

GP Online Services Guidance

*Online GP record access for other sectors*

Who is this guidance for:

* Sectors working with victims and survivors of abuse, including domestic abuse, trafficking, modern slavery and exploitation.
* Those with strategic responsibility for safeguarding in primary care (e.g. Named GPs/Nurses and Designated Health Professionals for Safeguarding) who should consider sharing this document with their local partner agencies.

Purpose of this guidance

To highlight automatic record access to GP records, the risks it may present to victims and survivors of abuse, and how they can be reduced.

Background

In England, patients have been able to have online access to their GP record for many years to order prescriptions, book appointments and see information such as test results and letters. There are many benefits to this as patients can be much more involved in their own healthcare.

To increase the proportion of the population with record access, automatic record access to GP data will be enabled. Every citizen aged 16 years and over who have an online account to access GP services (also called patient facing services) automatically has free and full access to all new entries on their GP record – as well as letters, test results and medications prescribed, this will include all consultations (which means everything that a health professional records in the patient record following any consultation).

Citizens use their smartphone, tablet or computer to access apps and web portals such the NHS App, Airmid, Evergreen Life and Patient Access that offer patient facing services, including GP online services. Patients who have used their access to book appointments or request prescriptions now have access to all new information added to their GP record, whether they want it or not. If they are worried about being unable to keep their record secure, they have to apply to their practice to switch off their individual record access. NHS England plans to include historical records in 2023.

Before automatic record access was enabled, patients had to apply to their practices to obtain online access to their record. This gave their GP an opportunity to check if the patient was at a safeguarding risk related to coercion to share their record access. They could review the record for signs of abuse and talk to the patient about keeping their record secure before deciding whether it was safe to switch on record access. With automatic record access via an NHS Login patients need not apply to the practice and so the safety net of clinical assessment of the safety of online record access for individual patients will be lost.

GP records hold a vast amount of safeguarding relevant information, from personal disclosures by patients of their experience of abuse to information about perpetrators of abuse and criminal records. The records also contain a significant amount of information from other organisations such as the police, social care and education services which could potentially be harmful in the hands of perpetrators of abuse. Multi-agency information often also contains large amounts of third-party information.

In addition, GP records contain lots of information about issues such as mental health, contraception, sexual health including HIV (human immunodeficiency virus), pregnancy, terminations and gender identity which could be dangerous in the hands of an abuser who has coerced the patient to give them access to their online record.

It is very hard for a victim to keep their online record secure and private within a coercive relationship (which can be between intimate partners, family members, friends, peer groups, and in the context of trafficking, modern slavery, criminal and sexual exploitation for example). The record is only protected by usernames and passwords, it is not necessary to use biometric data to access the GP record. Anyone who can use someone else’s NHS login, or coerce the patient to share their phone, tablet or computer screen once they have logged in to record access, can see the patient’s record.

There are also groups of patients who have a particular fear of authority and how authorities may want to access their online record, such as refugees and those whose immigration status is uncertain.

Victims and survivors of abuse may be deterred from seeking healthcare when they need it because of a fear that health records are no longer confidential.

Ways in which online access to GP records can be used as a tool for abuse by perpetrators:

* To see that their victim has accessed healthcare for any reason e.g. a victim has come to a GP for contraception when their perpetrator has told them they can't be on contraception
* To see what their victim has told the clinician in a consultation e.g. a victim discloses abuse
* Perpetrators may be able to infer that their victim has disclosed abuse if a consultation has been hidden from online viewing
* Perpetrators may become aware through information in their own record, or in their children's records, that their victim has disclosed abuse.

Perpetrators could be able to see this information by a variety of means for example:

* Coercing the victim into sharing their login details and record
* Sharing the same electronic devices as the victim
* Setting up online access without the victim even being aware

This can have the following impact:

* The victim is placed at an increased risk of harm from their perpetrator as 'punishment' for disclosing abuse. In high-risk abuse situations, this could mean an increased risk of severe violence or even death. This risk may also apply to any children in the situation – increased risk to an adult victim can also mean an increased risk to their children.
* The victim may be prevented from accessing healthcare at all, or the perpetrator will always attend with them.
* The victim no longer feels safe to disclose abuse to a healthcare professional therefore doesn't receive the help, support and protection they should have.
* The victim no longer sees healthcare settings as safe places and so does not seek help for any health issue which could result in poorer health outcomes.

How can the risks be reduced?

GP practices have two methods of protecting patients from safeguarding risks linked to the information in their health records.

1. Redact potentially harmful or confidential third-party information from view online. This is known as redaction. It does not redact the information from view by other healthcare professionals providing direct care to the patient or from reports provided by the practice.
2. Block or switch off a patient’s online record access and wider online services, but this can itself alert a perpetrator that their abuse has been discovered.

Organisations supporting victims and survivors of abuse can also help to reduce the risks by being aware of automatic record access and having discussions about it. Organisations may wish to add the following questions to their usual conversations and assessments with victims and survivors:

* Do you have access to your online GP record or GP Online Services via the NHS App or similar?
* Does anyone else have access to your online GP record?
* Has anyone ever asked you to allow them to access your online GP record?
* Are you worried that someone might already have access to your online GP record?
* Are you worried that someone might demand access to your online GP record in future?

If there is any concern that someone is being coerced into allowing access to their online GP services or that another person or persons already have access, consider advising them to:

* Contact their practice immediately to make them aware of these concerns and request a further discussion.
* Ask the practice to switch off their online services access. This could just be a temporary measure until such time as a conversation can take place between the patient and the practice about the concerns and how best to manage the safety of their online record. Remember that the act of switching off online record access can itself alert a perpetrator that their abuse has been discovered.
* Change their password or log in credentials, but the perpetrator may be able to coerce their victim to share the new password/log in credentials.
* Delete their NHS Login if they use one to access GP online services.