Guidance note for Cochrane Groups

Changes to data protection regulations relating to how personal data are stored

The General Data Protection Regulation (GDPR) from the EU came into effect on the 25th May 2018. This requires stricter data protection policies and practices in any organization that holds data on any EU citizens and it introduces large fines for those who fail to comply with the legislation. Therefore, it is vitally important that Groups read this guidance note and take action where required.

Within Cochrane, we have reviewed our policies to ensure we are compliant with regard to our central communications and IT infrastructure and as part of this we have revised our data policy[1], but this affects Groups as well, so we have put together this guidance note, which highlights key areas of change that Groups need to be aware of.

We have identified four key areas of Cochrane Group work that involve the handling of personal data and so need to be considered in light of this change in legislation:

1. Newsletter communications and any other communications that the law considers to be marketing.
2. Holding personal data in spreadsheets where it can easily become out of date or stored beyond when it is required.
3. Recording personal details of people wanting to get involved.
4. Elements of the editorial process where Groups handle personal data, e.g. topic proposal forms, approaching peer reviewers.

Important definitions

Data is information, which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of the Policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Anyone processing personal data must comply with the **eight enforceable principles of good practice**. These provide that personal data must be:

1. Processed fairly and lawfully.
2. Processed for specific purposes in an appropriate way.
3. Adequate, relevant and not excessive in relation to the purpose.

[1] https://community.cochrane.org/organizational-info/resources/policies/data-policy

4. Accurate and kept up to date.
5. Not be kept for longer than necessary.
6. Processed in accordance with the rights of the data subject.
7. Must be kept secure using technological and organizational measures.
8. Not be transferred outside the European Economic Area unless that country ensures adequate levels of protection for the rights of the data subject.

1 Newsletter communications

Overview

Due to the practical barriers of managing all Cochrane Group newsletters centrally, and our understanding of what is required in the data protection regulations, we recommend that Groups continue to manage their own mailing lists, but every Group with a mailing list needs to be able to demonstrate compliance with the below standards.

Standards

1. You must use a dedicated newsletter software such as MailChimp to store the personal data of your subscribers. You may not keep a spreadsheet of mailing list subscribers locally.

2. You must take appropriate technical and organizational measures to prevent unauthorised access to the data, including using suitably strong passwords.

3. Sign-ups to the mailing list must be explicit, clear, and recorded. For example, sending potential recipients a link to a mailing provider's website that allows them to sign up to the mailing list. MailChimp offers this functionality as standard.

4. You must not create a mailing list from Archie contact details – people must subscribe to your mailing list. You are free to write to people, e.g. when registering a title, to inform them about your mailing list, but you must not add people to mailing lists by default. **Performing a bulk export of contact information from Archie to send any mailings is not permitted according to the law.**

5. Recipients must be able to unsubscribe by clicking a button or hyperlink in the email. This should be tested to ensure it functions as expected. Note that many mailing providers, including MailChimp, supply this functionality as standard.

6. The following disclaimer must be included next to, or directly below the unsubscribe button / link. *"Please note: unsubscribing will remove you from the Cochrane XXXXX Group's mailing list, but it will not automatically unsubscribe you from other Cochrane Groups' mailing lists or from Cochrane's organizational mailing lists which you can manage at account.cochrane.org."*

7. Your newsletter should include relevant content, such as information about Group activities, news, recent publications, and information related to the Group's area of interest, which may include upcoming events and other information about which they may reasonably be expected to be informed.

8. Do not use or share the recipients' details for any purpose other than to send the newsletters.

Recommended processes for Groups

- Set up a newsletter in MailChimp with a group template following guidance above, including the appropriate disclaimer at the end. MailChimp is free to use up to 2000 subscribers[2].
- Advertise the sign-up link on your website, see here for an example: http://oralhealth.cochrane.org/news-events
- Incorporate a message about your newsletter into your standard communications to newcomers to your Group that recommends they sign up and provide a link.
- You can also promote your newsletter through social media channels.
- If you already use MailChimp and you have existing newsletter subscribers who have explicitly signed up then no action is required for those contacts, you can keep contacting them as before.
- Do not download contact lists from Archie to populate your newsletter subscriber list. These people have not explicitly said they want to receive the newsletter. The fact that they have received it in the past and not complained/unsubscribed is not sufficient as that is passive opt in, not the explicit active opt in that GDPR requires.
- If you are in any doubt you should remove people from the mailing list and write to them to ask them to re-subscribe.

Other communications

The above refers to newsletters as they fall under the category of marketing communications as far as the GDPR is concerned. Many of our day to day forms of communication are outside of this and can continue as before. The distinction here is that the below examples refer to content that is essential to communicate to the individual in order for them to complete their work with the Group. Examples of communications that continue unchanged:

- Workflow emails
- Personal emails to named individuals about a specific task
- Messages to groups of individuals, such as editors or authors, about something specific to their role, e.g. if you want to make all of your editors aware of a new checklist, you can send a group email. Or, if you have set a new policy that is directly linked to someone's role in the Group, e.g. if, hypothetically, you set a new policy to only accept review submissions that use ROB 2, you could write to all authors who are actively working on reviews to convey this message.

Newsletters, on the other hand, have more general content about news, new reviews, events etc., and it is not strictly necessary for them to receive this information to complete their role, and so they must be actively opt in, as explained above.

2 Holding personal data in spreadsheets

One key issue that affects Cochrane Groups is how data are stored on individuals. Cochrane provides central systems to store personal data and we would encourage you to use these systems. This ensures that all data is centrally, securely managed and kept up to date. **This means only using Archie to store data**

[2] MailChimp offer guidance here: https://mailchimp.com/resources/guides/getting-started-with-mailchimp/

on people. In this brief document we explain why this is preferable to using spreadsheets or other local systems.

To comply with the legislation, you need to:

- keep data secure,
- keep data up to date,
- ensure data held are correct; and
- ensure data held are relevant.

Complying with the legislation is easier to do on a centralized database, such as Archie. Using central systems means that Cochrane has more control over what is stored, why and how, which is of benefit in demonstrating compliance with the GDPR.

For example, if a person changes their email address, this can be updated on a centralised database quickly and efficiently. However, if their information is kept in multiple locations not all will be updated and this will result in Cochrane holding out of date data, a practice which is not compliant with GDPR. Contact preferences should also be maintained and updated when required on the central database. Furthermore, if a person requests disclosure of any personal data held this can be shared accurately. With a single database we can control what personal data are stored and be GDPR compliant

Data can be kept on spreadsheets, but they have to be securely stored, with relevant access controls, encryption and written procedures on how the spreadsheet is kept up to date, relevant and correct. If it is printed out, it should be stored securely (e.g. in a locked cupboard and keys not left on a desk), no copies left on desks/photocopiers and securely destroyed when no longer needed. Spreadsheets are easier to share too, which has risks attached.

If you do need to collect data on individuals outside of our core systems, then when you collect that data you should inform the individual about how you will store and process their data and either seek their consent for doing so or provide some other lawful basis for processing[3].

Fundamentally, storing information on a centralized database means it is easier for Cochrane to meet the 8 principles of the GDPR and means that you don't need to worry about the above issues.

Please take this opportunity to review the data you hold locally in spreadsheets or similar formats outside of Archie, and ask yourself:

- Is it necessary to store this personal data, if so what is the reason? If not, please delete/securely destroy it.
- Is storing all of the personal data necessary or just some of it, if the latter, remove unnecessary data.
- If storing the personal data is necessary, could this be stored on Archie instead, if not why not? If it can, please add all relevant details to Archie and delete/destroy the spreadsheets.
- If it is necessary to store the data and it can't be stored in Archie, please document how you will keep it up to date and ensure its security as described in the document above.

If you have any questions about this or need further assistance, please contact the community support team: support@cochrane.org

3 Getting involved requests

When newcomers approach the Group they should be directed to sign up at cochrane.org rather than adding people to local lists/databases. When someone signs up centrally they have access to *My Account* and can see and control their own personal details.

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

If the Group needs to add individuals directly in Archie their user account must be activated at this time to ensure they set up a password and can access *My Account* to update their own contact details.

Currently My Account only allows you to update *name*, *country* and *email*. We are working on allowing editing of other information, so that long term this will become the primary place where users go to control and update their contact details and communication preferences.

4 Editorial process (CRGs only)

In discussion with MEs we have identified some specific points in the editorial process where MEs need to handle personal data and so we have brought together the following responses to specific enquiries, which we think are useful to all CRGs.

Process	Specific action	Why might this be a data protection issue?	What can Groups do about it
Review proposal	Circulating review proposals for comment	Emailing someone's contact details around for no particular reason is unadvisable.	There is no reason to circulate someone's full contact details when you are circulating a title proposal to editors. You may wish to include the authors' name, job title, and institution, but not their mailing address, email, phone number, etc. We suggest you either remove contact information about the authors or perhaps capture contact details separately. Remember to store any documents containing contact details on Archie and not in local folders.
Title registration	Adding new authors	Adding new authors to Archie without them confirming T&Cs, confirming marketing preferences, etc, is not recommended.	Manually adding new authors to Archie is OK as long as you activate all accounts created so they get sent a notification and have to accept T&Cs.
Peer reviewers	Storing potential peer reviewers	Storing full contact details of potential peer reviewers without a specific purpose could breach their data protection rights.	For potential peer reviewers we need to (1) record in a note why we are adding them (2) set a retention policy on keeping them (3) delete them if they never engage (4) inform them when we contact them that we are holding their data and inform them of their rights (5) keep minimal data e.g. name, email, and why you need to store them. Completing a full Archie entry with address, phone numbers, gender etc. all based on online content is not necessary and so wouldn't be legal.
Peer reviewers	Registering peer reviewers who you are contacting	When contacting peer reviewers who you have had no previous contact with you should inform them that they are on our system.	Add text to workflow messages to ensure they are informed about our data protection policies and their rights. ME Support have added this to the templates in workflows.

Peer reviewers	Storing peer reviewer feedback with DOI of peer reviewers	DOI statements are personal data and so have all the GDPR rights attached	Don't store forms locally, store them on Archie. If someone says they want to know what data we hold about them or want us to erase all data we hold on them we can only do this if it is centrally stored. Archie workflows store peer review forms and this is all securely backed up, so there is no need to store copies locally.
Peer reviewers	Storing research interests of peer reviewers in spreadsheets	This information about their interests is personal data and so should be processed in accordance with data protection regulations.	This information should be stored in Archie, preferably using the Topic list tagging or some other Archie feature to collect this information. A key issue here is keeping records up to date: if someone ceases to work with us and their Archie record is deleted on request then all information is removed, but if they are listed in spreadsheets then technically we should be finding any mention of them in spreadsheets and removing them there too... that is the primary argument for avoiding spreadsheets.

5 General best practice points

- Don't store documents locally - Archie provides facilities to store review versions, editorial documents, DOI forms, etc. and so there is no need to store anything locally. Archie is regularly backed up and is secure.
- Don't store unnecessary data. Think before adding data to systems and ask yourself why we need that personal data.
- Use Archie workflows fully. This helps keep as much data as possible stored in Archie where we can ensure data protection compliance.
- Think before you share: does the recipient need all the data? Can personal data be removed?
- Only use spreadsheets where absolutely necessary and where you have processes documented for how you will keep personal data in them up to date and set retention policies for when you no longer need the data. Most spreadsheets serve a temporary process and can be deleted, consider setting calendar reminders to delete temporary spreadsheets created.
- If you come across any personal data that is no longer necessary, delete it.

If you have any questions or concerns about any of the above please contact the Community Support Team in the first instance: Support@cochrane.org