Safer Care Victoria

Incident review documentation

If you are reviewing a sentinel event or another serious incident, this fact sheet will help you understand what documents to collect and keep as part of the review. It provides guidance on best practice document production and management, and the answers to common questions we get asked by health services.

This fact sheet is useful for anyone involved in an incident review, including health service staff, consumers and independent external panel members. It is also helpful for health service executives, legal counsel, and quality, risk and safety leaders.

The information contained in this fact sheet does not constitute legal advice. To ensure legislative compliance, legal advice should be obtained by individual health services on a case-by-case basis in relation to the retention or destruction of the incident review report and any documents created as part of the incident review process.

Refer to your executive if your legal counsel is unknown.

What is considered an incident review document?

Both hard and soft (electronic) copy documents created in the course of the review of a sentinel event or serious incident.

All review documentation may be subject to a Freedom of Information (FOI) or other type of Request of Information (ROI).

Documents may include:

- spreadsheets
- audio/visual recordings
- notes and sketches
- memoranda
- minutes and agendas
- any other record relevant to the review or employed in the analysis and preparation of the final report document.

Safer Care Victoria

CREATING REVIEW DOCUMENTS

Managing hard copy documentation

Hardcopy documents and correspondence should be marked 'Confidential'.

Hardcopy documents should be returned to the review leader at the end of the meeting, or when no longer required.

Do not post or fax documentation as these methods are not considered secure.

All documentation created during the incident identification, analysis and management process should be carefully retained and securely stored.

Writing notes

Throughout the course of the review, make sure your notes are based on observations and evidence. Be clear, objective, and non-emotive.

All notes and documents should be system focused. Do not attribute blame to individuals.

Use role or position titles, not the names of the staff involved in the incident under review.

Managing electronic documents

Mark all electronic documents with a 'Confidential' watermark.

All documents should be password protected. Save your document as a PDF that can be password protected and encrypted. Generally, this action is undertaken by the review leader.

Where possible send the password for password protected documents separately via text to the recipient's mobile phone.

Do not create, save and/or store electronic review documents on your personal computer or devices.

Please be aware of your surroundings when viewing material on your computer screen (e.g. not in public places or in view of family members at home).

Do not leave information unattended. Always lock your computer when leaving your desk.

Sending emails

Re-read emails before you send them, adding the 'send address' as a last step before sending.

Use your work email address – not a personal email address – to send or receive emails about the review.

Use a clear subject line, such as:

- *** In confidence – for deliberative purposes only
- *** In confidence – do not distribute
- *** In confidence – do not print

Be clear about the purpose of your email, for example:

- This is for the purpose of a review in progress and confidential discussion.
- Sent for the purposes of obtaining legal advice.

It is good practice to securely save a copy of the email as back up.

Are all emails considered incident documents?

Emails relating to the logistical management of the incident review, such as meeting appointments, are not likely to be considered incident review documents.

Are you leading a review team?

Please brief your incident review team members on document management before you begin the review. This includes having a clear, agreed responsibility and pathway for hard copy and electronic document tracking and management.

Safer Care Victoria

SHARING DOCUMENTS

Be careful in how you distribute incident review documentation. Use secure encrypted or password protected systems when sharing electronic documents if available.

Sharing documents among the review team

Note: the review team includes independent (external) panel members and consumer representatives.

Email Encrypt emails and electronic documents. Please ask your local IT service for support.

Do not post or fax documentation as these methods are not considered secure.

Hard copy All documents should be returned to the lead reviewer at the end of the meeting, or when no longer required.

USB or portable hard drive We do not recommend you store documents on a portable storage device. If using one for meeting documentation, it should be encrypted, and password protected. (Refer to your local IT service if assistance is required with this.)

We do not recommend using third party electronic storage such as Cloud or Dropbox for confidential material. If electronic storage is required, seek advice from your local IT service and legal counsel.

Attaching documents to your incident management reporting system

Please seek advice from your legal counsel or external lawyers about attaching incident review documentation on the relevant incident management reporting system reporting page or quality improvement module.

Can I share a document with someone outside the review team (but within my organisation)?

All confidential documents considered by the review team should not be shared outside of the team.

Can I share a document with someone outside the organisation?

Unless legally obliged to do so, it is not recommended to share confidential and identifiable information as there are often complex privacy and other laws that may apply. Please discuss with your health service's records management team or legal counsel.

What if someone requests the review documentation?

Please seek advice from your health service's legal counsel.

STORING DOCUMENTS

Both hard copy and electronic documents should be stored securely. Do not store these documents in the patient's clinical file.

To ensure legislative compliance, we strongly recommend that you seek advice from your legal counsel.

How long do I keep the review documentation for?

Do not destroy notes, or any other review documents, made as part of the incident review without advice from your legal counsel.

Local health information services can also provide guidance on document retention.

What would I do in the event of a data breach or loss of confidential documents?

Please refer to your health service's policy/procedure around document management and escalation.

Is it acceptable to record interviews?

It is usually acceptable to record interviews with written consent. You should however, always seek advice from your legal counsel when you are considering recording an interview for the purpose of an incident review.

FOI and ROI documentation and exemptions

Review documents may be subject to freedom of information (FOI) in the public sector or request of information (ROI) in the private sector. Each FOI request or ROI request will be assessed on a case-by-case basis by the FOI officer, privacy officer or legal counsel.

While, in some cases it will be appropriate to release documents, there are times where some documents (or parts of documents) may be considered exempt and not appropriate for disclosure.

MORE INFORMATION

Please contact the Incident Response Team at sentinel.events@safercare.vic.gov.au.

Relevant legislation:

Commonwealth: *Freedom of Information Act 1982*

Victorian: *Health Services Act 1988, Public Records Act 1973,* S254 *Crimes Act 1958, Health Records Act 2001, , Privacy and Data Protection Act 2014*

To receive this publication in an accessible format phone 9096 1384, using the National Relay Service 13 36 77 if required, or email **info@safercare.vic.gov.au**

Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.

Available at www.safercare.vic.gov.au

VICTORIA State Government