Handling of personal information: emergency access in the My Health Record system

A privacy assessment of 300 General Practice (GP) clinics and retail pharmacies.

31 May 2024

Contents

Part 1: Executive summary

The Office of the Australian Information Commissioner (OAIC) conducted a privacy assessment of the use of the My Health Record emergency access function by 150 general practice (GP) clinics and 150 retail pharmacies.[1] This assessment considered privacy risks related to the following Australian Privacy Principles (APPs):

- APP 1.2 – taking reasonable steps to comply with the APPs, particularly APPs 6[2] and 11.1
- APP 11.1 – security of personal information.

The emergency access function enables healthcare providers to override patients' My Health Record access controls (i.e. a record access code). It allows health care providers to view the My Health Record, including any restricted information or documents, without the patient's consent.

This function is designed to be used under section 64 of the *My Health Records Act 2012* (Cth) (MHR Act). Section 64 authorises healthcare providers to collect, use and disclose My Health Record health information where they reasonably believe that:

- it is necessary to lessen or prevent a serious threat to an individual, it is unreasonable or impracticable to obtain the healthcare recipient's consent, or
- it is necessary to lessen or prevent a serious threat to public health or safety.

Assessment participants were surveyed about their use (including potential misuse) and governance of the emergency access function. Upon completion of the survey, assessment respondents received general guidance about their My Health Record emergency access obligations, feedback regarding potential risks identified in their responses, and guidance for addressing these risks. The assessment methodology is set out in Part 4.

Overall, the assessment found that there was a lack of oversight, governance and awareness of the emergency access function in healthcare provider organisations. For example, 65% of survey respondents were apparently unaware that the emergency access function was used in their organisation in 2022. This may have also affected the reliability of some survey responses.

The assessment identified the following areas of good privacy practice:

- **Prevention** – most survey respondents had at least two measures in place to prevent, identify and address potential misuse of the emergency access function.
- **Reporting** – most survey respondents were aware that misuse of the emergency access function must be reported to the Australian Digital Health Authority (ADHA) and OAIC.
- **Reasons for access** – when outlining their reasons for using the emergency access function, only 14 survey respondents (5%) failed to provide any authorised reasons for access under the MHR Act.

Areas for improvement that were identified for the assessment respondents include:

- **Identifying misuse** - stronger proactive measures are required to identify and address inappropriate access and breaches of the My Health Record system. Less than 13% of survey respondents review system access logs, which helps identify inappropriate use of the emergency access function once it occurs.

[1] Section 33C(1)(a) of the Privacy Act provides that the OAIC may assess whether personal information held by an APP entity is being maintained and handled in accordance with the APPs.

[2] APP 6 outlines the circumstances in which an organisation may use or disclose personal information that it holds.

- **Training** – less than half of the survey respondents train staff about My Health Record emergency access.
- **Intended usage** – a minority of survey respondents indicated that they use the emergency access function for its intended purpose under section 64 of the MHR Act.

From the assessment results, it is evident that despite the availability of guidance material to healthcare providers regarding their privacy obligations around the emergency access function, a barrier exists to understanding and implementing these obligations.

Assessments are not only designed to assess compliance, but are also an educative opportunity to build awareness, improve practices across all relevant regulated entities and ensure privacy protections are in place. The OAIC has developed a concise one page resource *Top tips for healthcare providers* informed by the areas of improvement identified as part of this assessment, to assist healthcare providers when using the emergency access function.

Please see Appendix A for a copy of this resource. This has also been provided to all survey respondents, and is published on the OAIC's website.

Part 2: Introduction

The My Health Record system is the Australian Government's digital health record system. A My Health Record is an online summary of a patient's key health information including medical conditions, treatments, allergies, tests and scans. At the time of writing, there are over 23.7 million My Health Records, which can be accessed by 99% of general practitioners and pharmacies.[3]

The healthcare sector presents particular privacy risks, given the volume and sensitivity of the personal information handled, including My Health Record information. Health service providers consistently report the highest number of data breaches under the Notifiable Data Breaches scheme.[4]

It is important that healthcare provider organisations implement measures and strategies to ensure that personal information in the My Health Record system is secure and handled appropriately. Measures to mitigate privacy risks are embedded in My Health Record legislation and the *Privacy Act 1988* (Cth).

Links to resources and guidance to assist healthcare provider organisations meet their My Health Record obligations are listed in Appendix E.

My Health Record emergency access

The emergency access function allows healthcare providers to override access controls (i.e. an access code set by the patient) to gain full access to a My Health Record, including restricted information and documents, but not deleted information, hidden documents and personal health notes.

The emergency access function is intended to be used under section 64 of the MHR Act, which authorises healthcare providers to collect, use and disclose My Health Record health information where they reasonably believe that:

- it is necessary to lessen or prevent a serious threat to an individual, it is unreasonable or impracticable to obtain the healthcare recipient's consent, or
- it is necessary to lessen or prevent a serious threat to public health or safety.

[3] This figure is correct at the time of writing. For more information about the My Health Record see https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record/statistics.

[4] For more information about Notifiable Data Breaches, go to https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications.

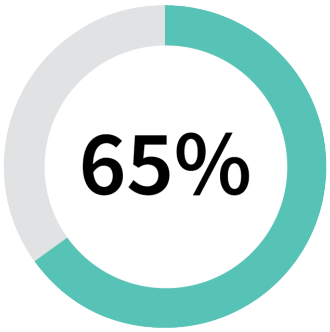
Part 3: Summary of the findings

The ADHA has logs of all usage of the emergency access function in the My Health Record system. In this assessment, these logs were considered and compared to information provided by the assessment survey.

General observations

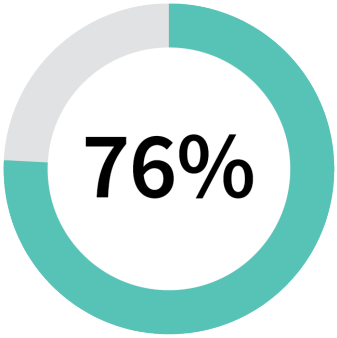
Generally, the assessment found that the respondents had limited awareness of when and how the emergency access function is used at their organisations.

Assessment participants were selected because ADHA data stated that they used the emergency access function in the 2022 calendar year (see Part 4 for more detail on the selection of assessment participants). However, 65% of respondents indicated that no such access had occurred in that period.[5] This proportion of under-reporting by survey respondents was similar for both GP clinics and retail pharmacies.



65% of survey respondents were apparently **unaware that the emergency access function had been used** at their organisation in the 2022 calendar year and many other respondents underestimated the number of emergency accesses.

Only 37 (16.67%) respondents **accurately self-reported** the number of times emergency access occurred at their organisation.



Overall, 76% of **respondents underestimated the number of emergency accesses** that had occurred at their organisations.

[5] This question was answered by 222 assessment participants, 145 of those respondents indicated that the emergency access function was not used at by their organisation in 2022.

65% of survey respondents were apparently unaware that the emergency access function had been used at their organisation in the 2022 calendar year and many other respondents underestimated the number of emergency accesses.

Only 37 (16.67%) respondents accurately self-reported the number of times emergency access occurred at their organisation in 2022.

Overall, 76% of respondents underestimated the number of emergency accesses that had occurred at their organisations. Only 37 (16.67%) respondent estimates were accurate.[6]

This indicates that most healthcare provider organisations do not have sufficient oversight of how the My Health Record system is used at their organisation. This may have also affected the accuracy of the information participants provided in this assessment.

When more users have access to the My Health Record system, there is a greater risk of inappropriate access or misuse occurring. Healthcare provider organisations with high numbers of My Health Record users may need to implement additional mitigation strategies, or implement them more frequently, to ensure that they can promptly identify, act upon and report security risks.

Governance

Under APP 11, healthcare provider organisations are required to take reasonable steps to protect personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.[7]

This assessment asked participants about their processes to prevent, identify and address potential misuse of the emergency access function (governance measures).

Areas of good privacy practice

Governance measures can be complementary and may address individual privacy risks in different ways. For example, policies and training encourage individuals to use the My Health Record system appropriately, while reviewing system access logs allows organisations to identify inappropriate access after it has occurred. The number and nature of governance measures that should be implemented depend on the individual circumstances and privacy risks of the healthcare provider organisation.

Most assessment participants implemented at least 2 governance measures, the most popular being:

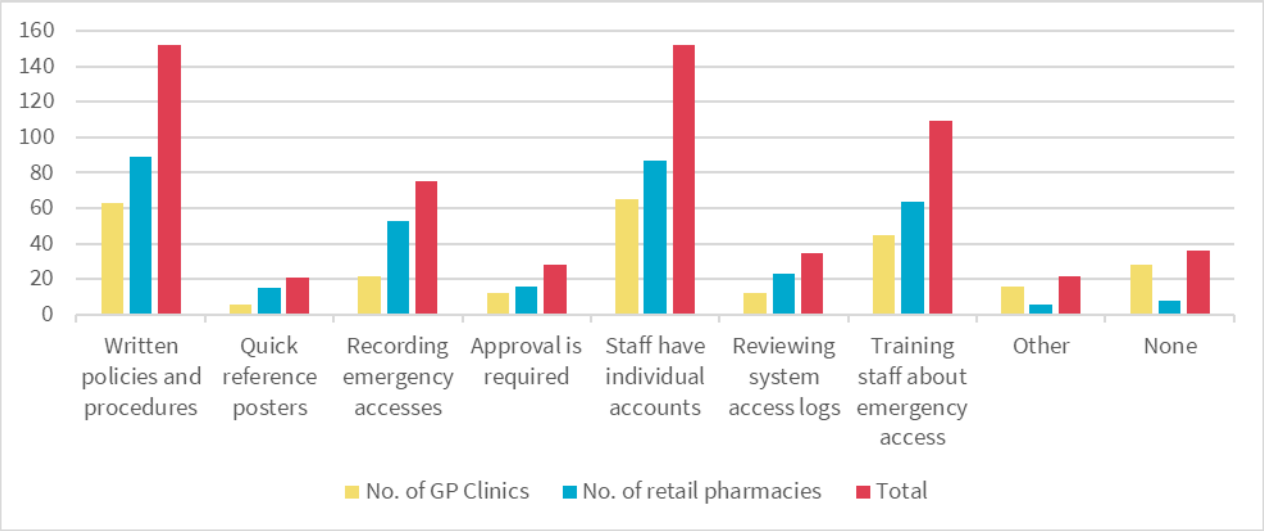
- written policies and procedures that address the emergency access function (152 respondents)
- individual accounts to access the My Health Record system (152 respondents)
- emergency access function training for all staff (109 respondents).

---

[6] Note this report differentiates between participants and respondents. Participants refers to the 300 selected for the survey, respondents refers to the 272(91%) who completed part or all of the survey. There is the potential that had all participants completed the survey the findings might present slightly differently.

[7] Healthcare provider organisations are also required to enforce mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management under Rule 42 of the My Health Records Rule. This was not in the scope of this assessment, but compliance with Rule 42 is considered a reasonable step under APPs 1.2 and 11.1.

Figure 1 — Governance measures at the participating healthcare provider organisations[8]



Policies and procedures

One of the most common governance measures reported in the assessment survey responses was written policies and procedures that addressed emergency access.

Where assessment participants advised that they had relevant policies and procedures, the majority indicated that those documents address the following:

- Appropriately using the emergency access function (133 respondents)
- Addressing potential misuse of the emergency access function (98 respondents)
- Consequences of potentially misusing the emergency access function (91 respondents)
- What records should be kept when using the emergency access function (89 respondents)
- Examples of potential misuse of the emergency access function (71 respondents)

Varied methods of training

Offering training in a variety of mediums accommodates users with different learning styles. Using multiple training sources also reduces the risk that key information will not be communicated to staff.

Of the 109 respondents that provide emergency access training to their staff, most indicated that they use more than one method to train staff. Most commonly this included conducting training internally, and using ADHA resources such as eLearning modules, webinars and podcasts.

Areas for improvement

Assessment participants lacked awareness of the extent to which the emergency access function was used by their organisation.

The governance measures most used by assessment respondents are preventative measures (like training and policy documentation). The measures in place did not *proactively* seek to identify inappropriate use of the My Health Record system in a timely manner (for example, through a regular audit of access log or a register that documented the circumstances of access

[8] Where a respondent selected 'Other' as their only answer, but corresponding free text indicated that they had not implemented any governance measures, these responses were counted as 'None' in this graph.

usage). Without proactive measures in place there is a privacy risk that inappropriate use may not be identified and addressed.

Record-keeping and reviews

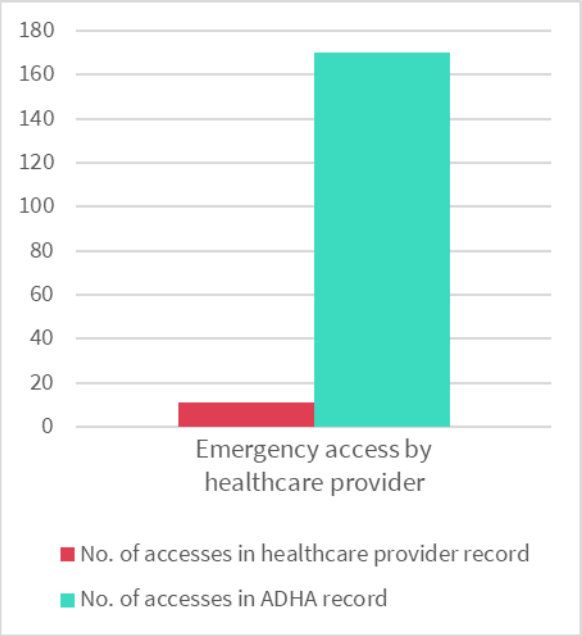
The OAIC recommends regularly reviewing system access logs to proactively identify breaches of the My Health Record system.[9] System access logs are often available in clinical software or can be requested directly from the ADHA by emailing myhealthrecord.compliance@digitalhealth.gov.au.

Only 28% of respondents advised that a record is made each time the emergency access function is used and less than 13% reviewed system access logs.

Where respondents reported that they review these records, more than half indicated that there was no schedule for reviews. If reviews are not done regularly, there is a privacy risk that inappropriate use of the My Health Record system may not be identified and addressed. Addressing inappropriate use promptly can mitigate harm for affected individuals and prevent future incidents.

Emergency access records should also be complete and accurate. Of the respondents that record each emergency access at their organisation, all but one of these records appeared to be incomplete, with respondents not recording every instance of access. Access logs record when the My Health Record system is accessed, including the user's identity, date, and time of access, whose My Health Record was accessed and the information that was accessed. The respondents' records generally showed lower numbers of emergency accesses than ADHA records.

Figure 2 — A comparison of the number of emergency accesses recorded by healthcare provider organisations against ADHA records



Most respondents indicated that emergency access records are made manually, which may result in inaccurate records. When maintained properly, manual records are important for capturing the circumstances of the emergency access, which can be used to assess whether access was appropriate

[9] Proactively reviewing audit logs is an effective means of detecting and investigating authorised access to the My Health Record system. Audit logs record when the My Health Record system is accessed, including the user's identity, date, and time of access, whose My Health Record was accessed and the information that was accessed. Audit logs can often be accessed via your clinical software https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/my-health-record/Security-and-Access-policies-Rule-42-guidance

and what action (if any) should be taken. However, manual records should be cross-referenced against automated system access logs (where available) to ensure that they are accurate and updated in a timely manner.

Implementation of practices and procedures

Although most respondents indicated that they have written policies and procedures addressing the emergency access function, many of these policies and procedures did not appear be implemented in practice.

For example, 89 respondents indicated that they have policies about keeping records when using the emergency access function. However, almost half of these respondents advised that they did not actually keep such records.

There is a privacy risk that staff at healthcare provider organisations may use the My Health Record system inappropriately if policies and procedures are not sufficiently implemented and enforced.

Training

Training about emergency access is conducted in less than half of the respondent organisations, and a minority of those respondents conducted refresher training.

Less than half of the survey respondents train their staff about emergency access in the My Health Record system.

Training and education are important to ensure that staff use the My Health Record system appropriately. This is particularly important for the emergency access function as staff may be required to use it in high-pressure emergency situations. There is a privacy risk that inappropriate access will occur where users of the My Health Record system are not sufficiently trained about when and how to use the emergency access function.

Organisations with no governance measures

Around 13% of respondents indicated that they had not implemented any governance measures to prevent, identify and address potential misuse of the emergency access function. This includes:

- 29 survey respondents that advised that they had no governance measures in place.
- 7 GP clinics that did not identify any governance measures in their responses and indicated that they were unaware of, or did not use, the emergency access function. These responses were taken to indicate that they had no governance measures in place.

A further 79 survey respondents reported having only one governance measure.

When no (or insufficient) measures have been implemented to prevent, identify, and address potential misuse of the emergency access function, there is a privacy risk that unauthorised access will occur and go undetected.

Reasons for emergency access

The emergency access function is designed to be used under section 64 of the MHR Act. Section 64 authorises a healthcare provider to collect, use or disclose health information included in a My Health Record if they reasonably believe that it is necessary to lessen or prevent a serious threat in certain situations.

In the assessment, participants were asked about their reasons for using the emergency access function. The most common reasons for using the emergency access function reported by assessment participants were:

- Access to the My Health Record was necessary to prevent a serious threat to the patient, and the patient's consent could not be reasonably or practicably obtained (95 respondents)
- The patient consented to the access (65 respondents)
- Access to the My Health Record was necessary to prevent a serious threat to the public (63 respondents)
- Access the My Health Record was necessary to prevent a serious threat to an individual (other than the patient), and the patient's consent could not be reasonably or practicably obtained (50 respondents).

Instead of identifying reasons for using the emergency access function, 84 respondents (31%) indicated that this question was not applicable to them as '[their] organisation does not use the emergency access function'. Noting that participants for this assessment were selected based on having used the emergency access function in the previous year, the response illustrates that 31% of the respondents were not aware, did not recall or kept no record of their usage, demonstrating a lack of oversight of the emergency access function. When outlining their reasons for using the emergency access function, only 14 survey respondents (5%) failed to provide any authorised reasons for access under the MHR Act.

Areas of good privacy practice

The most common reasons for using the emergency access function were authorised circumstances under the MHR Act. The reason that was selected the most was also consistent with the intended use of the emergency access function under section 64.

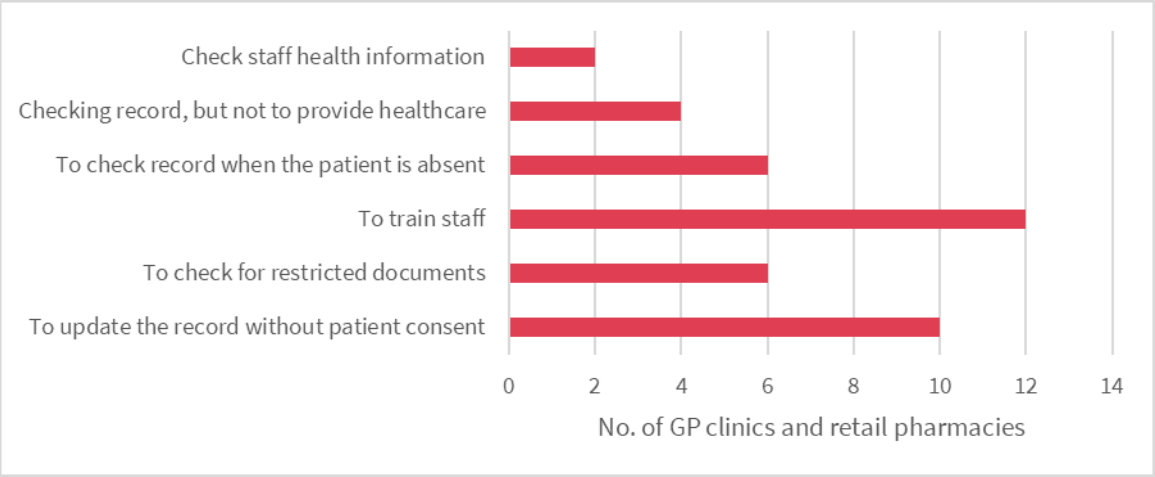
Use of the emergency access function for authorised purposes

Only 14 respondents (5%) indicated that they use the emergency access function only for reasons that are not authorised under the MHR Act.

Although this suggests that there is inappropriate usage of the emergency access function, it appears to be limited.[10]

[10] It is also possible that some of these reasons arose in circumstances that might be otherwise authorised under the MHR Act. For example, access to a My Health Record to train staff with the consent of the holder of that My Health Record, but this was not evident based on the responses provided.

Figure 3 — Responses with access reasons not authorised by the MHR Act



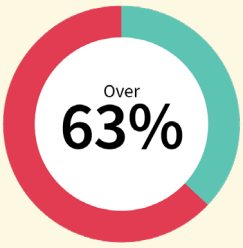
However, over one-third of respondents for this question indicated that they were either:

- unsure why the emergency access function was used at their organisation (16 respondents)
- unaware that the emergency access function was used at their organisation (82 respondents)

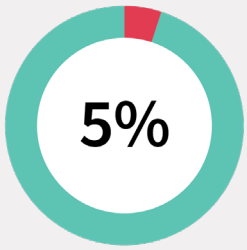
It is possible that inappropriate usage of the My Health Record system may have been underreported in this assessment due to a general lack of oversight by healthcare provider organisations. As noted above, healthcare provider organisations have obligations to take reasonable steps to protect personal information they hold from misuse, and unauthorised access, modification and disclosure. This includes implementing steps to ensure that the emergency access function is used appropriately.

Areas for improvement

The emergency access function was designed to give effect **to section 64 of the MHR Act** which authorises access to a My Health Record in certain emergency situations.



When asked about their reasons for using the emergency access function, over 63% of respondents **did not select any reasons consistent with section 64**.



Only 14 survey respondents (**5%**) failed to provide any authorised reasons

The majority of assessment respondents did not select any reasons that corresponded with the emergency access functions' intended usage under section 64. This suggests that healthcare provider organisations may need to do more to ensure staff are aware of how to use the emergency access function appropriately, including familiarising themselves with the criteria under section 64. The OAIC has developed a flowchart to assist healthcare provider organisations.

Access outside of an emergency

Some respondents advised that they use the emergency access function for reasons that may be authorised under the MHR Act, but not in an emergency scenario consistent with section 64. Most commonly, this related to accessing a My Health Record with the patient's consent,[11] but also included instances where users would access their own My Health Record using the emergency access function.[12]

Healthcare provider organisations should be aware that the emergency access function is not intended to be used in circumstances other than those outlined in section 64. Using the emergency access function will automatically notify the ADHA and may be subject to investigation.

The use of the emergency access function sends an automatic notification to the System Operator, the ADHA.

The System Operator may investigate healthcare provider organisations and require them to explain the circumstances surrounding emergency access use in each instance.

Misuse and notification

Under section 75 of the MHR Act, entities must report to the OAIC and the ADHA (as System Operator):

- Potential and actual unauthorised collection, use and disclosure of health information in a My Health Record (including via the emergency access function)
- Events or circumstances that have or may compromise the security of the My Health Record system.[13]

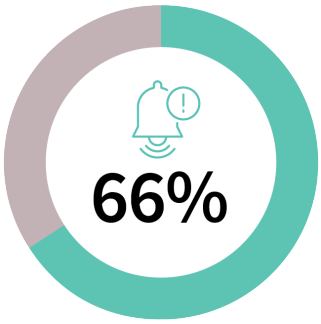
Areas of good privacy practice

Almost all of the respondents advised they had never identified any such misuse, but in the event of this occurring:

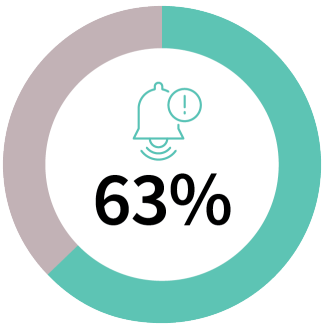
[11] For more information, see section 66 of the My Health Records Act.

[12] For more information, see sections 66(1) and 67 of the My Health Records Act.

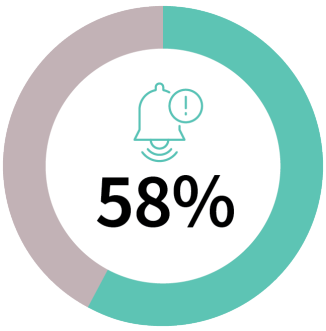
[13] Compliance with this requirement is also considered to be a reasonable step protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure under APP 11.



66% of these respondents would notify the **ADHA**



63% would notify the **OAIC**



58% would notify their organisation's **head office**.

In the assessment, 65% of these respondents also indicated that their organisation would directly notify the affected person.

Areas for improvement

Under section 75(5)-(6) of the MHR Act, only the ADHA is responsible for notifying healthcare recipients of a breach. However, only 27% (69 respondents) of respondents that had not identified misuse of the emergency access function correctly indicated that the affected person would be notified by the ADHA. This suggests that some healthcare provider organisations may have limited knowledge of their specific obligations, and those of other parties, in the event of a data breach.

Of the 16 assessment participants that advised that they had identified any potential or actual misuse of the emergency access function at their organisation:

- six respondents advised that they notified the ADHA of the incident
- five respondents advised that they notified the OAIC of the incident. This was only able to be verified in three cases.

Less than half of the assessments respondents that had identified potential or actual misuse of the emergency access function notified the ADHA and OAIC as required under section 75 of the MHR Act.

Less than half of the assessments respondents that had **identified potential or actual misuse** of the emergency access function notified the ADHA and OAIC as required under section 75 of the MHR Act.

Reporting matters under section 75 of the MHR Act is important for healthcare provider organisations to ensure that they have taken sufficient steps to address any risks to personal information held in the

My Health Record system. It also allows the ADHA and OAIC to identify and address these risks, including risks that may affect the My Health Record system more broadly.

Based on the responses in this assessment, it appears that more work needs to be undertaken by healthcare provider organisations to ensure that staff understand and act in accordance with the obligation to notify the ADHA and OAIC of certain matters.

After the survey

After the survey was completed, the OAIC was advised that the assessment had prompted some participants to review their use of the emergency access function, including potential instances of inappropriate access. The OAIC is working with some of these entities to review and address these instances as required.

At the time of writing, the OAIC is considering further regulatory action regarding other instances identified in this assessment where unauthorised access to a My Health Record may have occurred.

Part 4: Description of the Assessment

This assessment was conducted under s 33C(1)(a) of the Privacy Act, which provides that the OAIC may assess whether personal information held by an APP entity is being maintained and handled in accordance with the APPs.

Objective and scope

The purpose of this assessment was to identify privacy risks relating to healthcare providers' use of the emergency access function under:

- APP 1.2 – the requirement to take reasonable steps to comply with APPs 6 (use or disclosure of personal information) and 11 (security of personal information) by implementing practices, procedures and systems to ensure the emergency access function is used appropriately.
- APP 11 – the requirement to take reasonable steps to prevent and address the unauthorised access, modification and disclosure of personal information via the emergency access function.

Assessment participants

In 2022, the emergency access function was used 6557 times. There were 846 instances from GP clinics and 1597 instances from retail pharmacies. This accounted for 24% of industry usage of the emergency access function.[14] GP clinics and retail pharmacies are APP entities required to comply with Privacy Act.

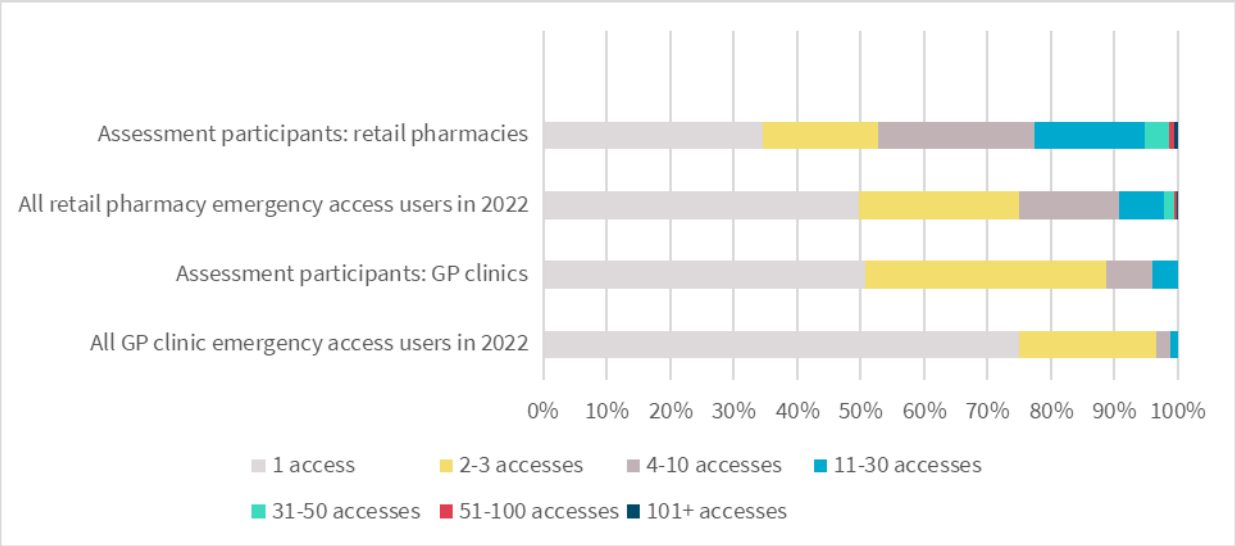
The OAIC asked 150 GP clinics and 150 retail pharmacies (referred to in this report as 'assessment participants') to participate in this assessment. Individual assessment participants were selected based on factors identified in 2022 ADHA data including:

- volumes of unique My Health Records accessed
- volumes of emergency accesses – all the assessment participants had used the My Health Record emergency access function at least once in 2022.

This selection criteria was designed to create an assessment sample that was relatively representative of users of the emergency access function, while also capturing entities with high potential privacy risk.

[14] The OAIC requested ADHA data on all organisation types who used My Health Record emergency access for general information purposes. Although their emergency accesses may have been proportionally higher, public hospitals are not APP entities and cannot be assessed under section 33C(1)(a) of the Privacy Act.

Figure 4 — GP clinics' and retail pharmacies' volumes of emergency access in 2022



The OAIC also considered that the assessment sample should contain representation from each Australian jurisdiction. The survey respondents supply services in each State and Territory or Australia-wide. The health care providers are not identified in this report. More details are in Appendix D.

Characteristics of the survey respondents

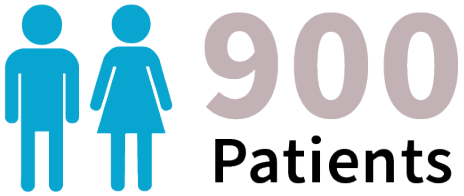
The sample of survey respondents contained a range of different sized organisations. Most survey respondents had 7 or fewer staff members with access to the My Health Record system, but 14% of respondents had 20 or more staff members with access to the My Health Record system. The highest reported number of authorised staff was 53.

Patient volumes were **relatively high** amongst the assessment participants.

78%
of respondent GP clinics saw at least 100 patients on an average day

60%
of respondent retail pharmacies handled prescriptions for more than 200 patients per day.

3
retail pharmacies advised that they dispensed prescriptions to over 900 patients a day.



Patient volumes were relatively high amongst the assessment participants. On an average day, 78% of respondent GP clinics saw at least 100 patients, and 60% of respondent retail pharmacies handled prescriptions for more than 200 patients per day. Three retail pharmacies advised that they dispensed prescriptions to over 900 patients a day.

Conduct of the assessment

Assessment participants were asked to complete an online survey. A copy of the survey is provided in Appendix B.

The survey asked assessment participants about their:

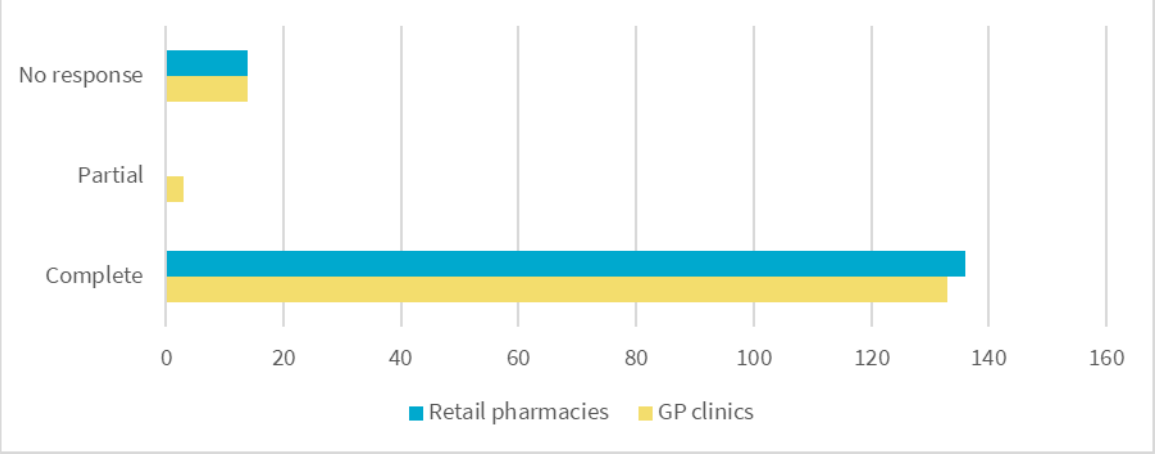
- organisational structure, size and location
- use of the emergency access function
- governance measures including policies, procedures and training,
- processes for identifying and addressing potential misuse of the emergency access function.

Upon completing the survey, respondents received a personalised email that contained feedback, reinforced best practice guidance, and provided links to resources. A sample of this email is available in Appendix C.

The assessment findings are primarily based on information provided by assessment participants in the online survey. The ADHA has logs of all usage of the emergency access function in the My Health Record system. In this assessment, these logs were considered and compared to information provided in the assessment survey.

Where the survey was not completed in full, the responses that were provided have been included in the survey analysis. Of the 300 assessment participants, 272 healthcare provider organisations provided responses in the survey (including partial responses). This was a response rate of 91%.

Figure 5 — Response rate of assessment participants



The assessment also considered data provided by the ADHA. The Respondents were not required to provide supporting documentation such as policies, procedures, templates, or registers.

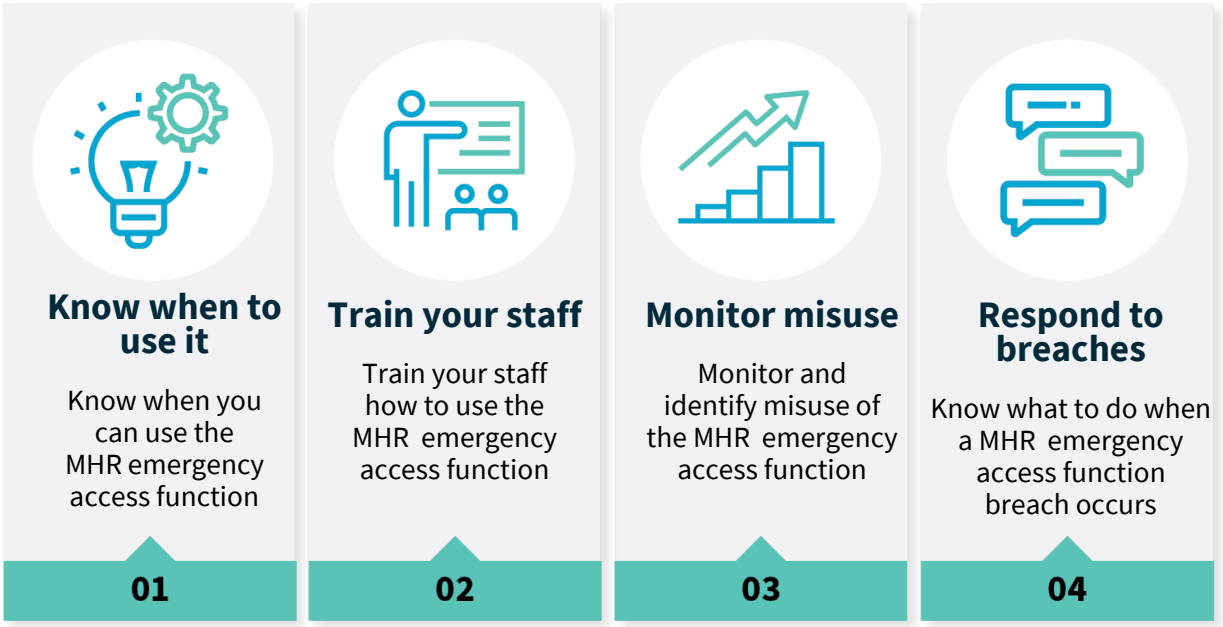
Appendix A: Top privacy tips for assessment respondents

The emergency access function of the My Health Record (MHR) system allows health care providers to override access controls in emergency situations to view patient health care information.

Our privacy assessment of this function, Handling of personal information: emergency access in the My Health Record system, drew attention to the gaps in healthcare providers' knowledge about:

- when the MHR emergency access function can be used
- what governance measures are required to comply with MHR legislation and the Privacy Act, and to adopt a best privacy practice approach.

Top privacy tips for assessment respondents



Based on our assessment findings, the OAIC's top tips for health care providers using the MHR emergency access function are:

1) **Know when you can use the emergency access function to access the MHR.**

   You can only override a patient's access controls to handle health information contained in a patient's My Health Record in limited circumstances:

   - if it is necessary to lessen or prevent a serious threat to the patient, and you are unable to obtain their consent, or
   - if it is necessary to lessen or prevent a serious threat to public health or safety.

   The emergency access function is not intended to be used in other circumstances, for example, when an individual has forgotten the record access code they have set on their My Health Record.

2) **The best way to ensure that your staff use the emergency access function properly is to train them in how to use the function.**
   All staff must be trained before they use the MHR system. Only staff who require access to perform their duties should access the MHR system.

   Trained staff are less likely to unintentionally breach their obligations.

3) **Know what misuse is, know how to identify it, and proactively monitor system usage.**

Oversight of emergency access function usage at your practice is an important part of meeting your obligations.

Proactively look for inappropriate use – this will complement preventative measures like training and policy documentation to ensure your staff appropriately use the MHR system.

Regularly check system access logs or any record used to document your practice's instances of MHR use. Access logs should capture each use of the MHR system and any use of the emergency access function. Check who used the emergency access function, confirm with them why they used it and whether it was for an authorised reason.

4) **If a breach of the My Health Record system occurs, notify the OAIC and ADHA**.
Only the ADHA is responsible for notifying the healthcare recipients of a breach.

For more information see:

- The OAIC My Health Record emergency access function guidance
- The OAIC My Health Record emergency access function flowchart
- The OAIC Report a My Health Record Data breach | OAIC
- The ADHA Emergency access information for healthcare providers
- The ADHA My Health Record Podcast: Emergency access
- The ADHA eLearning Module: My Health Record Security, Privacy and Access

Appendix B: Survey questions

Introduction

Thank you for participating in the Office of the Australian Information Commissioner's (OAIC's) 2022-23 My Health Record assessment regarding the use of the emergency access function on behalf of [Organisation Name].

If you are not related to [Organisation Name], please advise assessments@oaic.gov.au as soon as possible. Please do not complete this survey at this time.

If your organisation was [Organisation Name] but has since rebranded or changed its name, you may complete the survey. Please advise us of your organisation's new name in a comment at the end of the survey.

This survey will take approximately **15-25 minutes** to complete. You can save this survey before it has been completed and return to finish it at any time before the survey closes on **27 August 2023**.

Please answer carefully. You will not be able to change your answers once you continue to the next question.

Please do not provide any personal information, including health information, about your employees or patients in your responses.

If you have any questions about this assessment or how to complete the survey, please email assessments@oaic.gov.au.

After the survey

Based on your responses in this survey, you may be required to provide further information or asked to participate in further regulatory activities.

This may include, but is not limited to:

- providing copies of policy and procedural documentation, training and other resources
- participating in a further privacy assessment.

The results of this survey will be published in a de-identified privacy assessment report on the OAIC website, and a link will be provided to you once this occurs. This report will not identify your organisation or any of the survey respondents.

Terms used in this assessment

The **emergency access function** is also known as a 'break glass' function. It allows a representative of a healthcare provider organisation to override any access controls set by an individual and gain full access to their My Health Record, including restricted documents, in certain situations.

This function may appear differently depending on your clinical software. For example, it may appear as a button, checkbox or drop-down list.

In this survey, you will be asked questions about your organisation including:

- how it uses the My Health Record system, particularly the emergency access function
- governance processes when using and monitoring use of the emergency access function
- how it identifies and addresses potential misuse of the emergency access function

Your organisation

1. What geographical areas does your organisation provide services to? (If you are part of a larger organisation, please answer only for your branch. For example, where your premises is located.)

   a. Australia-wide

   b. State/Territory-wide, please specify the State or Territory:

   c. Local area, please specify the post code and State or Territory (e.g. 2000 NSW):

2. If GP clinic:
   Approximately, how many patients does your organisation provide services to on an average day?

   a. Less than 15

   b. 15-30

   c. 31-50

   d. 51-70

   e. 71-100

   f. 101-150

   g. 150-250

   h. Over 250

   If retail pharmacy:
   Approximately, how many patients does your pharmacy dispense prescriptions for on an average day?

   a. Less than 50

   b. 51-100

   c. 101-200

   d. 201-500

   e. 501-700

   f. 701-900

   g. Over 900

3. How many staff are authorised to access the My Health Record system at your organisation?

   Please enter a number (e.g. '5')

4. What clinical software is used at your organisation? (Select all that apply)

   a. Best Practice

   b. Communicare

   c. Genie

   d. Medical Director

   e. Zedmed

f. Fred Dispense

g. The Provider Portal

h. Other, please specify:
please specify

Emergency access function

5. Approximately, how many times did your organisation use the emergency access function in the 2022 calendar year?

    a. 0

    b. 1-2

    c. 3-10

    d. 11-20

    e. 21-50

    f. 51-70

    g. 71-100

    h. Over 100

    i. I don't know

6. Which of the following are reasons for your organisation using the emergency access function? (Select all that apply.)

    a. To allow users to check their own My Health Record.

    b. The patient has forgotten their My Health Record access code.

    c. To train staff in using functions of the My Health Record system.

    d. The patient has consented to the user accessing their My Health Record.

    e. To check whether a My Health Record has additional restricted documents.

    f. Access to the My Health Record is necessary to prevent a serious threat to the public.

    g. To check current or potential staff are compliant with employment conditions (e.g. test results, vaccination status, etc.)

    h. To check an individual's My Health Record for information, other than to provide them healthcare (e.g. to obtain contact details).

    i. The patient is present, consent cannot be reasonably or practicably obtained, but access is necessary to update their My Health Record.

    j. Access to the My Health Record is necessary to prevent a serious threat to the patient, and the patient's consent cannot be reasonably or practicably obtained.

    k. To check a patient's My Health Record when they are not present and, therefore, cannot provide their access code (e.g. to prepare for a consultation).
    A patient is considered to be present if they are attending via telephone or online.

l. Access the My Health Record is necessary to prevent a serious threat to an individual (other than the patient), and the patient's consent cannot be reasonably or practicably obtained.

m. Other:
please specify

n. Other:
please specify

o. Other:
please specify

p. My organisation does not use the emergency access function. **[Go to 8.]**

q. I don't know. **[Go to 8.]**

7. Please rank the most common uses of the emergency access function at your organisation?

   You may rank more than one item, but must rank at least one item (the most common reason).

   [This question showed the answers selected in Question 6 as answer options to be dragged and dropped into a box for ranking.]

8. Have staff at your organisation ever had a reason to use the emergency access function outside of standard operating hours?

   a. Yes, for the following reason(s):

   b. No

   c. I don't know

Governance

9. Which of the following governance processes have been implemented at your organisation to prevent, identify, and address potential misuse of the emergency access function? (Select all that apply)

   a. Written policies and procedures address the emergency access function **[Ask policies and procedures questions]**

   b. Placing quick reference posters in workspaces to remind staff how and when to use the emergency access function.

   c. A record is made of each use of the emergency access function, and why it was required. **[Ask record-keeping and auditing questions]**

   d. Approval (formal or informal) from a colleague is required to use the emergency access function. **[Ask peer review questions]**

   e. Processes have been implemented to ensure that staff use only their individually assigned accounts to access the My Health Record system.

f. System access logs are reviewed to identify when the emergency access function is used and whether it has been used appropriately and according to organisation policies and procedures (if any). **[Ask auditing questions]**

g. Training that addresses appropriate use of the emergency access function is provided to all users (including short-term staff and contractors) with access to the My Health Record system. **[Ask training questions]**

h. Other:

i. Other:

j. Other:

k. None of the above

Policies and procedures

You mentioned that your organisation has **written policies and procedures.**

10. Do these policies and procedures address any of the following? (Select all that apply)

a. How to appropriately use the emergency access function

b. Examples of potential misuse of the emergency access function

c. The consequences of potentially misusing the emergency access function

d. How to address potential misuse of the emergency access function

e. What records should be kept when using the emergency access function

f. Our written policies and procedures address using the My Health Record system, but not using the emergency access function specifically.

g. None of the above

Record-keeping

You mentioned that your organisation **records each use of the emergency access function and why it was required.**

11. Where is this information recorded? (Select all that apply.)

a. In a log or register

b. In the patient file

c. Other:

12. How many entries are recorded in the emergency access function register or log for the 2022 calendar year?

Auditing

You mentioned that your organisation either:

- **records each use of the emergency access function and why it was required.**
- **reviews system access logs to identify when the emergency access function is used and whether it has been used appropriately and according to organisation policies and procedures (if any).**

13. How are these registers or log maintained? (If you have multiple registers or logs, please select all that apply.)*
    a. Entries are manually recorded by users
    b. Entries are automatically recorded by clinical software
    c. Audit logs are requested from the Australian Digital Health Agency as the System Operator
    d. Other:

14. How often is the register or log reviewed?*
    a. As needed
    b. Multiple times per month
    c. Every 1-3 months
    d. Once or twice a year
    e. Every few years
    f. The register is not reviewed.

15. How long do you keep the register or log for before it is destroyed or deleted?*
    a. For a specific period of time (e.g. 5 years):
    b. Indefinitely
    c. I don't know

Peer review

You mentioned that **approval from a colleague is required to use the emergency access function.**

16. When is this approval obtained? (Select all that apply)
    a. Before the access occurs
    b. After the access occurs

Training

You mentioned that **your organisation trains users of the My Health Record system about appropriate use of the emergency access function.**

17. When is training conducted? (Select all that apply)
    a. As needed
    b. Induction for new staff
    c. Refresher training multiple times a year
    d. Refresher training once a year
    e. Refresher training every 2-3 years

18. How is the training delivered? (Select all that apply)
    a. A member of staff provides training
    b. Using an external training provider (including online training)
    c. Using Australian Digital Health Agency eLearning modules, webinars, or podcasts
    d. Staff read guidance on the Australian Digital Health Agency and/or OAIC websites
    e. Other:

    f. Other:

Potential misuse

19. Has your organisation previously identified any potential or actual misuse of the emergency access function at [Organisation Name]?
    a. No
    b. Yes **[Go to 21]**

20. If your organisation was to identify potential misuse of the emergency access function, which of the following parties would be notified? (Select all that apply) **[Go to Comments]**
    a. The clinical software provider
    b. Your organisation's head office
    c. The Office of the Australian Information Commissioner
    d. The Australian Digital Health Agency as the System Operator
    e. The affected patient (including their authorised representative) would be notified by
    f. your organisation
    g. the Australian Digital Health Agency as the System Operator

h. The affected patient's family (other than an authorised representative)

i. Other: please specify

j. Other: please specify

k. Other: please specify

l. None of the above (I would not notify anyone)

21. What was the reason for the potential misuse of the emergency access function?

22. Which of the following actions did your organisation take after identifying potential misuse of the emergency access function? (Select all that apply)

a. Training all staff

b. Training the staff member concerned

c. Informing the clinical software provider

d. Suspending/terminating the staff member

e. Notifying the Office of the Australian Information Commissioner

f. Notifying the Australian Digital Health Agency as System Operator

g. Reviewing and updating policies, procedures, and staff access levels

h. Temporarily or permanently revoking staff access to the My Health Record system

i. Directly notifying the affected patient (including their authorised representative)

j. Directly notifying the affected patient's family (other than an authorised representative)

k. Asking the Australian Digital Health Agency to notify the affected patient (including their authorised representative)

l. Asking the Australian Digital Health Agency to notify the affected patient's family (other than an authorised representative)

m. Gathering and reviewing information to determine whether misuse of the My Health Record system occurred

n. Consulting with third parties (including reviewing online guidance) to determine whether misuse of the My Health Record system occurred

o. Other:

p. Other:

q. Other:

r. None of the above (no action was taken)

Comments

23. Do you have any additional comments or feedback?

Appendix C: Post-survey email[15]

Thank you for completing the Office of the Australian Information Commissioner's (OAIC's) emergency access survey for [Organisation Name]. Your response will assist the OAIC in supporting healthcare provider organisations to comply with their privacy obligations. We may also reach out to you to discuss your survey responses further.

The purpose of this email is to provide your organisation information about when emergency access to a My Health Record is permitted and practices that your organisation should consider.

Please read this email carefully as it sets out legislative requirements and the OAIC's guidance regarding the emergency access function. The survey was designed to allow respondents to provide responses that accurately reflect their practices and processes, but some survey response options may not represent appropriate use of the emergency access function or the My Health Record system.

When to use emergency access

Based on your survey response, your organisation may be using the emergency access function in circumstances that are not appropriate. If you have not done so already, we recommend that you review any previous uses of the emergency access function and consider whether the accesses may constitute misuse and/or unauthorised access to a My Health Record.

You should only use the emergency access function to access a patient's My Health Record where you reasonably believe that it is **necessary to lessen or prevent a serious threat** to:

- **public** health or safety, or
- **an individual**'s life, health or safety, and it is unreasonable or impracticable to obtain the patient's consent (such as, where the patient is unconscious).

You and your colleagues are not authorised to use the emergency access function:

- to view your own My Health Record or a family member's record. Your record can be accessed via myGov or selected mobile applications.
- to demonstrate how to use the emergency access function. Training resources, including simulators of clinical software are available on the Australian Digital Health Agency (ADHA) website.
- to check for restricted documents where it is not necessary to lessen or prevent a serious threat.
- when a patient has forgotten their record access code. Patients can reset their access code by accessing their record via myGov or telephoning the My Health Record Helpline 1800 723 471.
- where it is not necessary to lessen or prevent a serious threat and you are not providing healthcare to the person whose My Health Record you are accessing. For example, you must not use the emergency access function to check the vaccination status or test results of applicants for employment.

Unauthorised use of the My Health Record system is subject to civil and criminal penalties under the *My Health Records Act 2012* (Cth).

Most patients do not have access controls in place, and you will be able to view their record for the purpose of providing healthcare to the patient or as otherwise authorised by law. If you need to access a My Health Record with access controls, but the circumstances do not warrant use of the

[15] This email is an example of the information that an assessment respondent may have received upon completing the assessment survey. As emails were personalised based on the survey responses, some emails may have contained less information than that shown.

emergency access function, you should contact the patient to obtain their consent to view their information and ask them to provide their access code.

Notifying others of misuse

If the emergency access function has been used to gain unauthorised access to a My Health Record, or you suspect this may have occurred, you must report this to both:

- the OAIC
- the Australian Digital Health Agency (ADHA) as the System Operator.

Unauthorised access includes using the emergency access function by mistake.

In addition to reporting the unauthorised access, you must also ask the ADHA to notify all affected patients (or the general public if required), where your organisation becomes aware of:

- **confirmed** unauthorised access of the My Health Record system
- **potential** unauthorised access of the My Health Record system where:
    - there is a reasonable likelihood that the data breach occurred, and
    - the effects might be serious for at least one healthcare recipient.

Your survey response indicates that your organisation has previously identified potential or actual unauthorised access via the emergency access function. We may contact you to discuss this further.

For more information, our Guide to mandatory data breach notification in the My Health Record system is available on the OAIC website.

Emergency access at [Organisation Name]

Your survey response suggests that there may not be appropriate oversight of when users of the My Health Record system at your organisation use the emergency access function.

It is expected that the need to use the emergency access function will be rare. As a result, your organisation's Responsible Officer, Organisation Maintenance Officer, Practice Manager and/or persons in a similar role should have an awareness of when and how the emergency access function is used in order to ensure that the function is being used appropriately. You may wish to consider the governance procedures you have in place or could implement to ensure that your organisation has appropriate oversight of use of the My Health Record system.

Governance

Based on your survey response, your organisation appears to have limited governance processes to prevent, identify, and address potential misuse of the emergency access function.

Healthcare provider organisations have obligations to take steps that are reasonable in the circumstances to protect the personal information they hold from unauthorised access, modification and disclosure (Australian Privacy Principle (APP) 11), and implement practices, procedures and systems to ensure they comply with the APPs (APP 1.2).

The steps that your organisation must take will depend on your circumstances, but may include:

- Preparing written **policies and procedures**.
- Placing **quick reference posters** in workspaces for staff.
- Encouraging or requiring staff to **consult with their peers or colleagues** where possible to ensure that access via the emergency access function is appropriate.
- Maintaining and reviewing a **log or register** of all accesses to the My Health Record system.

- **Recording the circumstances of all emergency accesses** including identifying the time and date of access, the patient, the serious threat that the access was required to lessen or prevent, and why it was not reasonable or possible to obtain the patient's consent.
- Regularly **training** staff (including short-term staff and contractors) about appropriate use of the emergency access function.

Your organisation is also required under the My Health Records Rule 2016 to implement and enforce a written policy that addresses various governance measures, including:

- **training** staff to use the system accurately and responsibly
- a process for **identifying a person who requests access** to a patient's My Health Record and communicating the person's identity to the System Operator
- **mitigation strategies** to promptly identify, act upon and report security risks.

For more information about your general obligations under the My Health Records Rule, please read our Security and Access policies – Rule 42 guidance.

More information

If you would like to learn more about the My Health Record emergency access function, resources are available on the OAIC and ADHA websites. These include:

- The OAIC My Health Record emergency access function guidance
- The OAIC My Health Record emergency access function flowchart
- The ADHA Emergency access information for healthcare providers
- The ADHA My Health Record Podcast: Emergency access
- The ADHA eLearning Module: My Health Record Security, Privacy and Access

We encourage you to share these resources with your staff. Should you have any questions please email assessments@oaic.gov.au.

Appendix D: Assessment participant service areas

Table 1 — Assessment participants' service areas

Service area	No. of general practices	No. of retail pharmacies	Total
Australia-wide	11	8	19
ACT	2	4	6
NSW	36	28	64
NT	1	1	2
QLD	33	39	72
SA	13	8	21
TAS	1	2	3
VIC	27	25	52
WA	12	22	34
No response	14	13	27
Total	150	150	300

Appendix E: Resources for users of the My Health Record system

Information and resources have been developed by the OAIC and ADHA to assist healthcare provider organisations in meeting their My Health Record system obligations and mitigating privacy risks relating to the emergency access function.

- OAIC Guidance: My Health Record emergency access function
- OAIC Guidance: Security and Access policies – Rule 42 guidance
- OAIC Guidance: Guide to mandatory data breach notification in the My Health Record system
- ADHA Guidance: Emergency access information for healthcare providers
- ADHA My Health Record Podcast: Emergency access
- ADHA eLearning Module: My Health Record Security, Privacy and Access

Additional information and resources can be found on the OAIC page for health service providers.