

GP Online Services Guidance

*Coercion*

Contents

1. Introduction 1
2. The context in which coercion occurs 2
3. Coercive control 2
4. Online record access for young people 3
5. Identifying coercion in Primary Care 4
6. What can practices do when coercion is suspected? 4
7. Proxy access and coercion 7
8. Summary 7
9. Flowchart – Identifying and dealing with coercion 8

Introduction

‘Coercion’ is the act of persuading someone to do something against their will by force or threats.

Online services of all types are vulnerable to coercion. If the victim of coercion has online access to their GP data, they may be forced to share their login credentials, giving their abuser access to their medical history, consultation records, repeat prescription, appointment booking details and other private, personal information. This may allow the abuser to discover evidence that the patient has reported that they are being abused or enable them to completely control the patient’s access to healthcare. Information in the record may lead to the patient suffering an escalation of violence from their abuser.

Practices have processes in place to manage instances of suspected coercion related to paper-based and face-to-face services.

The purpose of this guidance is to review the context in which coercion may be applied to patients who have online access to GP Online Services and to help practices minimise the harm that patients may suffer if coerced to share their access.

Ref: RCGP Safeguarding Toolkit - https://www.rcgp.org.uk/clinical-and-research/safeguarding.aspx (accessed 6 July 2022)

Ref: Helen Bamber Foundation: Quick Guide to Modern Slavery and Human Trafficking - https://elearning.rcgp.org.uk/pluginfile.php/170658/mod\_book/chapter/347/QUICK%20GUIDE%20TO%20MODERN%20SLAVERY%20AND%20HUMAN%20TRAFFICKING%20Final.pdf (accessed 30 March 2022)

The context in which coercion occurs

All practice staff must be aware of the potential impact of coercion and the indications to look out for in order to help patients who might be subject to coercion.

Coercion often, although not always, occurs in the context of abuse. In England and Wales at least 29.9% of women and 17% of men will experience domestic abuse in their lifetime and every year an estimated 2 million adults experience some form of domestic abuse.

Coercion to share or misuse of online access is most likely to happen if the patient is a child, an adult in an abusive situation, a patient with a learning disability or cognitive impairment, those who are elderly, or patients who are otherwise vulnerable such as those with severe mental health or substance misuse issues.

There will be instances where patients are persuaded without force or threats to share their access to their GP Online Services with someone who, unknown to them, does not have their best interests at heart. They may share their login details or by asking the practice to give the third-party proxy access with their own login details (see the section on proxy access below).

Patients who do not have capacity to understand the implications of their decision are particularly at risk of sharing their access willingly without realising the dangers. Alternatively, patients who have capacity, may have never been given the right information about the risks and benefits to be able to make an informed decision. They may share their login details to their online account or they may ask the practice to give the third party their own login details. This is called **Proxy access** (see below). Practices should be carefully assess the risk that someone asking for proxy access is wishing to control or harm the patient. For example:

* parents who are concerned about their child's welfare or who want to support their child with healthcare may persuade their child into sharing their record, but this could later prevent a young person accessing healthcare confidentially due to fear of their parents finding out
* adult family members wishing to support the health and wellbeing of an elderly relative with dementia may persuade them into sharing their record, but this could lead to family members finding out confidential information that the elderly person would not have chosen to disclose to their family.

Ref: There is more information about proxy access in the Record Access section of the Toolkit.

Coercive control

This is central to many types of abuse.

“Coercive control is an act or pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim. This controlling behaviour is designed to make a person dependent by isolating them from support, exploiting them, depriving them of independence and regulating their everyday behaviour.”

Ref: “What is coercive control”, Women’s Aid - <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/> (accessed on 30 March 2022)

Examples of coercive control:

* Isolating someone from friends and family
* Depriving someone of basic needs such as food
* Monitoring someone’s time
* Monitoring someone via online communication tools or spyware
* Taking control over aspects of someone’s everyday life, such as where they can go, who they can see, what they can wear and when they can sleep
* Depriving someone of access to support services, such as medical services
* Repeatedly putting someone down, such as saying they are worthless
* Humiliating, degrading or dehumanising someone
* Controlling someone’s finances
* Making threats or intimidating someone

Perpetrators of domestic abuse often use a variety of online tools, of which online record access is just one, to abuse their victims.

Ref: Women’s Aid, Online and digital abuse - https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/ (accessed 10 March 2022)

Ref: UK Parliament, rapid response - <https://post.parliament.uk/technology-and-domestic-abuse/> (accessed 10 March 2022)

Online record access for young people

Automatic record access is switched on for young people when they reach their 16th birthday if they who have a patient facing services account for requesting repeat prescriptions or booking appointments. They may not be expecting this to happen but may then be subject to coercion to share their online. If it suspected that a young person will be at risk of abuse, consider if it would be appropriate to add the SNOMED CT term *Enhanced review indicated before granting access to own health record* (1364731000000104) to their record before their 16th birthday. This will prevent record access being switched on automatically on their birthday or if they get an NHS Login in the future.

Ref: There is more information about how to prevent future automatic record access below and in the Toolkit in “SNOMED CT Terms that Control Automatic Record Access”.

Reviewing their access to GP Online Services when someone reaches 16 years provides an opportunity to discuss your suspicions with them and make a shared decision about whether to block online record access while they are at risk. If the risk resolves, you may override the blocking “…104” term in the record by adding the SNOMED CT term *Enhanced review indicated before granting access to own health record* (1364731000000106). You can then switch on record access, if they request it, using the GP Online Services controls in the practice computer system.

Ref: There is more detailed guidance on the issues discussed in this section in the Toolkit in the guidance on “Children and Young People” and “Safeguarding Vulnerable Groups” documents.

Identifying coercion in Primary Care

**Everyone in the practice team should understand and know how to identify coercion and coercive control and be vigilant in its detection in order to provide support and protection to patients at risk. They should also be able to provide the relevant information to patients, so that they can make informed decisions for themselves, unless there is evidence that they do not have capacity to do so.**

Below are some examples of how coercion and coercive control may become apparent in a Primary Care setting. This is not an exhaustive list, nor are these indicators always a sign of coercive control. On their own, these examples below are not conclusive indications that the patient is a victim of coercive control. There may be valid non-abusive reasons for these circumstances to arise. A parent may reasonably attend appointments with their children; a family member may attend with their relative to pass on their concerns about their relative. However these signs should lead staff to consider whether the patient could be a victim of abuse and coercive control, especially if several of these behaviours are witnessed or there are already suspicions of abuse.

* The patient is always accompanied to an appointment
* A third-party always speaks for the patient
* The practice receives communications about a patient from a third-party, especially communications which attempt to undermine the patient in some way
* A third-party is demanding full or proxy access to the patient's record
* A third-party contacts the practice to know why the patient’s online access has been blocked, switched off or online access has not been given or why consultations or documents are hidden from online access
* The patient always has to check with a third-party before they agree to anything

Ref: for further reading about how to raise issues of abuse with patients in SafeLives’ “General Practitioner (GP) Profile” - https://safelives.org.uk/GP-pathfinder-profile (accessed 7 July 2022)

What can practices do when coercion is suspected?

If a patient is identified or suspected to be a victim of abuse or coercive control, online record access places them at risk. Management of the patient’s risk from coercive control should include discussions with the patient about record access. It is important to assess whether record access may become a tool of abuse in the hand of their abuser and whether the patient can have online record access safely.

1. Seek evidence of coercive control

**In the first instance you might ask a specific question to open the discussion about record access and the issue of coercion such as “Is it possible that you may come under pressure to give someone access to your personal health record on your phone, tablet or computer against your will?**”

The statements in box below should be included in a registration form for patients requesting online services for the first time (a template for a new application form is available in the Toolkit). Patients should understand and tick all six statements in the template application form before access is granted. The questions may also be used as an open a discussion about coercion and record access.

These questions may lead to disclosure of abuse or coercive control and every discussion of this sort should be carried out sensitively, in a trauma-informed way and in private with the patient alone. The discussion should be led by a practice team member with the appropriate level of safeguarding training such as Level 3 Child and Adult Safeguarding Training. Usual safeguarding procedures should be followed.

Recommended statements that patients may be asked to agree to, for inclusion in registration forms for access to GP Online Services

1. I have read and understood the information leaflet provided by the practice
2. I understand how to keep my online GP services and the information they contain about me secure
3. If I choose to share my information with anyone else, this is at my own risk
4. If I suspect that my account has been accessed by someone without my agreement, I will contact the practice as soon as possible
5. If I see information in my record that is not about me or is inaccurate, I will contact the practice as soon as possible
6. If I think that I may come under pressure to give access to someone else unwillingly, I will contact the practice as soon as possible.

If the patient struggles to agree with any of these statements or raises any concerns, recommend that the patient makes an appointment with an appointed person in the practice to discuss their concerns before signing them up for GP online services. You can include the statements in an application form.

 Ref: Intercollegiate document, hosted by Royal College of Nursing, Safeguarding Children and Young People: How to Identify and Escalate Concerns - https://www.rcn.org.uk/magazines/Students/2019/Safeguarding-children-how-to-identify-and-escalate-concerns-advice-for-student-nurses (accessed 10 August 2022)

Ref: Intercollegiate document, hosted by Royal College of Nursing, Adult Safeguarding: Roles and Competencies for Health Care Staff - <https://www.rcn.org.uk/Professional-Development/publications/adult-safeguarding-roles-and-competencies-for-health-care-staff-uk-pub-007-069> (accessed 10 August 2022)

Ref: There is a template application form practice use for GP online prescription, appointments or record access services in the Toolkit.

2. Review the record for potentially harmful information

The patient’s record may contain information that may lead to harm to the patient if an abuser comes into possession of it. It may be possible to enable record access for the patient if you are confident that any such information is not visible to the patient online and that any future potentially harmful information will be redacted (or hidden from view online) as it is added to the record. However if it may be possible that harmful information may become visible online, it may be necessary to block, switch off or limit record access.

Ref: There is more information about “Managing Potentially Harmful Information” in the Toolkit.

3. Refuse or limit online record access

You should choose to block, switch off or limit the scope of record access to patients who may be at risk of coercion to allow time for individualised discussions to take place with the patient and a joint decision to be made about what level of record access would be in the patient’s best interests.

If the patient does not have online record access you can block future access by this route by entering a SNOMED CT term in their record: *Enhanced review indicated before granting access to own health record* (1364731000000104). If the patient already has record access, the GP Online Services settings in the general practice’s computer settings need to be changed to reduce or switch off record access.

Ref: There is more information about how to prevent automatic record access in the guidance on using “SNOMED Terms that Control Automatic Record Access” in the Toolkit.

You should be mindful of patients who may face difficulty in reading or understanding written information about GP Online Services because of poor literacy, poor comprehension or ability to speak or read English, or low intellectual capacity. Practices will need to ensure that the information given to these patients is accessible, given in a way that they understand, for example - reading out loud for them or using a formal interpreting service.

Practices also need to be mindful that a patient may not recognise that they are currently in an abusive relationship or situation.

The purpose of the discussions about online services is to come to a decision about how record access can be made safe for the patient and whether in their individual circumstances the benefits outweigh the risks. It may be necessary to avoid record access entirely or it may be possible to switch on limited record access, just the detailed coded record perhaps or it may be possible to switch on full record access but agree to redact certain potentially harmful information from view by the patient.

The risks from online record access and how to manage them should be understood by the whole practice team, should be part of routine practice training and included in the practice safeguarding policy.

Ref: There is a lot more information on safe record access in the “Managing Potentially Harmful Information” guidance in the Toolkit

Ref: There is information for patients about online safety from SafeLives - https://safelives.org.uk/tech-vs-abuse

Proxy access and coercion

Patients may choose to share their NHS login credentials with trusted family, friends and carers (including staff in a care home). They can do this by sharing their personal login details but it is far safer if the trusted third-party (called the patient’s proxy) is given their own online account to access the patient’s record by the practice (this is called proxy access).

Advantages of formal proxy access are that

* The practice will be aware that a third-party has access to the patient’s record and can limit the level of access that the proxy is given, neither of which are likely if the patient shares their own login details.
* The application process creates the opportunity to seek evidence of coercion and advise the patient of the risks of shared record access.
* It easier for the practice to switch off or limit the proxy’s access in the future if suspicion later develops that the proxy is acting against the patient’s best interests.

In some circumstances such as early dementia or end of life care it may be appropriate to obtain the patient’s consent to future proxy access when they are no longer able to manage their health record and record the patient’s consent in an advance directive. This may be part of an advanced directive and may be part of a discussion about lasting powers of attorney. The possibility of coercion should still be considered when eventually proxy access is switched on in these circumstances.

It is important to record the discussions with the patient and the outcome in the patient’s record.

Ref: Proxy access is considered in more detail in the “Proxy Access” guidance and the clinical guidance for “End of Life Care” and “Dementia” in the Toolkit.

Summary

If anyone in the practice team, GPs, nurses or non-clinical staff, has any suspicions that a patient is being coerced into sharing their online record, that patient should not be registered for any GP Online Services or their record access should be switched off and/or blocked until the suspicion is explored and an informed decision can be made jointly between the practice and the patient as part of the patient’s management of the wider risks to the patient.

If any staff member has concerns and are not sure what to do, they should seek advice from their Practice Safeguarding Lead/Caldicott Guardian/information Governance Leads.

No risk

Risk

confirmed

Risk

confirmed

Risk

confirmed

If coercion is possible, suspected or proven, the practice should decline record access, and explore safeguarding risks.

If coercion is possible, suspected or proven, the practice should consider switch off or limiting record access, explaining the reason to the patient.

**Identifying and dealing with coercion**

No risk

No risk

**START**

Patient requests
access to their
record online

Patient has online
 record access and a suspicion of abuse arises

Assess the patient’s risk of coercion using the six questions in the RCGP
application form

Assess the patient’s risk of coercion in the usual way. Consider blocking or switching off record access to allow time for
the assessment

Patient completes identity
verification and the records are reviewed to redact potentially harmful data and identify
evidence of a risk to the
 patient from record access

Record access approved, patient sign up completed and identity verification evidence recorded in the patient’s record

If the risk of coercion is low, switch record access back on or continue with current access. Inform patient that potentially harmful selected information may
be hidden from their online view