Royal College of General Practitioners

GP Online Services Guidance

Coercion

Contents

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 Online Services, 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 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 should have processes in place to manage instances of suspected coercion related to the services they provide.

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

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 a 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 more 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 GP Online Services with someone who doesn't have their best intentions at heart. They may do this by sharing the login details to their online account or by asking the practice to give the third party their own login details. This is called **Proxy access** (see below).

Patients who do not have capacity to understand the implications of their decision may share their access willingly without understanding the risks. 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. 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.

Coercive control

Central to many types of abuse is coercive control.

"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 GP Online Services 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

If a young person is experiencing coercive control it is important to reaslise that access to records is automatically enabled for young people who have their own account for GP Online Services when they reach their 16th birthday. If it is suspected that a young person is 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 set up an account in the future.

Reviewing GP Online Access when someone approaches 16 provides an opportunity to discuss any suspicions with the young person and make a shared decision about if access is appropriate. Should they no longer be at risk, consider if it would be appropriate to add the SNOMED CT term term *Enhanced review indicated before granting access to own health record* (1364731000000106). Ref: Using Enhanced Review (SNOMED) codes when giving a patient access to their health record. https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/using-enhancedreview-snomed-codes-when-giving-a-patient-access-to-their-health-record
Ref: There is more detailed guidance on the issues discussed in this section in the GP Online Services Toolkit in the guidance on "Children and Young People".

Identifying coercion in Primary Care

All staff should understand and know how to identify coercion and coercive control and be vigilant in its detection in order to provide support and protection for patients who are at risk. They also need to 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 or evidence that they are making decisions under duress or coercion.

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. 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.

On their own, these examples below are not conclusive indications that the patient is a victim of coercive control. There are some signs that 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. Some signs such as:

- 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 attempts 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 SafeLives, - General Practitioner (GP) Profile - https://safelives.org.uk/GP-pathfinder-profile (Accessed 6 April 2022)

What can practices do when coercion is suspected?

If a patient is identified or suspected of being a victim of abuse or coercive control, access to GP Online Services may place 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 online record access may become a tool of abuse in the hands 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 need to understand and tick all six statements in the template application form before access is granted. They may also be used as an opening question 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 GP Online 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: Roles and Competencies for Healthcare Staff - https://www.rcn.org.uk/professional-development/publications/pub-007366 (accessed 30 March 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/pub-007069 (accessed 30 March 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, it may be possible that harmful information may become visible online, it may be necessary to block, switch off or limit record access.

3. Refuse or limit online record access

You may choose to, switch off or limit the scope of record access to patients who may be at risk 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 prevent future access being automatically given by entering a Systemized Nomenclature of Medicine – Clinical Terms (SNOMED CT) code 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 GP computer settings need to be changed to reduce or switch off record access.

Ref: Using Enhanced Review (SNOMED) codes when giving a patient access to their health record. https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/using-enhanced-reviewsnomed-codes-when-giving-a-patient-access-to-their-health-record.

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 disable some services 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 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 should be discouraged from doing this by sharing their personal login details as it is far safer if the 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).

Providing proxy access means that the practice will be aware that a third-party has access to the 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 also creates an opportunity to discover

evidence of coercion and advise the patient of the risks of shared record access. Proxy access makes 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. It is important to record the discussions with the patient and the outcome in the patient's record.

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.

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, 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 is not sure what to do, they should seek advice from their Practice Safeguarding Lead/Caldicott Guardian/information Governance Leads.

Identifying and dealing with coercion

START

Patient requests access to their record online

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

No risk → 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

No risk → Record access approved, patient sign up completed and identity verification evidence recorded in the patient's record

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

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

Patient has online record access and a suspicion of abuse arises

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

No risk → 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

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