****

GP Online Services Guidance

*Information governance for record access*

Contents

1. Introduction 1
2. Applications for GP Online Services 2
3. Automatic record access 3
4. Coercion 4
5. Identity Verification 5
6. Clinical assurance of the record 6
7. Informed patients 6
8. Proxy access 7
9. Patients who already have access to their practice online services 8
10. Recording third party data 9
11. Legal, employment and insurance matters 9
12. Documenting practice privacy policies 10
13. Data Privacy Impact Assessment 10
14. Disclaimer 11
15. Further reading 12
16. **Introduction**

The purpose of this guidance is to describe the practice’s legal and formal responsibilities in relation to the processing of confidential patient information in offering and providing online services. It pulls together all the key information from other guidance in one place to ensure that practices have a clear overview of the whole subject. It is intended primarily for the practice online services lead and Caldicott Guardian but is relevant to the roles and responsibilities of everyone working with the practice online services.

This guidance covers the practice’s responsibilities for:

1. Management of new applications for practice online services by patients and people acting on their behalf
2. Information governance of the records of patients who already have access to online services
3. Supporting patients’ appropriate use of their GP Online Services.

Information governance is the term used to describe the standards organisations apply when they manage information. It covers the behaviour and management needed to ensure that confidential information is handled legally, securely, efficiently, effectively and in a way which maintains public trust. It is based on the balance established in law between privacy and sharing of confidential data which is fundamental to health and social care.

Practice policies and any associated guidelines on information governance should be updated to cover GP online services. All team members need to understand what to do, particularly in circumstances that may be unfamiliar to them.

If doubts arise about how to manage a specific event, you can seek specialist advice on information governance issues from Local Medical Committees, local Caldicott Guardians, medical indemnity organisations, or the General Medical Council.

i Advice can be sought from the Information Governance Alliance[, https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga](file:///C%3A%5CUsers%5Cgmarsden%5CDownloads%5C%2C%20https%3A%5Cdigital.nhs.uk%5Cdata-and-information%5Clooking-after-information%5Cdata-security-and-information-governance%5Cinformation-governance-alliance-iga)

i NHS England has launched an Information Governance (IG) Portal, [www.nhsx.nhs.uk/information-governance](https://transform.england.nhs.uk/information-governance/)on behalf of the Health and Care IG Panel which is the one stop shop for IG guidance and advice

1. **Applications for GP Online Services**

The principles of information governance are very important in registering patients who have requested access to GP Online Services. They are introduced here and discussed in more detail in the following sections of the guidance:

1. Always actively seek evidence of **coercion** of the patient to allow someone else to have access to their online services or record unwillingly and act on any suspicion that this may happen.
2. Take extra care when signing up applicants for **record access** because of the risk of exposure of particularly potentially harmful confidential patient information.
3. **Verify** the applicant’s **identity** to ensure they relate to the record on your practice clinical system that they are asking to access.
4. **Clinically assure** that the record is ready for the patient to read before. Potentially harmful information may need to be redacted. If that is not possible, consider limiting, refusing or blocking their access as appropriate.
5. **Provide information** to the patient about how the practice’s online services work, how to keep their online access secure, to help them understand the health information it contains and know that the practice is ready to discuss any questions they may have about their record.
6. **Deliver login credentials** to the patient securely, by the method of their choice, by hand, post or email, ensuring that the patient understands the risks of each method of delivery.
7. Assess and provide **Proxy access** by someone acting on behalf of the patient appropriately.  This may be a carer, partner or parent, appropriately
8. Under the UK GDPR, **children** under the age of 13 must not be given control of an internet service such as GP Online Services.

i There is information about signing up new patients for GP online services in the section of the Toolkit on Registering New Patients for GP Online Services.

i There is more information about managing coercion and safeguarding risks in the section on Clinical Safety and in the Toolkit

i “Where point (a) of [Article 6(1)](https://uk-gdpr.org/chapter-2-article-6/) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.” (article 8, UK General Data Protection Regulation), https://uk-gdpr.org/chapter-2-article-8/

1. **Automatic record access**

Patients aged 16 and over, who have an active account with a patient facing services app or web portal, such as the NHS App, will have automatic access to their full GP record from 2022. If they access the services through an NHS Login, identity verification is carried out online when they apply for the Login.

i There is a list of patient facing services apps that use the NHS Login here - <https://www.nhs.uk/nhs-services/online-services/nhs-login/websites-and-apps-you-can-access-with-nhs-login>/

**Practices remain responsible for ensuring that patients do not come to harm from automatic online access. Before automatic record access becomes available it is very important that practices assess all their patients for evidence that they may be subject to coercion to share their record access or at risk of harm.**

It may then be appropriate for these individuals where there is a suspicion that serious harm may result from online record access (as defined by GDPR) to prevent future automatic record access adding a specific SNOMED term to their record. After discussion with the patient, it may be possible to switch on record access in the usual way using the practice clinical system GP Online Services controls or override the first term by adding the second term below to the patient’s record.

The SNOMED terms that affect automatic record access only operate if the patient has automatic access to their GP record. They are:

* **1364731000000104 Enhanced review indicated before granting access to own health record**
* **1364731000000106 Enhanced review not indicated before granting access to own health record**

**1364731000000104 Enhanced review indicated before granting access to own health record** blocks future implementation of automatic record access for the individual patient if it is entered into the patient’s record **before** three critical events when automatic record access would be switched on for the patient.

1. On the launch date of automatic record access
2. When the patient reaches their 16th birthday.
3. When a patient with no account for GP Online Services set up an NHS login or applies to the practice for a PFS (patient facing services) account.

Automatic record access is only available to the records from a patient’s current practice. If they change practice their access to their previous GP practice records is blocked and they will receive automatic record access at the new practice if they use an NHS Login.

It also means that practices must be mindful all the time of whether new information that they are adding or filing in patients’ records has the potential to cause harm, especially serious harm. All such information should be hidden from online view by default before it becomes visible to the patient.

To have access to the record from their old practice, they will have to apply to their new practice in the usual way. They will also have to apply to the practice for login credentials if they do not want to use an NHS Login to access their GP Online Services.

Practices can switch off existing automatic record access using the GP Online Services controls in the practice clinical system because of fears about coercion and patient safety. For patients who do not currently have automatic record access, it is possible to prevent future automatic record access being switched on by adding a specific SNOMED CT term.

If their automatic record access is blocked, patients can apply to have their access restored by the practice in the usual way.

i There is more information about managing automatic record access safely in the “Working with Automatic Record Access” and “Preparation for Automatic Record Access”, and how specific SNOMED terms affect automatic record access in the “SNOMED Terms that Control Automatic Record Access” guidance and the “Flowchart - SNOMED Triggers for Automatic Record Access.”

1. **Coercion**

All practice staff must be aware of the potential risks of coercion and the indications to look out for to help patients who might be subject to coercion. It is the act of governing the actions of another by force or by threat, to overwhelm and compel that individual to act against their will. In this context, coercion might result in patients being forced to share access to their record, including login details, medical history, repeat prescriptions, and GP appointments. It gives someone abusing the patient the ability to control their access to healthcare.

Coercion to share or misuse access to GP Online Services is most likely to happen if the patient is a child, an adult in an abusive relationship, or an elderly person who lacks capacity, or an otherwise vulnerable adult.

You may already have processes in place to manage safeguarding risks of suspected coercion relating to paper-based and face-to-face services but GP Online Services create new and additional opportunities for coercive behavior that must be addressed specifically. Everyone in the practice who signs up patients for any practice online services must be aware of the possibility of coercion and actively seek indications of it.

Always discuss the issue of coercion with patients who ask to sign up for online services. and ensure that they understand and accept the risks. Every new applicant should be asked a question to raise the issue of coercion such as “Is it possible that you may come under pressure to give someone access to your personal information against your will”. The question should be included in a registration form for online services for patients.

Any suspicion or evident risk of coercion must be referred to the practice online services lead or a senior clinician who knows the patient to consider withholding online access at least until the situation can be thoroughly investigated and assessed. It may be possible to sign the patient up to limited access. Any information in the record indicating abuse must be redacted.

i There is more information about Coercion and Safeguarding risks and a template for a new application form in the Toolkit.

i RCGP, NICE, SafeLives and IRIS (Identification & Referral to Improve Safety) have published guidance for practices to help effective response to patients experiencing domestic abuse (see Resources below).

i There is more information on the management of harmful data in the guidance on “Managing Potentially Harmful Information” in the Toolkit.

1. **Identity verification**

Providing access to GP Online Services demands a consistent and robust approach to ensure that the person applying for access to a patient’s services is the person that the record relates to.

Patients may book an initial appointment online as soon as they have completed a simple online registration process but a stronger identity verification process is required before full access to appointments, repeat prescriptions or clinical records is switched on.

Patients may use the NHS App to verify their identity but the practice can use any one of three methods that can give them certainty that the applicant is who they claim to be.

1. Most patients can prove their identities by providing **two forms of documentary evidence:** one must include a photo that clearly matches the patient and the other must confirm that the applicants address is the one that you have on your records. Acceptable documents include passports or photo driving licences with photographs and documents bearing the address that are likely to have been posted to the patient such as a bank statement. Bills do not usually satisfy this criterion. A full list of acceptable documents is published by the Cabinet Office (see further reading).
2. There will always be some patients (e.g., temporary residents, travellers or young people living with their parents) who do not have acceptable identity evidence. In these cases, an authorised member of staff, who knows the patient well enough to verify that they are who they say they are, and that no deception is taking place, may be able to **vouch for their identity**. Practices must judge each patient application on a case-by-case basis while ensuring that the agreed policy takes into account the duration of registration and frequency of patient contact
3. If neither of these two methods of verification are possible, consider **using information in the patient’s health record** to verify the identity of the applicant. A trained member of staff may be able to satisfy themselves of the applicant’s identity by obtaining responses to questions from information held in the medical records. This should take place discreetly and ideally in a planned appointment. It is extremely important that the questions posed do not incidentally disclose confidential information to the applicant before their identity is verified.

i There is more information about this in the “Identity Verification” guidance in the Toolkit.

1. **Clinical assurance of the record**

Clinical assurance of the record is an essential process to complete before record access is switched on by the practice or automatically. It serves two purposes:

1. If the patient has applied for access to historical records or has given consent for a trusted third-party to have proxy access. It involves screening the past record to ensure that the patient or the proxy cannot see information that may cause them harm or reveal confidential information relating to a third person, which they have no right to see. Such information may be redacted. If this is not possible, it may be necessary to refuse access to the historical record.
2. Before automatic record access is switched on it is helpful to screen the records of all patients who are eligible for automatic record access for evidence of anything that puts the patient at risk from online record access such as a safeguarding risk, serious mental health problem, substance misuse or impaired intellectual capacity. Patients identified in the audit may then by assessed individually to determine whether the risk is significant. Where possible this assessment should include a confidential discussion with the patient (see the section on automatic record access above)

It can be useful to follow the same process of screening the record for potentially harmful information or safeguarding risk for new patients joining the practice because redaction flags put in place by previous practices are not currently transferred by GP2GP and the need to redact future information or refuse online record access may not be apparent.

Clinical assurance of large records can be time-consuming. There is commercial software that can speed up the process by searching the record, including scanned documents, for potentially harmful codes and text. A trained medical summariser can also help to check the records and redact clearly potentially harmful data but the final decision on redaction and refusal or restriction of record access if potentially harmful data cannot be redacted should lie with a senior clinician.

i There is more information about clinical assurance in the guidance on “Managing Potentially Harmful Information” and “Safeguarding Vulnerable Groups” in the Toolkit.

1. **Informed patients**

Patients need to know how to use their GP Online Services safely, to protect their access and keep their data secure. If patients want to be able to use the online services but lack the computer skills that they will need, they may be able to use a local centre to learn to use computers securely. There is a network of learning centres throughout the UK co-ordinated by the Good Things Foundation (see further reading below).

Patients who have access to their practice’ online services have a responsibility for the security of the confidential health information that they can access, and they need to know how to protect it. They should also be aware that the information they see may be harmful or upsetting, if they see information that they disagree with, that is incomplete, or inaccurate. They may identify things that are missing that they would like to have in the record such as allergies or past vaccinations. They may see confidential information relating to a third person that they should not have access to. The practice should make sure that patients are fully informed about all these possibilities when they apply for any GP Online Services.

i There is more information about the information that patients need to use GP Online Services in the guidance on “Patient Information Themes for GP Online Services” in the Toolkit.

Tried and trusted techniques such as “chunk and check” and “teach back” help patients retain information about their health and GP services. Verbal advice about GP Online Services should be backed up by accessible written information on paper or on the practice website, which patients with a visual disability often prefer. Patient leaflets, posters, websites and any other means of communication available to the practice can be used to communicate with patients about GP Online Services.

i There is information in the Health Literacy Place about “chunk and check” here - <https://www.healthliteracyplace.org.uk/toolkit/techniques/chunk-and-check/> and “teach back” here <https://www.healthliteracyplace.org.uk/toolkit/techniques/teach-back>/

i There is also more guidance on “Patient Information Themes for GP Online Services” in the Toolkit and templates for patient leaflets on understanding abnormal laboratory results and other topics.

Patients can use their detailed coded record as a list of terms to learn about how to understand their condition. By encouraging patients to engage with their own health record, they are more likely to become inquisitive and engaged with their diagnoses, investigations and treatments that they identify within the record itself.

i There is more information about how to support health literacy in the [RCGP Person-Centred Care Toolkit](https://www.rcgp.org.uk/clinical-and-research/resources/toolkits/person-centred-care-toolkit.aspx.),

Useful websites that patients can rely on for information about a wide range of health matters include:

* <https://www.nhs.uk>
* <https://patient.info>
* <https://labtestsonline.org.uk>
1. **Proxy access**

Some patients find it helpful for a second person to have access to their GP Online account. This is called proxy access. It may be an informal arrangement by which the patient shares their log in credentials with their proxy and the practice may know nothing about it or, if the GP system has the capability, a more formal arrangement where the practice give the proxy their own personal log in credentials and sets the proxies level of access, which may be different to the patient’s access.

This normally requires the patient’s consent but, in some circumstances, where the patient is not able to consent, the practice may make the decision to allow proxy access if it is clearly in the best interests of the patient. The decision is made more easily if the patient made an advanced decision to allow a named individual to have proxy access when their health deteriorated when they are no longer able to manage their own healthcare, or if the proxy has a lasting or enduring power of attorney or is a Court Appointed Deputy. It is also possible to allow proxy access for a child up to their 11th birthday to someone who has parental responsibility for the child.

Where proxy access is being considered for direct care by health professionals with a legitimate relationship with the patient, access should only be named individuals and a data sharing agreement should be completed by the practice and the health professional or their organisation.

**Children** - It is also possible to allow proxy access for a child up to their 11th birthday to someone who has parental responsibility for the child. As young people mature into their teens, there may be something that they do not want their parents to know about. parental access to them may inhibit their use of health services. To avoid this, you should switch off parental proxy access to a child’s GP Online Services on their 11th birthday. It is helpful to write to a patient’s parents six months earlier to tell them that it will happen. This gives them time to ask the practice if they feel that their child would benefit from continued proxy access.

i There is specific guidance on “Proxy Access”, and the “Children and Young People” in the Toolkit. There is information about sharing GP record access for direct care with organisations such as nursing homes in the “Dementia” guidance in the Toolkit. There is also a template consent form in the Toolkit that you can use to record the patient’s consent to their proxy receiving access to their GP Online Services.

1. **Patients who already have access to the practice online services**

Practices have a continuing responsibility for patients who have active GP Online Services access.

**Safeguarding** - It is important to be aware of the risk to vulnerable patients where access to their GP Online Services may be used by someone as part of a pattern of abuse. If a safeguarding risk arises or is suspected, or where there is suspicion that a patient may be subject to coercion to allow someone to have access to their online services unwillingly, the practice will review access It may be necessary to disable some services entirely or it may be possible to limit access, for example by restricting record access but continuing to allow access to appointments and prescriptions.

**Record data quality** - Patients appreciate high quality, complete, accurate and unambiguous record data that clearly represents their health history. Staff should take care to avoid the use of abbreviations and euphemisms that may be misunderstood by patients and avoid recording third-party data. It is not always easy to know if a patient has online record access and it is impossible to know who may have access in the future. Consider ensuring that all clinical records are fit for sharing with patients. This includes the redaction of any potentially harmful data that may harm the patient or reveal confidential information about a third person.

Some data may be particularly harmful for patients who are subject to abuse. Always consider redacting records that refer to any suspicion or actual abuse. Data that is confidential information about a third-party that the patient has no right to know should always be redacted. If it is not possible to redact some potentially harmful data, it may be best to refuse or restrict record access for that patient. Abnormal test results can cause undue worry to patients if they see them online before they have had an opportunity to discuss them with a clinician. It is usually best to redact them until they can be discussed.

i There is more information on the management of data quality in the Data Quality guidance and potentially harmful data in the guidance on “Safeguarding” “Data Quality for Record Access”, “Managing Potentially Harmful Information” and “Working with Automatic Record Access” in the Toolkit.

1. Recording third-party data

This is data received from a third-party or data about a third-party (e.g. agreed recorded family history data) recorded in the patient’s record; or consultation data, test results or scanned documents recorded by mistake in the wrong patient’s record. Disclosure may be a breach of data protection law and may result in harm or distress to the patient or breach the confidentiality of the third-party.

Before recording anything about a third-party in a patient’s record, including identifying the source of information about the patient provided by a third-party, you should discuss the possibility that the patient will see the information if they have access to their records. There are four steps that you can take:

* Ensure that the third-party understands that the patient may be able to infer the source of the information
* Ensure that the third-party is prepared to bear that risk or to have their identity explicitly recorded.
* Obtain and record the consent of the third-party for the patient to have access to the information before recording the information
* Redact the information so that the patient cannot see it online but it may still be included in a paper printout of the patient’s record and available to the patient through a subject access request under the Data Protection Act 2018.

The third-party may decide to withhold the information or make it clear that they do not wish it to appear on the record of the patient.

i There is more information about how to report a breach of personal data to the Information Commissioner at [https://ico.org.uk/for-organisations/resources-and-support/pdb/](https://ico.org.uk/for-organisations/resources-and-support/pdb/%20)

1. **Legal, insurance and employment reports**

Patients may consider using the clinical record information that they can see in their online record to complete applications or reports for legal matters, insurance, financial arrangements, or employment. They should be advised against it and they should not use a printout of their available record in place of completing a personal health report form. Online record access does not replace full subject access request,

There are several reasons for this advice.

* Online access does not display all the information in the GP record.
* Significant information may have been redacted.
* The information that is available to the patient may not be presented in a way that makes it possible for the patient to summarise its contents.

All these possibilities mean the report may be incomplete, which may put the patient at risk.

The language of the information displayed by GP Online Services is often technical and may be mis-interpretated by the patient. A patient may include something in the record that they do not fully understand and unintentionally give the wrong impression of their health to the recipient of their report.

Finally, the report may be mistakenly attributed to the practice and deemed to be a medical report by whoever the patient shares it with.

1. **Documenting practice privacy policies**

As data controllers, practices are required to create and maintain a Record of Processing Activities. Your Practice is likely to have a documented record around Patient Access through a PFA app already. You will have to update the ROPA to reflect the changes (patient access to full record by default for future/prospective record).

Practice privacy notices should include all types of online record access including automatic record access. NHS Digital provide information you may want to include in your privacy information at the link below to “Access to Patient Records Through the NHS App”. You might just include the link.

i Information Commissioner’s Office, “Records of Processing and Lawful Basis” - <https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/>

i BMA, GDPR Privacy Notices for General Practice [- https://www.bma.org.uk/advice-and-support/ethics/confidentiality-and-health-records/gdpr-privacy-notices-for-gp-practices](file:///C%3A%5CUsers%5Cgmarsden%5CDownloads%5C-%20https%3A%5Cwww.bma.org.uk%5Cadvice-and-support%5Cethics%5Cconfidentiality-and-health-records%5Cgdpr-privacy-notices-for-gp-practices)

i NHS Digital, Access to Patient Records Through the NHS App - [https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/accelerating-patient-access-to-their-record](https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/guidance-on-nhs-app-features/accelerating-patient-access-to-their-record)

1. **Data Protection Impact Assessment**

The risks related to the automated online record access risks will vary from practice to practice as each will have different characteristics, population demographics, turnover in patients, staff expertise, vulnerable groups of patients. Practices have a responsibility to carry out and document a Data Protection Impact Assessment (DPIA) in these circumstances. It is a tool designed to help establish what processing is taking place, what risks this new processing brings and then describe the steps the practice may take to mitigate these risks which may include restricting access for certain cohorts (applying SNOMED codes to certain groups), staff training and other risk mitigation processes.

In some circumstances it is a legal requirement under UK GDPR to carry out a DPIA and this is typically when there is processing “likely to result in high risk” to individuals. Excluding patients though the use of code sets would automatically trigger the requirement for a DPIA as it could be seen as a “Denial of service” or “profiling” both of which risk the rights and freedoms not only of those who are excluded but also those who should have been excluded but weren’t.

NHS England has created a template DPIA that should help General Practices understand the risks and then tailor it to the specific needs of their practice and patients. The ICO has produced guidance on creating a DPIA and have an example template online that could be used by practices (see the links below). It has all the necessary questions that practices need to consider before enabling this processing. Both these documents should be considered when tailoring the DPIA for the individual practice.

i Information Commissioner’s Office, “When do you need to do a DPIA” - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when2>

i Information Commissioner’s Office, “Data Protection Impact Assessments” - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

i NHS England, DPIA template- <https://transform.england.nhs.uk/documents/129/Data_Protection_Assessment_template.odt>

1. **Disclaimer**

This guidance is a public resource providing general information and not advice relating to specific issues. Users of this guidance should consider taking advice tailored to their particular circumstances. This guidance is intended, but not promised or guaranteed, to be correct and up-to-date at the time of its publication. The Royal College of General Practitioners does not warrant, nor does it accept any responsibility or liability for, the accuracy or completeness of the content or for any loss which may arise from reliance on information and material contained in this guidance.

1. **Further reading**

**Information Governance Policy**

**Royal College of General Practitioners**, GP Online Services: The Road Map 2013, is available in the GP Online Services Toolkit

**General Medical Council**, Review of public and professional attitudes towards confidentiality of healthcare data: Final report, 2015 at <https://www.gmc-uk.org/-/media/documents/review-of-public-and-professional-attitudes-towards-confidentiality-of-healthcare-data_pdf-62449249.pdf>

**Care Quality Commission** - describe the approach to information governance that they expect health and social care organisations to take in their Policy Statement on Information Security and Guidance at <https://www.cqc.org.uk/sites/default/files/20160411%20Final%20Policy%20Statement%20on%20Information%20Security%20July.pdf>

**The Caldicott Review** Information: To share or not to share? The Information Governance Review, 2013 is a guide to the principles of information governance for health records including the management of third-party information at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf>

**British Medical Association**, GDPR (General Data Protection Regulation) - a guide for BMA members, 2018, at <https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr>

**NHS Digital,** Data Security and Protection Toolkit, 2018, at <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>

**Information Commissioner’s Office** There is more information about the right of patients under the General Data Protection Regulation 2018 to have personal data rectified at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/>

**Coercion**

**RCGP** has several resources on its website on domestic violence and safeguarding adults and children<https://www.rcgp.org.uk/clinical-and-research/safeguarding.aspx>

**NICE** has succinct advice on recognising and responding to evidence of domestic violence or abuse = QS116 (https://www.nice.org.uk/guidance/qs116) and in their guidance on Domestic violence and abuse: multi-agency working - PH50 (<https://www.nice.org.uk/guidance/ph50>).

**Safelives** provides many useful resources on coercion and domestic abuse, including resources for GPs and guidance on identifying domestic abuse <https://safelives.org.uk/policy-evidence/about-domestic-abuse> and <https://communications.safelivesresearch.org.uk/Pathfinder%20Toolkit_Final.pdf>

**IRIS** (Identification and Referral to Improve Safety) is a charity that offers a general practice-based domestic violence and abuse (DVA) training support and referral programme that has been evaluated in a randomised controlled trial - <http://www.irisdomesticviolence.org.uk/iris/>

**Identity Verification**

**Cabinet Office** - Good Practice Guide 45 “Identity-proofing-and-verification-of-an-individual” lists acceptable documents for identity verification at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>

**NHS Digital** - “Identity Verification and Authentication Standard for Digital Health and Care Services”, 2018 at [https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3051-identity-verification-and-authentication-standard-for-digit](https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3051-identity-verification-and-authentication-standard-for-digital-health-and-care-services).

**Information for Patients**

**NHS England’s** team offer materials for patients, including easy read leaflets which you can order online at <https://www.england.nhs.uk/gp-online-services/support/supporting-material/patient-information-guides/>

**The RCGP Toolkit** contains templates forms for signing up new applicants for GP Online Services and proxy access and information leaflets on abnormal laboratory results.

**Computer literacy and digital inclusion**

**The Good Things Foundation** coordinates a network of learning centres where patients can boost their computer skills. Find your local centre at <https://www.goodthingsfoundation.org/online-centres-network>