NHS England's GPIT Futures framework and has provided IG assurance through that framework. In addition, eConsult have committed to uplifting their data processing terms with Docman within six months. NHS Digital is a trusted party and has completed NHS England's Data Processor Assurance checklist.
Will the contract use NHS England's standard data processing agreement template?	Yes, NHS England's standard Data Processing Agreement template has been put in place with eConsult and NHS Digital, while commercial contracts will be established through Principal Agreements between eConsult and primary care providers, or their CCGs on their behalf.
Will the contract contain standard clauses to require compliance with the GDPR?	Yes
Will the contract contain clauses to address the secure transfer of the personal data to a successor data processor should this become necessary or upon the expiry of the term?	Yes

Collection of personal data

Will personal data be collected from the data subject?	Yes
Will personal data be obtained from sources other than the subject?	No
Will personal data be collected from a third party(ies)?	Yes
If Y, please identify the third party(ies)?	Where using NHS Login to verify patient identity, NHS Login will provide and present the NHS number to verify against information provided by the data subject.

Is the provision of personal data obligatory or voluntary?	Voluntary, as patients will not be required or mandated to use online consultation services.
If obligatory, why/how is that the case?	Not applicable
What are the possible consequences for a data subject if there is a failure to provide the requested personal data?	The patient will be unable to use the online consultation service; however, this will not prohibit them from arranging a traditional appointment with their GP.

Privacy information

How will the data subjects be informed of the processing of personal data about them?	Privacy information will be made available to data subjects through the following mechanisms: • NHS England's privacy notice • The NHS App's privacy notice • Directly via eConsult solution  eConsult FPNs v1.0 FINAL.docx

Accuracy of personal data

How will we ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	For ID verification via NHS Login, NHS Login provides a check between the NHS number held by NHS Login and the Patient Demographic Service (PDS) to ensure validity and consistency. The PDS service has robust procedures for ensuring the accuracy of data held within it. Where NHS Login is not used, the primary care provider will manually confirm a patient's ID prior to the consultation beginning and will update any inaccuracies in personal data in line with local procedures. Data accuracy will not be an issue for personal data associated with consultations, as this will be provided directly by the data subject and summarised for the GP through automated algorithms.

How will we monitor the quality of the personal data?	For ID verification, this will take place in real time as the patient's ID is confirmed.

Subject access and data subjects' rights

How will it be possible to provide a copy of the personal data processed about a particular individual to them (redacted as necessary) should they request access to this information? (If you are purchasing an information management system, you should consider including requirements in the specification about searching and subject access requests.)	Under the joint controller arrangements, the primary care providers will retain responsibility for responding to Subject Access Requests in line with local policies and procedures.
What processes will be put in place to ensure that other data subjects rights can be appropriately applied to the personal data if necessary?	Under the joint controller arrangements, the primary care providers will retain responsibility for responding to Subject Rights Requests in line with local policies and procedures.

Data sharing (other than between NHSE and NHSI)

Will some or all of the personal data be shared with a third party (other than NHSE / NHSI)	No, beyond sharing with data processors identified above and any necessary sub-processors (described below).

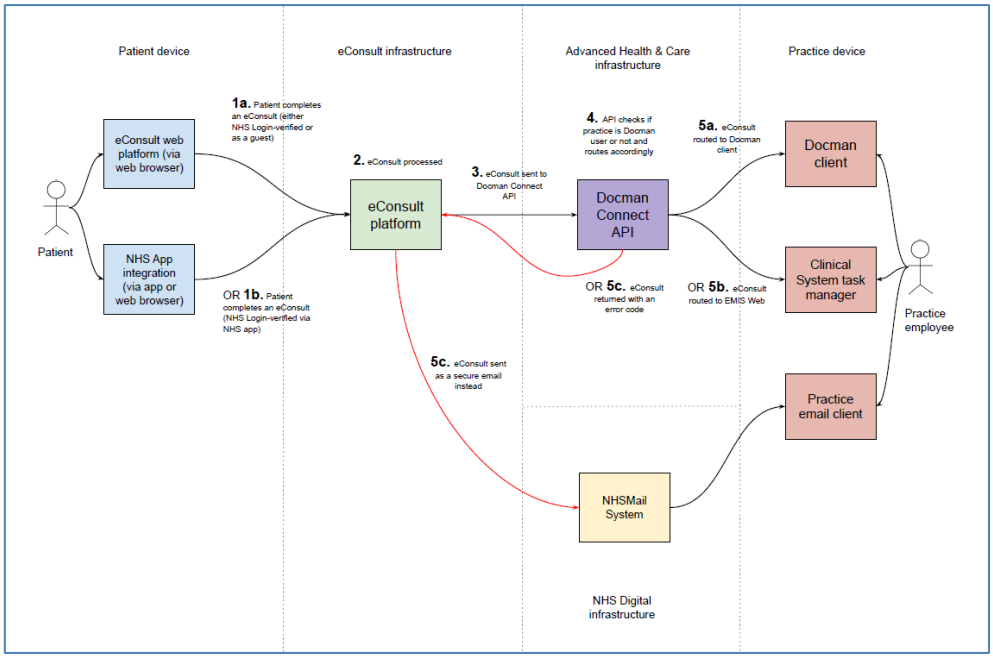
If N, please skip outflows in the next section …

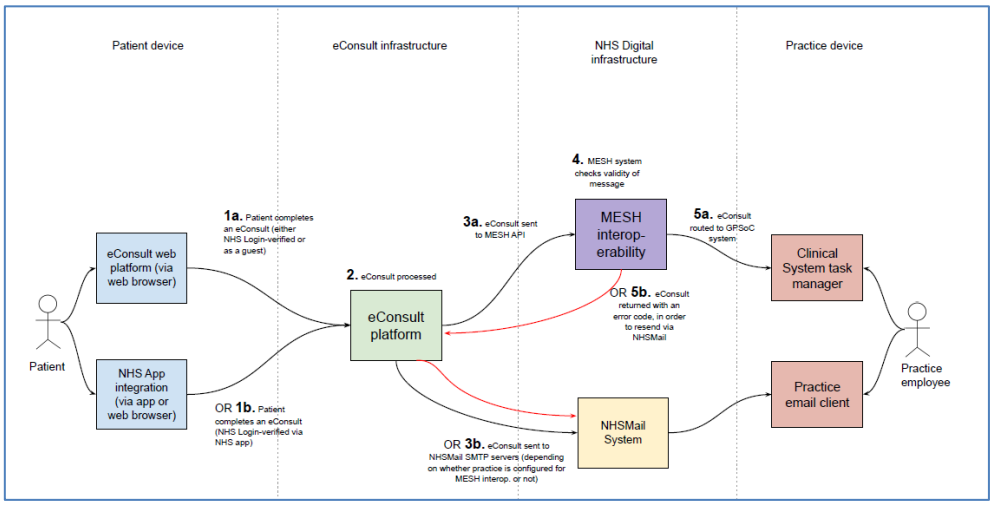
If Y, will the personal data be disclosed to a recipient(s) in a country outside the EEA or an international organisation?	Not applicable

Data flows

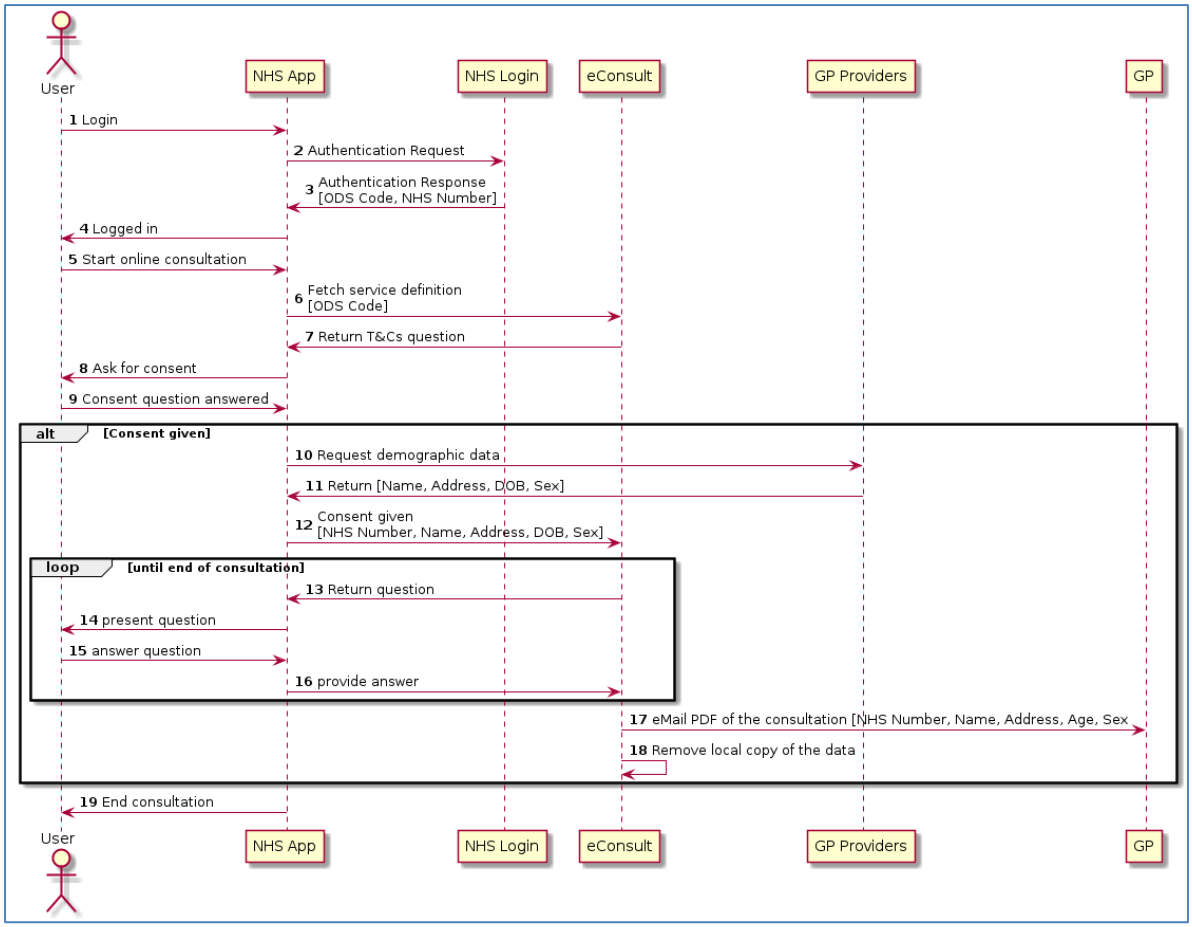
Attached below are data flow maps representing the end-to-end journey of personal data for primary care providers utilising eConsult in the following scenarios:

1. Via the NHS App (verified through NHS Login), the eConsult platform utilising NHS Login or the eConsult platform as a guest (where patient identification is then manually confirmed by practice staff)
2. Where the primary care provider utilises MESH interoperability, Docman integration or NHS Mail to receive the consultation summary from eConsult





Attached below is a data flow map of the personal data flow via the NHS App for patient ID verification:



Inflows

Sender	*Content*	*Pseudo?*	*Mode*	*Security*	*Recipient*
Data subject (Verification)	Demographic data and identifiers	No	eConsult website or NHS App	Encrypted in transit and at rest	NHS Login
NHS Login (Verification)	NHS Number	No	NHS App	Encrypted in transit and at rest	NHS App
Data subject (Consultation)	Demographic data and data concerning health	No	eConsult website or NHS App	Encrypted in transit and at rest	eConsult (via NHS App or directly)

Outflows

Sender	*Content*	*Pseudonymised*	*Mode*	*Security*	*Recipient*
eConsult (Consultation)	Demographic data, identifiers and	No	Docman MESH client	Encrypted in transit and at rest	Primary care provider

	consultation summary		NHS Mail		

Risks

What are the identified risks of the processing? Please complete risk register attached.

20181010 DPIA - Risk Assessment v2 F

Incident reporting

What plans are in place in relation to the internal reporting of a personal data breach? (NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.)	If and where an incident occurs relating to patients of a single primary care provider, this will be managed locally in line with the provider's established incident management procedures. The provider will be responsible for reporting to the ICO, where necessary. If and where an incident occurs relating to a high volume of patients spanning multiple primary care providers (e.g. a system-wide failure or breach), this will be managed nationally by NHS England in line with its established incident management procedure. NHS England will be responsible for reporting to the ICO, where necessary.
What plans are in place in relation to the notification of data subjects should there be a personal data breach? (NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.)	Where a primary care provider is responsible for managing an incident, as described above, they will manage notification to data subjects as per local incident management procedures. Where NHS England is responsible for managing an incident, as described above, it will liaise with the impacted primary care providers to ensure affected data subjects are notified.

Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	The NHS App and NHS Login use cloud hosting infrastructure, supported by real-time backup solutions which mirror the data sets required. Both services

	have tested their Business Continuity Plans within the last quarter. eConsult's disaster recovery procedures are outlined in the System Compliance Assessment List (SCAL) and DSPT submission

Records Management

Will records be created and / or managed as a result of this processing?	Yes, a summary of each patient's online consultation will be generated by eConsult and shared with the primary care provider before consultation data is deleted from the system.
Where will these records be stored?	A summary of a patient's online consultation will be sent to the primary care provider for inclusion in the patient's medical record.
Will a suitable individual, trained in records and information management, be responsible for managing these records?	NHS England will not receive consultation summaries. Within primary care providers, suitably qualified officers will be expected to manage patient records in line with local procedures and the IGA Records Management Code of Practice for Health and Social Care.

Retention of personal data

What is/are the retention period(s) for the personal data?	Consultation summaries will be retained in line with retention schedules applied to patient's medical records. Personal data associated with confirming patients' identities will be retained for 12 months. Personal data associated with audit and improvements of the NHS App will be retained for 8 years.
What is the basis for this retention period? (Please indicate applicable guidance or rationale)	Data will be retained according to the NHS' records retention schedule.
Where personal data are processed outside of NHSE's or primary care	Not applicable, as eConsult deletes all personal data associated with a

providers' premises or systems, how will they be securely returned for the remainder of the retention period(s) as and when this becomes necessary (e.g. following the closure of the project)?	consultation once the summary has been sent to the primary care provider.

Direct marketing[10]

Will any personal data be processed for direct marketing purposes?	No
If Y, please describe how the proposed direct marketing will take place:	Not applicable

Data portability

Where the processing is based on consent or due to a contract, it is carried out by automated means and the data subject has provided the personal data to us, will it be possible to provide them or a different controller with the personal data in a structured, commonly used and machine-readable format?	Not applicable

Automated processing

Will the processing result in a decision being made about the data subject solely on the basis of automated processing[11] (including profiling[12])?	No. The eConsult solution will produce a diagnostic outcome based on information provided by the data subject, however they shall not be in any way bound by that outcome.
If Y, is the decision: • necessary for entering into, or performance of, a contract between the data subject and a data controller	Not applicable

[10] direct marketing is "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

[11] examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

[12] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

• authorised by law • based on the data subject's explicit consent?	
Please describe the logic involved in any automated decision-making.	Not applicable
Please outline the significance and the envisaged consequences of such processing for the data subject.	Not applicable

ICT

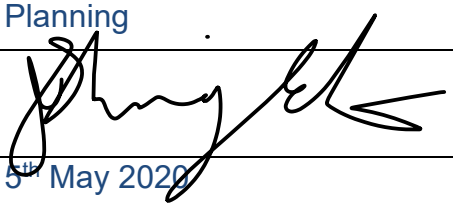
Will we, or the data processor(s), be using a new system to process the personal data?	No, both the NHS App and eConsult are established solutions.

If Y to the above question around new systems, please ensure that a System Level Security Policy is completed before proceeding to the sign off stage below.

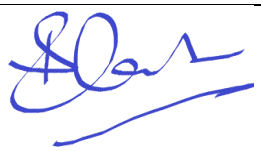
eConsult have supplied a Supplier Conformance Assessment List, originally provided to NHS Digital and meets the equivalent requirements of a SLSP.

Sign Off of DPIA and Processor Checklist (as appropriate)

IG Lead

Name	Jon Shingleton Senior Lead – IG Assurance and Planning
Signature	
Date	5th May 2020

ICT

Name	Brendan Plant Security Consultant – NHS Login and NHS App (NHS Digital)
Signature	
Date	12th May 2020

Data Protection Officer

Name	Carol Mitchell Data Protection Officer
Signature	
Date	12th May 2020

Information Commissioner's Office

(Where DPIA submitted for review)

Advice of the ICO:
Not applicable / not sought

Caldicott Guardian

Name	Prof. Stephen Powis National Medical Director and Caldicott Guardian
Signature	
Date	11 May 2020

Senior Information Risk Owner

Decision of the SIRO:	
DPIA approved, subject to formal review of IG arrangements within six months from go-live.	
Name	Mark Blakeman Deputy Senior Information Risk Owner
Signature	
Date	12th May 2020

Processor Checklist

SUPPLIER INFORMATION	
Supplier name: NHS Digital	
Address: 1 Trevelyan Square, Boar Lane, Leeds, LS1 6AE	
Telephone number: As per details of key contact	
Name of key contact: Chris Fleming	
Email address of key contact: chris.fleming@nhs.net	
If your organisation is registered with the ICO please provide Data Protection Notification number: Z8959110	
Is your organisation compliant with the Data Security and Protection Toolkit: Yes	
SERVICE TO BE SUPPLIED	
Please describe the service which is to be provided: Provisioning of connectivity to OLC services from the NHS App. Data processing of personal data in line with agreed data flows.	
CHECKLIST	
1. Do you have policies covering all elements of Data Protection and Information Security (e.g. records of processing activities, data subject rights' management)?	Yes
2. Do you have a register containing the processing activities conducted on behalf of NHS England and NHS Improvement and NHS Improvement?	Yes
3. Has the Data Processor appointed a Data Protection Officer if required? Please provide contact details if a DPO is required.	Yes Kevin Willis Kevin.willis2@nhs.net

4. Will you be processing at an NHS site? If so, where?	Yes Bridgewater Place, Water Lane, Leeds, LS11 5BZ
5. Will your staff have remote access to NHS England and NHS Improvement data? If yes, please explain.	Yes. Staff have secure remote access to the NHS App platform so that they can maintain the service.
6. Will you be storing any NHS England and NHS Improvement data in paper format for any length of time? If yes, how will the data be stored?	No
7. Will you be storing any NHS England and NHS Improvement data in electronic format?	Yes
8. If yes to Q7: - Do all users of your systems have their own log-in and password?	Yes
- How are access rights to systems controlled?	NHS D corporate ICT policies are followed. Users must complete an account access form which is authorised by the team manager. Access is periodically checked and monitored. As part of the Joiners Movers and Leavers Process (JML) users follow a process where the system access rights are removed.
- Are back–ups encrypted?	Yes
- What protection do you have against malicious code?	All code required for the service is subject to code review. All transactions are processed via a Layer 7 application firewall which inspects all of the traffic.
- How often do you apply security patches?	In line with NHSD corporate ICT Policies.
- How often do you risk assess your security controls?	Weekly scans are run on the platform. An annual CHECK ITHC is also performed on the NHS App platform.
- What business continuity/disaster recovery plans do you have in place?	The platform is a cloud hosted service on Microsoft Azure. The service is commissioned as a High Availability service.

	The service can be maintained remotely over a secure connection with multi-factor authentication. The BCDR plan was last checked in December 2019.
- Are USB ports/CD writers on staff equipment disabled?	No. There is a corporate Data Loss Prevention (DLP) system in place to identify data egress from the systems. The service uses Splunk – a Security Indecent and Event Management (SIEM) product to monitor access.
- Will you be storing data outside the UK? If so, where? What information governance considerations have been taken into account?	No data is stored outside of the UK.
- Will the data be linked with any other data collections? If so, how will the linkage be achieved?	Yes. NHS Number is used as a unique identifier between the NHS login and NHS App service in line with the current legal direction as such, no DARS authorisation is required.
9. What security controls do you have in place for your office premises?	Bridgewater Place is an access controlled site. This is supplemented with an Access control system on the office floor being used by the NHS App team to deliver the service. A designated office area is used by NHS App to provision the service. The office location is located on the 8th floor, as such, protected from casual viewing inside the office. Clear desk policies are in place.
10. What controls do you have in place for the security of your equipment?	Kensington locks are used to secure ICT in the workplace. Privacy screens are available for staff. The office area is also policed by security staff periodically.
11. Have you had any personal data breaches in the last three years? If so, please explain.	Yes. ID verification breaches – surfaced from one of the following: - Mis-verification of ID via NHS login; - Mismatch of ID due to a confusion record on PDS.
12. Please list the policies you have in relation to information security, data protection and incident reporting?	DPIA; SLSP; Information Asset Register entry; Incident Management Process;

	Business continuity Plans; Cloud Hosting Policies; Cyber Security Policies; DPO Breach Investigation Report Process; Vetting and Screening Policy.
13. Describe potential disciplinary actions for breach of policy.	Staff administrative warning Staff administrative dismissal
14. What steps do you take to ensure that the people your recruit have the honesty and integrity to handle person identifiable data?	All staff have a minimum of Baseline Personnel Security Standard (BPSS) prior to working on the project. Staff who have access to Privileged accounts/services will be put through National Security Vetting (NSV) process for Security Check (SC).
15. How do you ensure that your staff understand the importance of data security and how to keep person identifiable data secure?	Mandatory Staff training – Data Security Awareness training.
16. How frequently do you provide your staff with any training on data security and confidentiality and is their learning tested?	Annually Yes
17. Will you ever transfer NHS England and NHS Improvement data electronically? If so, how will it be transferred?	All transactions where the data is in transit will be encrypted in line with NHSD policy.
18. Will you ever transport any NHS England and NHS Improvement hard copy data? If so, what security controls will be in place?	No
19. Will you ever destroy any NHS England and NHS Improvement data? If so, how will this be done and what evidence of the destruction will you provide?	Yes. NHS D manage the encryption keys and certificates associated with the data, in transit and in storage. Destruction/revocation of the keys/certs associated with the data will render the data useless. A record of the destruction is available.
20. Will you ever sub-contract work in relation to NHS England and NHS Improvement data? If so, in what circumstances? And if so, do you have relevant contractual relations with any sub-processors and have these been approved	Yes. Akamai Web Application Firewall – used to inspect all traffic. A component of this also provides a content delivery network which provides a high availability of the service; Microsoft Azure – Cloud Hosting.

by NHS England and NHS Improvement and NHS Improvement?	All contracts are GDPR compliant.
APPROVAL	
Date completed	12th May 2020
Completed by	Jon Shingleton
Telephone number and email address	england.igpolicyteam@nhs.net

SUPPLIER INFORMATION	
Supplier name: eConsult Health Limited	
Address: 3rd Floor, Moorfoot House 221 Marsh Wall London E14 9FJ	
Telephone number: 020 7062 5737	
Name of key contact: Steve Lillywhite (Chief Technology Officer)	
Email address of key contact: steve.lillywhite@webgp.com	
If your organisation is registered with the ICO please provide Data Protection Notification number: Z2881782	
Is your organisation compliant with the Data Security and Protection Toolkit: YES	
SERVICE TO BE SUPPLIED	
Please describe the service which is to be provided: Primary care, patient-facing online communication system	
CHECKLIST	
1. Do you have policies covering all elements of Data Protection and Information Security (e.g. records of processing activities, data subject rights' management)?	Yes
2. Do you have a register containing the processing activities conducted on behalf of NHS England and NHS Improvement and NHS Improvement?	Yes
3. Has the Data Processor appointed a Data Protection Officer if required? Please provide contact details if a DPO is required.	Yes Caroline Leuder privacy@webgp.com

4. Will you be processing at an NHS site? If so, where?	No
5. Will your staff have remote access to NHS data? If yes, please explain.	No
6. Will you be storing any NHS data in paper format for any length of time? If yes, how will the data be stored?	No
7. Will you be storing any NHS data in electronic format?	Yes
8. If yes to Q7: - Do all users of your systems have their own log-in and password?	Yes
- How are access rights to systems controlled?	Access granted only to key, senior members of technology team. Procedures in place to remove access when staff leave or roles change.
- Are back–ups encrypted?	Yes
- What protection do you have against malicious code?	Platform has built in protection against typical attack vectors, such as XSRF, HTML injection and SQL injection. Regular penetration tests are run against the platform.
- How often do you apply security patches?	Minimum quarterly
- How often do you risk assess your security controls?	Minimum annually
- What business continuity/disaster recovery plans do you have in place?	eConsult is hosted on a fault-tolerant, load balanced, HSCN-facing environment. The data centre is Tier 3 and ISO27001. Much of our infrastructure is multi-zone, and our key services have built-in elastic scaling, allowing the product to scale at ease. We have multiple levels of monitoring in place; to detect infrastructure outages, system-level issues and application-level issues. A defined business continuity plan is in place, covering the main premises and hosted data

	centres. It is included as part of the Data Security & Protection Toolkit documentation and is reviewed regularly. It defines the incident response teams, risk impact assessments, and notification & escalation procedures. We also run regular disaster simulations to review our ability to adhere to our guidelines, and ensure we adapt and improve accordingly.
- Are USB ports/CD writers on staff equipment disabled?	No
- Will you be storing data outside the UK? If so, where? What information governance considerations have been taken into account?	No
- Will the data be linked with any other data collections? If so, how will the linkage be achieved?	No
9. What security controls do you have in place for your office premises?	The eConsult team primarily works out of two offices: London – Moorfoot House, is used by the Executive, Operations and Clinical teams. Paper assets are stored at this office. No patient sensitive data is stored. Brighton office is primarily used by the Technology team. No paper assets or patient sensitive data are stored at this office. No members of the public are allowed onto either premises unless a member of staff is present. Both offices use key fobs, with tightly controlled access. Visitors are not left unattended and staff are responsible for ensuring that visitors are entered into the reception diary.
10. What controls do you have in place for the security of your equipment?	Staff lock their workstations when leaving them unattended and do not share passwords or log in details. Multi-factor authentication is used wherever possible.
11. Have you had any personal data breaches in the last three years? If so, please explain.	No
12. Please list the policies you have in relation to information security,	- Browser and accessibility standards - Unauthorised disclosure or transmission of patient identifiable data

data protection and incident reporting?	- GDPR compliance - Device encryption standards - Device security policy - Account-based access - Compliance with data security standards - Clinical risk management plan - Incident reporting
13. Describe potential disciplinary actions for breach of policy.	Formal, structured, disciplinary processes have been put in place by the HR Manager to ensure any such breach is fully investigated and that the employee is fairly represented. Disciplinary meetings are documented, chaired by a senior manager and employees given the choice to have a companion at all times. Disciplinary penalties have three stages; two written warnings and dismissal.
14. What steps do you take to ensure that the people your recruit have the honesty and integrity to handle person identifiable data?	All staff are required to have a DBS check. Any member of staff with administrative access must sign an internal document stating they understand their responsibilities. Recruitment processes have been standardised across the company.
15. How do you ensure that your staff understand the importance of data security and how to keep person identifiable data secure?	Standard, annual data security and protection training for all staff.
16. How frequently do you provide your staff with any training on data security and confidentiality and is their learning tested?	Annually at a minimum, using an online, DSP Toolkit-approved training course
17. Will you ever transfer NHS data electronically? If so, how will it be transferred?	Patient data is transferred from eConsult to practices electronically, using a TLS-encrypted connection, via the HSCN network.
18. Will you ever transport any NHS hard copy data? If so, what security controls will be in place?	No
19. Will you ever destroy any NHS data? If so, how will this be done and what evidence of the destruction will you provide?	No
20. Will you ever sub-contract work in relation to NHS data? If so, in what circumstances? And if so, do you have relevant contractual relations with any sub-processors and have these been approved by NHS England?	Yes, contractual relations are in place with our sub-processors for this service at the approval of NHS England.

APPROVAL	
Date completed	5th May 2020
Completed by	Jon Shingleton
Email address	england.igpolicyteam@nhs.net