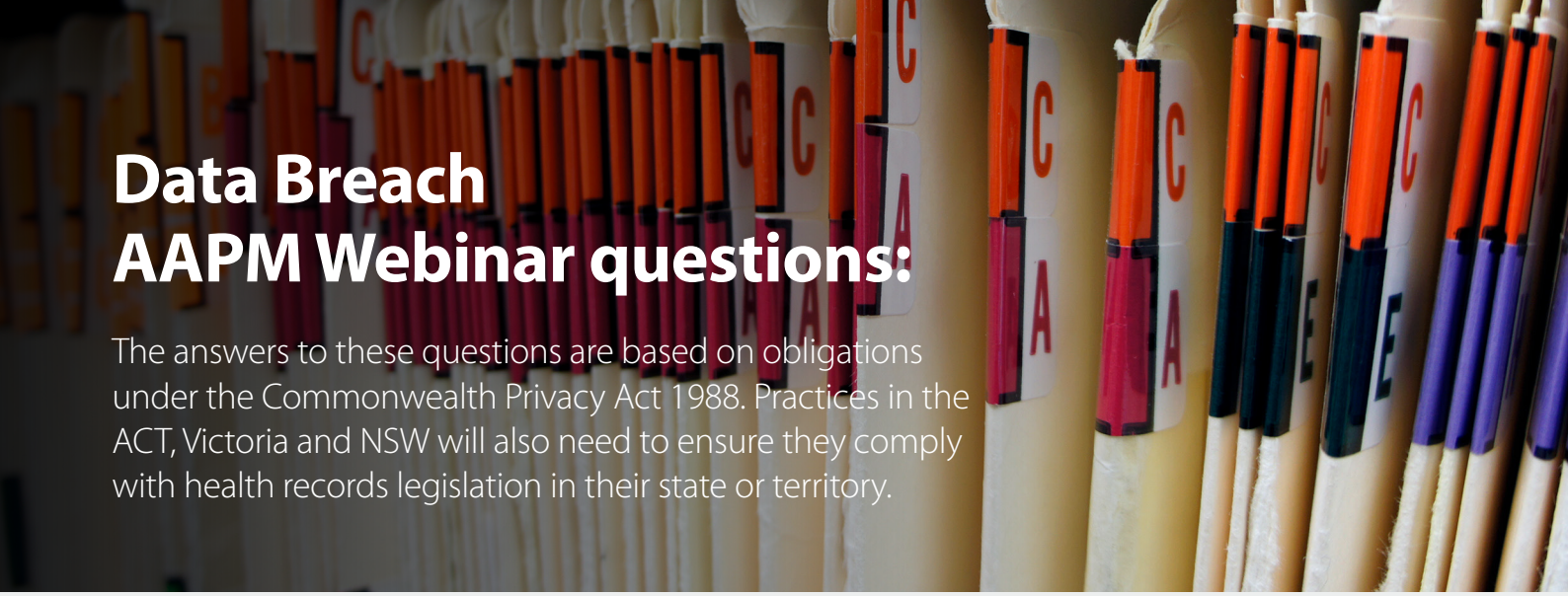

Data Breach AAPM Webinar questions:

The answers to these questions are based on obligations under the Commonwealth Privacy Act 1988. Practices in the ACT, Victoria and NSW will also need to ensure they comply with health records legislation in their state or territory.

General privacy questions:

Release of medical records to a third party

Are we required to release medical records to an insurance company when a patient has signed the release form but the practice is concerned the patient may not be fully informed as to what they have agreed to?

Generally, if you receive a request for medical records from an insurance company and the patient's authority authorising the release, you are required to release the records. However, you should check the scope of the authority against the request from the insurer. Sometimes the request is for the whole of the record; sometimes it is only for certain records. Sometimes the request is for all of the medical records, but the authority signed by the patient only authorises disclosure of records relevant to the claim or injury.

Read the request carefully to ensure that you only include documents captured by the scope of the patient's authority.

Check all records before you send them to ensure that you are sending what has been authorised by the patient.

If you are concerned that the patient may not fully understand the extent of their authority, for example where the records contain sensitive information, contact the patient directly and check with them and confirm that that are happy to release the records, in accordance with their authority. Carefully document any conversations you have with the patient.

If we have received records from another clinic for a new patient and then the patient has a WorkCover claim and WorkCover requests medical records, can we send whole file including records, results, etc from previous clinic?

If you receive a WorkCover request for all records relating to a patient and the patient's authority permits release of all the records, records you hold from the patient's previous clinic should be included.

Once a previous clinic's records are received by a new clinic, they form part of the patient's medical record at the new clinic.

Email

Please clarify the requirements for practices using emails.

Email can be used by a practice to transmit information outside the practice. Many practices are reluctant to email because it is not regarded as a secure form of communication. Patients and organisations are however increasingly requesting that information be sent to them via email.

Your practice has an obligation to take reasonable steps to protect the privacy and security of information it holds including when it is transmitted or disclosed outside the organisation. What will be reasonable will depend on several factors.

The Office of the Australian Information Commissioner (OAIC) recommends considering these issues:

- Do you avoid sending certain types of personal information via unsecured email (for example sensitive information)?
- Do you use secure methods for communicating information, such as a secure website or to a secure online mailbox?
- Do you use secure messaging where appropriate and available?
- Do you obtain a recipient's consent to send their own personal information to them via email?
- Do you validate the email address with the recipient before sending the unencrypted email to reduce the chance of unauthorised disclosure to a party who is not the intended recipient?
- Do you ensure that accurate records are kept regarding when external emails are sent and received?
- Do you only send sensitive information or large amounts of non-sensitive personal information by email as an encrypted or password protected attachment?

The use of passwords or encryption can reduce the risk of a data breach, although there is no legal requirement that emails be encrypted or password protected. The RACGP outlines various steps that can be used to reduce the risk of interception of data and sending emails to incorrect addresses, including:

- use of passwords
- use of encryption
- verification of the recipient's email address
- obtaining consent
- use of secure messaging facilities between practices.

The RACGP recognises that encryption may be impractical when communicating with patients who wish to send and receive information via email. In its "Guiding principles on using email in general practice" the RACGP recommends informing patients who request information by email about the risks associated with unencrypted email and confirming they still wish to have the information sent in that way.

It is better to use secure messaging to send information between practices, rather than fax or email.

You should have a policy and procedure in place to manage the electronic transmission of personal information, including the steps that the practice will take to ensure that the privacy and security of information transferred outside your practice is protected.

Medical information outside of the practice

What about surgeons taking paper patient files to theatres or home for dictation?

You have an obligation under the *Commonwealth Privacy Act 1988* to take reasonable steps to protect the personal information you hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Many doctors take paper files out of the practice to use them in theatres or to work at home. There is nothing that prevents them from doing so, as long as they take reasonable steps to protect the privacy of the records when they take them off -site. Avant has seen many instances where doctors have taken paper files off-site and then had the bag or even the car that the records were in, stolen. This would potentially be a serious data breach, requiring notification under the notifiable data breaches scheme. We suggest that you discuss in your practice how best to protect the privacy of the information while enabling doctors to have access to files if necessary so they can do their work.

You could have a policy at your practice that if physical files are removed from the practice that they must be transported in a locked bag, and laptops and flash drives must be encrypted or password protected.

What happens re remote access from home?

There is nothing preventing you from having remote access to practice records provided you have adequate security measures in place to prevent unauthorised access. This might include multi-factor authentication of user access and use of a secure remote access program. You should seek the advice of your IT consultant on the best system for your practice. You may also wish to consider having a practice policy on remote access and appropriate use, particularly regarding downloading documents to home computers, and ensuring that staff are trained on remote access and its acceptable use.

Should a practice owner keep a copy of the patient database even after selling the practice, for medico-legal purposes to access the notes if needed in the future?

Whether or not a practice owner can keep a copy of the patient database after selling the practice will depend on the terms of the sale of practice agreement.

Although a practice owner may wish to keep a database copy of the records in case there is a dispute in the future, the OAIC has been critical of organisations where there have been data breaches involving information that has been kept beyond the period it was needed for the organisation to perform its functions.

If a practice owner keeps a copy of the records, then they will continue to have obligations under the Australian Privacy Principles to take reasonable steps to ensure the privacy and security of the information they hold.

In addition, under the Australian Privacy Principles, a person who holds information must take reasonable steps to destroy or de-identify that information once it is no longer needed for any purpose for which it may be used or disclosed. This would require the practice owner to regularly consider which records in the database should be kept and which should be destroyed or de-identified.

The better option is to reach agreement with the new owner to allow the former owner to access or obtain copies of the medical records of past patients if needed in the future, for example if any dispute arises about a patient treated at the practice, or a patient complains about the treatment they received.

Data breach questions

What is remedial action?

As outlined in the webinar, if remedial action can be taken to prevent serious harm occurring as a result of a data breach, then there will be no obligation to report the breach to individuals potentially affected or to the OAIC.

Remedial action will depend on the circumstances of the case and the nature of the breach. It requires you to be satisfied that the action taken in response to a breach has prevented the risk of harm occurring to potentially affected individuals.

A doctor leaves their smart phone on public transport and when they get to work they realise it has been lost. The smart phone includes clinical photographs. The doctor is able to remotely delete the information on the smart phone. Because of the security measures on the phone, the doctor is confident that the content could not have been accessed in the short period between when it was lost and when its contents were deleted.

An email attaching a letter about a patient is sent to the wrong specialist's email address. The sender realises the error, and contacts the specialist's practice. The practice confirms they have not accessed the letter and that they have deleted the letter and the email.

Although there is no mandatory obligation to notify individuals in circumstances where action can be taken to prevent harm, it is good medical practice to inform the patient about an error leading to a data breach, in accordance with a doctor's professional obligation to disclose adverse events to patients.

Does remedial action mean contacting the patient to resolve and so you are not required to report to the regulator or is the notification only for the regulator?

Sometimes the remedial action will involve contacting the patient so that they can take steps to protect their information (such as cancelling a credit card or Medicare card). If, as a result, there is no risk of serious harm to the patient or other individuals, then the data breach is not notifiable and there is no need to notify the OAIC.

If you can't take remedial action to prevent the risk of harm to individuals then you need to notify potentially affected individuals and the OAIC.

Doctors have a professional obligation to disclose adverse events to patients. This includes where there has been an error leading to a data breach. It is good medical practice to inform the patient about an error leading to a data breach even if it does not need to be notified to the OAIC.

Is it a notifiable data breach if results are emailed to the wrong patient?

Whether this is a notifiable breach will depend on the circumstances. You would need to consider the three steps:

1. Is there a breach?

   In this case, yes, because information about the patient has been disclosed to the wrong person.

2. Is the breach likely to result in serious harm, from the perspective of a reasonable person?

   This will depend on the nature of the information and to whom it has been disclosed. If the email is password protected or encrypted then the risk of harm will be reduced.

3. Can remedial action be taken to prevent the risk of harm?

   Again this will depend on the circumstances. You may be able to recall the email via your email program so that the wrong patient doesn't receive the email or it is deleted automatically. You could telephone the recipient of the email and ask them to delete the email.

Even if this is not a notifiable data breach, you may want to contact the patient to let them know. You should also take steps to prevent this happening in the future. This might include disabling the auto fill address function on your software, training staff to double check addresses before they send emails, or sending emails that are password protected or encrypted.

Can a staff member be held personally responsible for a data breach?

The practice will generally be responsible for the actions of its employed staff.

This only applies to staff who are employees. Some doctors or other health practitioners are independent contractors and not employees of the practice. Independent contractors will be personally responsible for their own breaches.

However the practice may take disciplinary action against a staff member (whether employee or contractor) for a data breach if it happened because the staff member deliberately failed to follow a policy or procedure. This will depend on the terms of the staff member's contract with the practice.

As the entity that holds personal information for the purposes of the Privacy Act, it is likely that the practice will be responsible for co-ordinating notification to the OAIC and taking action to respond to a data breach.

Does it make a difference if a staff member has signed a confidentiality agreement?

A confidentiality agreement is a way of ensuring that staff know what their obligations are. Having staff sign a confidentiality agreement is one of the 'reasonable steps' that a practice can take to protect the personal information held at the practice from misuse, interference and loss, and from unauthorised access, modification or disclosure. It will not make a difference to whether or not a breach is notifiable, but it may give the practice grounds for disciplinary action if a staff member releases confidential information in breach of the confidentiality agreement.

What does a 'reasonable person' mean?

'Reasonable' and 'reasonably' are not defined in the Privacy Act. A 'reasonable person' is a concept used in the law to describe the ordinary, reasonable person in the particular circumstances being considered. It is a legal concept from English law, where the reasonable person was described as 'the man [sic] on the Clapham omnibus'; adopted in Australian cases as 'the man [sic] on the Bondi tram' and 'the man [sic] on the Bourke St tram'.

What is reasonable can be influenced by current standards and policies. In the context of notifiable data breach, you need to consider whether the ordinary, reasonable person would consider it likely that the breach would result in serious harm to a person.

To confirm, was the test whether a 'reasonable person' would think it could harm, OR whether the breach would harm a reasonable person.

The test is whether from the perspective of a reasonable person, the data breach would be likely to result in serious harm to an individual whose personal information was involved in the breach.

Is a data breach response plan included in the RACGP 5th editions?

Criterion C6.3 and C6.4 of the RACGP 5th edition Standards for General Practice relate to privacy and information security. There is no data breach response plan included in these standards but the RACGP Computer and information security templates provides detailed information and templates for ensuring computer and information security at medical practices. A data breach response plan is included.

Cyber security questions

Ransomware

Do ransomware type attacks such as cryptolocker where files are encrypted but not released or distributed denial of service (DDOS) attacks count as a breach?

Where there has been no unauthorised access, disclosure or loss of data, there is no breach for the purposes of the notifiable data breach scheme. You will need to take steps to contain, evaluate and respond to the breach, but you will not have a mandatory obligation to report the breach to the OAIC.

Resources available

Can you recommend some other resources?

Avant resources

- Avant Learning Centre>Data breaches

Office of the Australian Information Commissioner

- Office of the Australian Information Commissioner Data breach preparation and response – a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)
- OAIC Guide to mandatory data breach notification in the My Health Record system
- OAIC Guide to Securing personal information

RACGP resources

- RACGP standards
  - Criterion C1.2 Telephone and electronic communication
  - Criterion C6.4 Information Security
- Computer and Information Security Standards

Australian Digital Health Agency

Stay Smart online

Australian Signals Directorate

- Essential Eight Explained

Australian Cybersecurity Centre

Department of Health

- My Health Record notification of breaches

2312 03/18 (0996)