Patient Online Services in Primary Care

Good Practice Guidance on Identity Verification

NHS England INFORMATION READER BOX		

Directorate		
Medical	Commissioning Operations	**Patients and Information**
Nursing	Trans. & Corp. Ops.	Commissioning Strategy
Finance		

Publications Gateway Reference:	**02160**
Document Purpose	Guidance
Document Name	Good Practice Guidance on Identity Verification
Author	Richard Sewart
Publication Date	25 February 2015
Target Audience	GPs
Additional Circulation List	Information Governance leads and practitioners
Description	This guidance is to help GPs to apply consistent good practice in identity management when giving patients access to online services.
Cross Reference	
Superseded Docs (if applicable)	
Action Required	Registered professionals and organisations must have regard to this guidance when offering online services
Timing / Deadlines (if applicable)	
Contact Details for further information	Stuart A Notholt Information Governance Taskforce, NHS England Skipton House, 80 London Road SE1 6LH 07796 994375

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet

Patient Online Services in Primary Care

Good Practice Guidance on Identity Verification

Version number: 1.0

First published:

Updated: n/a

Prepared by: Richard Sewart, Data Sharing and Privacy Specialist, Information and Transparency Group, Patients and Information Directorate.

Contents

1 Executive summary

NHS England has a duty under the NHS Act 2006 to publish guidance on the processing of patient information. This Good Practice Guidance fulfils this obligation in respect of identity management for patient online services. It provides options for how general practice staff can verify the identities of patients registering with, or currently registered at a practice before providing them with online services.

This guidance is intended for GPs and general practice staff. It is also intended as a reference document for the development of further guidance and training materials.

GPs and other health professionals that offer online services must have regard to this guidance.

The document is arranged in three parts:

Part 1 – Introduction: context, legal and contractual requirements;
Part 2 – Principles;
Part 3 – Guidance: roles and responsibilities and requirements for business processes;
Part 4 – Appendices: supporting materials.

PART 1 – Introduction

2 Context

2.1 Purpose

The purpose of this guidance is to help General Practice[1] to apply consistent good practice in identity management when providing patients access to online services such as booking appointments, ordering repeat prescriptions, and viewing clinical records. Offering online services is a requirement of the General Medical Services Contract 2015/2016.

This guidance gives practical options for identity management (i.e. verifying the identities of patients registering with, or currently registered at, a practice) prior to enabling online access[2].

The focus of this guidance is on identity management in primary care as part of the *Patient Online* initiative. It forms part of a strategy on identity management for online access by patients across all care settings. This is looking at approaches that should reduce the burden on local organisations – approaches such as federated identity management and the use of online registration.

2.2 Audience

The audience for this guidance is GPs and general practice staff. It is also intended as a reference document for the development of further guidance and training materials.

2.3 Scope

This guidance covers the processes required in General Practice to verify the identities of patients or their delegated representatives (proxies – e.g. parents or carers), before enabling access to online services for them.

The following issues are out of scope:

- Requirements for enabling lawful proxy access in addition to identity verification;
- Protection against coercion.

Accompanying guidance on these issues will be published separately.

[1] Reference to General Practice or GP Practice in this document refers to a provider of essential primary medical services to a registered list of patients under a General Medical Services, Personal Medical Services or Alternative Provider Medical Services contract.

[2] The guidance also applies to the verification of proxies, who with due authorisation may hold accounts allowing access to services on behalf of other patients. A proxy need not necessarily be registered at the practice as a patient.

2.4 Definitions

Some key terms relating to identity management in the context of enabling access to online services are set out in Appendix 1.

The word **must** is used in this document to identify a legal requirement.

The word **should** is used to indicate that, in particular circumstances, there may exist valid reasons to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

The word **may** is used to indicate a truly optional activity. This includes decisions where a permissive legal power is available.

3 Legal and contractual requirements

NHS England is required by the NHS Act 2006[3] to publish guidance for professionals and organisations registered with the Care Quality Commission (CQC) on the processing of patient information. This guidance fulfils this obligation in relation to the processing of information in the context of patient online services offered in primary care.

In accordance with the 2006 Act, CQC registered professionals and organisations must have regard to this guidance when offering such services.

The main legal and contractual requirements for GPs in their delivery of online services arise from the Data Protection Act 1998, the common law duty of confidence, and the General Medical Services contract. Further details are provided in Appendix 2.

[3] NHS Act 2006 s. 13S, inserted by the Health and Social Care Act 2012 s. 23(1)

PART 2 – Principles

4 Principles

The following statements of principle highlight the obligations on all GPs when offering access to online services. Supporting guidance is then provided on each of these areas.

Table 1 – Principles

Principles	**Guidance**
1. Practices that offer online access to their practice system should understand their responsibilities under the law to provide a secure and confidential service.	Section 3 & Appendix 2
2. Practices should have in place an Access Management Lead and named individuals responsible for access management, including oversight, identity verification, registration for services, authorising proxy access and incident management.	Section 5
3. Before access is given to an individual, the practice must verify that the applicant for online access is the person whose recorded identity will be associated with the user account issued to the applicant.	Section 6
4. The identity verification process should allow an individual to prove their identity in a straightforward way whilst also creating effective barriers to those trying to claim to be somebody they are not.	Section 6
5. Access should be managed with a consistent level of security, while providing flexibility to accommodate the needs of individuals and practices.	Sections 6 & 7
6. Patients should be clearly informed of, and formally acknowledge, the limits of the organisation's responsibility, and their responsibilities to keep their information secure.	Section 8
7. Arrangements must be put in place to ensure that system suppliers (data processors) are contractually bound to guarantee the security of the data held on behalf of their customers (data controllers).	Appendix 2

PART 3 – Guidance

5 Roles and Responsibilities

Practices should appoint an *Access Management Lead.* We recommend that the person nominated as the practice's Confidentiality Lead ("Caldicott Guardian") should take on the role of Access Management Lead. The Access Management Lead is responsible for

(a) overseeing the access management process
(b) leading the investigation of any incidents
(c) identifying which named individual(s) in the practice are authorised to conduct each of the tasks listed in Table 2.

Table 2 – Roles and Responsibilities

Authorised Roles	**Task**
Identity verification by presentation of documents	verify the identity of applicants by presentation of documents.
Identity verification by vouching	vouch for the identity of an applicant.
Registration for online services	register users on the system for access to online services.
Authorisation for additional online services (record access)	review applications for services in addition to appointment booking, repeat prescription and demographics. (Record access is not enabled by default, and requires a specific action on the system.)
Authorisation of proxy access	authorise applications by carers or other third parties.

Whilst one person may have more than one role in the process, registration on the system should be performed by someone other than the person verifying identity.

6 Identity verification

6.1 Rationale

The processes outlined here are intended to establish that the identity of an applicant for online services matches that of the individual registering with or registered at the practice and recorded on the GP system. They also apply to the verification of proxies, who with due authorisation may hold accounts allowing access to services on behalf of other patients, who need not themselves be registered for online services. A proxy is not necessarily registered at the practice as a patient.

Identity verification protects both patients and the practice from the consequences of fraudulent, accidental, or otherwise unauthorised access. To ensure that the practice can demonstrate that it meets its common law and statutory duties, it is important that the identity verification procedures are robust and that they are applied consistently.

This guidance is developed from guidance published by the Cabinet Office and CESG: *Identity Proofing and Verification of an Individual – Good Practice Guide No. 45 (GPG45)*[4]*.* The aims and stages of GPG45 are summarised in Appendix 4.

To accommodate the practicalities of verifying identities in a GP practice, the requirements presented in this guidance are designed to assure identities *as known at the practice*, and not necessarily real world identities. This is because, for example, document validity checks are not possible in the practice and vouching is based on personal knowledge only. For this reason, identities verified by practices in line with this guidance must not be used to support the registration of users for online services that are beyond the scope of the practice's responsibilities as a data controller.

6.2 Registered online service users

A "registered online service user" (ROSU) is the account on the practice system that gives access to patient online services. The identity of a ROSU applicant must be verified before credentials are issued, and this should be done in accordance with the processes outlined in section 6.4, regardless of the services requested.

6.3 Online self-registration

Some systems offer the ability for patients to register online for certain services without the need for identity verification. Where this functionality is available, the only service available at the practice is to book a non-urgent appointment. The account created in this context is not a "registered online service user" and cannot be updated to access other services.

[4] *Good Practice Guide No. 45 – Identity Proofing and Verification of an Individual* (issue no. 2.3, Cabinet Office and CESG 2014)

6.4 Identity verification process

Once a form requesting online access has been completed by a patient, the first step for the practice is to confirm the identity of the person making the request.

6.4.1 Options for identity verification

Broadly speaking, there are three ways of verifying the identity of a patient requesting online services:

1. Vouching (where an authorised person is satisfied that s/he knows the person well enough to verify their identity as recorded in the practice system).

2. Vouching with confirmation of information held in the applicant's records (where an authorised person does not know the person sufficiently well to vouch for them directly, but is able to do so by confirming information held in the applicant's records).

3. Presentation of documents (an authorised person checks that the documents provided by the patient are acceptable as evidence of their identity, and compares the applicant's face to their photo ID).

6.4.2 What to consider when choosing a method for identity verification

In selecting the most appropriate process to use for a particular patient, practices will need to assess:

1. Whether the applicant is known[5] to the practice (i.e., is registered and has a history of attendance);
2. Whether a member of staff authorised to vouch knows the applicant well enough to verify their identity;
3. Whether the applicant is able to provide evidence of identity from the list of acceptable documents;
4. Whether they already have access to any online services (e.g., appointment booking or repeat prescription requesting) and evidence of the identity verification that took place when this access was enabled.

6.4.3 Authorised roles

As described in section 6, practices will need to agree which members of staff are authorised to vouch for an individual's identity, verify identity by presentation of documents, and register patients for online access. See Table 2. Whilst one person may have more than one role in the process, registration on the system should be performed by someone other than the person verifying identity.

The names of the person approving access and the person performing registration should be recorded in the system against the registered online service user's account record.

[5] Whether the applicant is sufficiently "known" in the practice, or by a member of staff intending to vouch for them is a matter for professional judgement.

6.4.4 The application form

Each approach starts with the applicant filling in a form to request access. Example forms will be made available as downloads as part of the Patient Online Toolkit[6] being developed jointly by the Royal College of General Practitioners and NHS England.

Patients are asked to:

- Complete name and address details;
- Provide an email address and mobile phone number;
- Indicate which services they are applying to access;
- Read and sign an agreement to associated terms and conditions.

6.4.5 Details of the identity verification process

Once an application for online access has been completed, one of the following processes should be used to verify the applicant's identity before access is enabled:

1. Vouching
   a. the applicant attends the practice and meets a member of staff authorised to verify identity by vouching;
   b. the authorised person confirms that s/he knows the person well enough to verify their identity as known at the practice;
   c. the authorised person counter-signs the application form to confirm that this identity is known at the practice and recorded on the system.

2. Vouching with confirmation of information held in the applicant's records
   a. the applicant attends the practice and meets a member of staff authorised to verify identity by vouching;
   b. the authorised person poses questions to the applicant based on facts from the medical record;
   c. once satisfied, the authorised person counter-signs the application form to confirm that this identity is known at the practice and recorded on the system.

   Note: It is extremely important that the questions posed in this discussion do not inadvertently disclose confidential information to the applicant before their identity is verified. For example, the following would *not* be an appropriate question:

   > *"Please can you confirm when you were referred to the Improving Access to Psychological Therapies service?"*

   Instead, an appropriate question might be:

   > *"Please can you confirm when you last attended the practice and for what reason"*, followed by further non-disclosive questions about further details until the staff member is satisfied.

[6] http://elearning.rcgp.org.uk/patientonline

When using this option it is important for the authorised person to be particularly conscious of the risk of enabling fraudulent access through impersonation.

3. Presentation of documents
    a. the applicant attends the practice and meets a member of staff authorised to verify identity by presentation of documents;
    b. the applicant presents documents from the list of acceptable identity evidence in Appendix 3 (typically a passport or photo driving licence plus a bank statement). These documents must include at least one item of photo ID;
    c. the authorised person checks the documents for consistency and compares the applicant to the image on the photo ID;
    d. once satisfied, the authorised person counter-signs the application form to confirm that this identity is known at the practice and recorded on the system.

Appendix 3 sets out the requirements for presentation of documents, as defined by the Cabinet Office guidance, and lists the acceptable documents. In line with RCGP guidance[7] one of these should be a photo ID. A passport and a bank statement would, for example, be sufficient evidence.

Note that document validity checks are not practical in a GP practice setting and that authorised staff may not be familiar with some of the types of acceptable evidence. For these reasons, or where there is any cause of doubt, we recommend that verification be supplemented by confirmation of information held in the applicant's records, as described above.

It is important to ensure that the person submitting the application is the person with the verified identity, not just that the verified identity is known at the practice. This is the reason for the face-to-face meeting between the applicant and the member of staff that is required in order to verify the applicant's identity.

6.4.6 Recording of identity evidence

Once an identity has been verified, the information required by the practice system will be entered as part of the process of enabling access. The name of the person verifying the individual's identity, the method used, and the name of the person registering the individual on the system should all be recorded in the system.

6.4.7 Temporary residents

Feedback from those practices already offering online services suggests that it is usual to give online access only to permanent residents and not temporary patients/temporary residents. However, practices may consider it beneficial to offer appointment booking and repeat prescriptions to such patients, subject to the required identity checks. Note Section 6.3 regarding online self-registration for appointment booking purposes only.

[7] http://www.rcgp.org.uk/Clinical-and-research/Practice-management-resources/~/media/Files/Informatics/Health_Informatics_Enabling_Patient_Access.ashx

7 User registration processes

7.1 Local procedures

Practices should have clear procedures for the following business processes:

- Identity verification;
- Creation of registered online service user accounts and issuing credentials;
- Authorisation of proxy access.

The Access Management Lead is responsible for designing these processes, and for identifying the roles suggested in Section 5.

Practices may choose to offer online services to patients registering with the practice for the first time and thereby reduce the need for additional administration.

7.2 Registration of online service users and issuing credentials

A registered online service user (the user account) can be created at any time following the presentation of a completed application form and a signed Terms and Conditions declaration. The account may be activated and credentials issued only when the identity verification process has been completed.

Account credentials may be printed to give to the user, or sent to a verified e-mail or mobile phone.

8 Account security and user responsibilities

Applicants for online services should sign a declaration agreeing to Terms and Conditions (T&Cs) as part of the registration service. T&Cs should include the following:

- that the user is responsible for the security of information viewed or downloaded;
- that sharing of information by the user with anyone else is at the user's risk;
- that the user will contact the practice as soon as possible should there be a suspicion that their account has been accessed without authorisation;
- the user will log out and contact the practice as soon as possible should they access information about anyone other than themselves or a patient for whom they are an authorised proxy.

Practices should provide or direct users to advice on keeping their accounts secure. An excellent Guide on this has been has been produced by the BCS, the Chartered Institute for IT, and the Department of Health[8].

[8] *Keeping your online health and social care records safe and secure* (Department of Health 2012), available at http://www.bcs.org/upload/pdf/guidance-health-and-socal-records.pdf

9 Managing information security incidents

The practice should have an established procedure for the management of security incidents relating to online user accounts, including nominated responsibilities for practice staff. A suggested template for such a procedure is given in Appendix 5.

PART 4 – Appendices

Appendix 1 – Definitions

Table 3 – Definitions

Authentication	User access to the system using secure credentials and management of these credentials (e.g., password reset).
Assured Identity	A claimed identity that is linked to an applicant with a defined level of confidence that it is the applicant's real identity.
Claimed Identity	A declaration by the applicant of their current name, date of birth and address.
Identity Verification	A way of confirming whether the applicant is the owner of a claimed identity (i.e., is who they say they are).
Proxy access	Access by third parties such as parents of non-competent children, carers or others acting on behalf of a patient.
Registration of online service users	Creation of a Registered Online Service User on the practice system.
Registration for additional online services	Approval and enablement of access to online services in addition to the default enabled on registration as an online service user. These additional services include viewing clinical records.
Vouching	Verification by an authorised person that an identity claimed by an applicant is the identity of the individual known at the practice and recorded on the practice computer system.

Appendix 2 – Legal and contractual requirements

This section describes the main legal and contractual requirements for GPs in their delivery of online services.

The common law duty of confidence

The common law duty of confidence requires that where there is an established expectation of confidentiality between parties, for example a health professional and a patient, information imparted by the subject will not be further disclosed by the recipient without the consent of the subject. The duty is not absolute and information may be disclosed without consent where it is required or permitted by law, or in exceptional circumstances where the public interest outweighs the individual's right to confidentiality.

In the context of online access to information or services, the legal justification for granting access to anyone other than the data subject requires that, where necessary, appropriate consent should be obtained for the enablement of any service that involves disclosure of information to someone other than the subject – e.g. proxy access.

Where consent is not obtained for the enablement of such a service, it is important to establish the legal basis for the disclosure, for example where a parent requests access to the records of a child who is not competent[9] in respect of the decision, or where a carer or other third party requests access to the records of an adult who may lack capacity.

The Data Protection Act 1998

GP practices are Data Controllers under the Data Protection Act 1998. As such, they must comply with the principles and other requirements of the Act in their use and disclosure of information. Particularly important in relation to identity management and the enablement of online access are:

- The First Principle: that personal data must be processed fairly and lawfully;
- The Fourth Principle: that personal data must be accurate and, where necessary, kept up to date;
- The Seventh Principle: that personal data must be processed securely and that both technical and organisational measures must be in place to achieve this requirement.

To meet the First Principle requirements, the purposes for which personal data are to be used must be transparent, processing must not be outside reasonable expectations of the subjects, and must not cause unwarranted detriment. The common law duty of confidence and other relevant laws must be respected. Further conditions are specified, including for the use and disclosure of "sensitive data". In the context of online access, where access is to be given to someone other than the

[9] In line with the Fraser guidelines established in *Gillick v West Norfolk & Wisbech Area Health Authority* [1985] UKHL 7 (17 October 1985), and reinforced by *Axon v Secretary of State for Health* [2006] EWHC 37 (Admin), (Axon).

subject, “explicit consent” is the most applicable condition, complementing the common law requirement.

The Fourth Principle is particularly important in the identity verification and registration process. It is essential that online accounts are associated with the correct individual on the system, and that personal details are recorded accurately and kept up to date.

To meet the Seventh Principle it is necessary that systems holding personal data are both technically secure, and that the Data Controller has in place organisational measures to ensure that the data is managed securely. These should include business processes, operational procedures and provisions for staff training and awareness.

The General Medical Services Contract

GPs are required under their contract[10] to comply with all relevant legislation and also to have regard to the *Good Practice Guidelines for General Practice Electronic Records*[11]. They are also required to nominate a person with responsibility for practices and procedures relating to the confidentiality of the personal data they hold. This person is instrumental in implementing procedures locally to perform the functions described below.

The contract also requires that practice computer systems holding patient records are accredited in accordance with the HSCIC GPSoC assurance process[12] before NHS England gives permission for their use. Compliance with this supports Data Processor requirements.

Assurance by system suppliers as Data Processors

Where an organisation makes use of IT services hosted by a third party (a Data Processor), under the Data Protection Act responsibility for the security of the data remains entirely with the Data Controller. To meet this responsibility, there must be a contractual arrangement in place that requires the Data Processor to act only on the instructions of the Data Controller, and binds them to ensuring the security of the data in accordance with the Seventh Principle of the Act.

In the context of hosted GP systems, this requirement is met by the GPSoC-R contract, which requires suppliers to sign a deed of undertaking in a form prescribed by the Health and Social Care Information Centre. This provides direct contractual assurances to practices as Data Controllers that the supplier will comply with data processing conditions specified in the contract.

[10] Standard General Medical Services Contract, section 16

[11] *Good Practice Guidelines for General Practice Electronic Records* (Version 4, Department of Health 2011), available at https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011

[12] HSCIC GPSoC Common Assurance Process (GPSoC CAP). Information on this can be found at http://systems.hscic.gov.uk/gpsoc/interface/assurance

Appendix 3 – Acceptable identity evidence

Based on the requirements of GPG45, the options for presentation of documents are as follows:

- *Two pieces of Level 3 evidence*; or
- *One piece of Level 3 evidence and one piece of Level 2 evidence*

from the acceptable identity evidence listed in table 4. In either case, one piece of evidence must include a photograph.

Table 4 – acceptable identity evidence

Level 2 Identity Evidence	Level 3 Identity Evidence
• Firearm Certificate • DBS Enhanced Disclosure Certificate • HMG issued convention travel document • HMG issued stateless person document • HMG issued certificate of travel • HMG issued certificate of identity • Birth certificate • Adoption certificate • UK asylum seekers Application Registration Card (ARC) • Unsecured personal loan account (excluding pay day loans) • National 60+ bus pass • An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level) • An education certificate gained from a well recognised higher educational institution • Residential property rental or purchase agreement • Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number) • Police warrant card • Freedom pass • Marriage certificate • Fire brigade ID card • Non bank savings account • Mobile telephone contract account • Buildings insurance • Contents insurance • Vehicle insurance	• Passports that comply with ICAO 9303 (Machine Readable Travel Documents) • EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004 • Northern Ireland Voters Card • US passport card • Retail bank/credit union/building society current account • Student loan account • Bank credit account (credit card) • Non-bank credit account (including credit/store/charge cards) • Bank savings account • Buy to let mortgage account • Digital tachograph card • Armed Forces ID card • Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number) • Secured loan account (including hire purchase) • Mortgage account • EEA/EU full driving licences that comply with European Directive 2006/126/EC

Appendix 4 – GPG45 aims and stages

The aims of identity verification as defined by GPG45 are:

- to confirm that the applicant's *claimed identity* exists in the real world,
- that the applicant is the owner of the identity:
- that it is genuine.

At the end of the process, the claimed identity becomes an *assured identity* that may be used with confidence to enable online services for the applicant.

The stages of identity proofing and verification given in GPG45 may be summarised as follows:

1. The applicant is required to declare their full name, date of birth and address so there is no ambiguity about the claimed identity;
2. The applicant is required to provide evidence that the claimed identity exists;
3. The evidence is checked to confirm that it is genuine and valid (validation);
4. The applicant is compared to the evidence about the claimed identity to determine whether it relates to them (verification);
5. The claimed identity is subjected to checks to determine whether it has had an existence in the real world over a period of time (activity history);
6. The claimed identity is checked to ensure that that it is not a known fraudulent identity and to help protect individuals who have been victims of identity theft (counter-fraud checks).

Independent counter-fraud checks are neither practical, nor relevant to registration of applicants for online services by GP practices. It is also impractical to for practices to establish processes for the validation of identity documents (e.g., by comparison with information held or published by the issuing/authoritative source, or by trained staff confirming that they are genuine).

Consequently, approaches to assuring locally known rather than real world identities are described in section 6 of this document.

Appendix 5 – Incident Management Checklist

The *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (SIRI)*[13] gives guidance on the management, investigation and reporting of Serious Incidents Requiring Investigation (SIRIs) including a methodology for assessing severity, and reporting requirements based on severity.

The guidance defines a Serious Incident Requiring Investigation (SIRI) as any incident that involves an actual or potential failure to meet the requirements of the Data Protection Act 1998 or the common law duty of confidence, including the unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches, and inappropriate invasion of people's privacy. Such personal data breaches could lead to identity fraud or have other significant impact on individuals. These rules are irrespective of the media involved and include both electronic media and paper records.

Under this definition, suspected unauthorised access to an online user's account, or confidential data produced from it constitutes a SIRI. Practices should have measures in place to ensure an appropriate and consistent response should such an incident be reported. The lead responsibility for the management of responses to a suspected information security incident is the Confidentiality Lead. Table 5 outlines the steps involved in handling such an incident.

Table 5 – Steps involved in investigating a SIRI

Steps	**Details**
Detection and reporting	All staff should understand the necessity for investigating reported or suspected breaches of information security. There should always be someone available to the practice that is authorised to assess the incident and decide whether to initiate the immediate response. There should always be someone available to the practice with user privileges to disable online user accounts.
Assessment and decision	A decision should be made immediately on whether the report could constitute an abuse of an account warranting disabling the account.
Immediate response	1. Disable the account. 2. Ask the user to retain any evidence they have that the account has accessed inappropriately or otherwise abused – e.g. access messages sent to e-mail. 3. Make a record of the reasons why the user believes that the

[13] *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (SIRI)* (version 4.0, HSCIC 2014), or later version

	account has been abused.
Investigation	1. Generate audit trails of access to the account. 2. Confidentiality Lead to review audit trails to identify potential evidence of abuse with reference to the user's concerns. 3. Invite the patient to meet the Confidentiality Lead to review audit trails and other evidence, and to consider any other factors such as user password strength and security. 4. Establish the immediate and root cause of the incident. 5. Consider any wider implications for the technical security of the system and business processes in the practice.
Incident response	Consider actions needed to prevent recurrence of this incident including: 1. Advice to the user on account security; 2. Revisions to the business processes at the practice; 3. If there is suspicion that this is a technical breach, raise this concern with the supplier contract manager.
Assess severity level	Assess the severity of the incident in line with *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (IG SIRI)*
Report the incident	If the incident is assessed as being a level 2 SIRI, it should be reported in accordance with the Checklist Guidance.

All organisations processing health and adult social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the Department of Health, to the Information Commissioner's Office.

Appendix 6 - Equality statement

Equality and diversity are at the heart of NHS England’s values. Throughout the development of the policies and processes cited in this document, we have given due regard to the need to:

- Reduce health inequalities in access and outcomes of healthcare services integrate services where this might reduce health inequalities
- Eliminate discrimination, harassment and victimisation
- Advance equality of opportunity and foster good relations between people who share a relevant protected characteristic (as cited in under the Equality Act 2010) and those who do not share it.”