Search for answers...

General Data Protection Regulation (GDPR)

How Cliniko helps you with GDPR compliance.

Written by Emily Gable
Updated today

If you're using Cliniko to manage your practice and handle or process the data of any person who lives within the European Union—even if you're not physically located in the EU—the GDPR rules apply to you.

First things first—and this is the most important thing!—we're working tirelessly to ensure that Cliniko is GDPR-compliant by the deadline—May 25th, 2018.

And we're on track for this deadline! 🙌 We might be a little biased, but Cliniko is a great choice for managing your business if you need to meet the GDPR requirements.

Now, it is a work in progress, and like all things relating to security and privacy, changes take time! This document will be constantly updated as we make changes to accurately reflect how we help you comply with GDPR.

GENERAL

In some cases, we serve as a Processor *and* a Controller. It's our responsibility to ensure that we have the right documentation and procedures in place to support you.

The following outlines how we've done that:

- The establishment of a Data Processing Addendum (DPA).
- Updated our Privacy Policy and Terms of Service.
- Formalised internal company policies with regards to how we handle any of your data.
- Appointed a Data Protection Officer (DPO).
- Hired an EU representative to serve as an additional point of contact for any privacy-related inquiries.
- "Flagging" accounts in the EEA zone (so we can communicate any GDPR-related information to only the relevant parties).
- Ensuring that any third-party vendors we work with also meet GDPR compliance.

Data Processing Addendum (DPA)

This is an additional agreement (separate from our regular Privacy Policy) that you'll agree to, and it means that although Cliniko and its subprocessors aren't *physically* in the EU/EEA, you are still allowed to use Cliniko to manage your patient information.

The DPA includes **Standard Contractual Clauses** (also known as "Model Clauses"). These are an approved set of provisions which offer sufficient safeguards and protection for data that's processed outside of the EU/EEA.

When you are ready, download the Cliniko Data Processing Addendum, sign it, and send it back to us. (There are detailed instructions within the document). The agreement is valid as soon as we receive it.

Updated our Privacy Policy and Terms of Service

We've updated our Privacy Policy and Terms of Service to ensure that the agreements we have in place with you meet the requirements of GDPR, as well!

For example, our servers are located in Australia—but as long as we have the right documentation in place, *this is allowed* by GDPR standards. When you agree to our policies and terms, you're abiding by GDPR's requirements around data that's processed outside of the EEA. This means that despite your patient data being physically stored outside of the EEA zone, you are *still allowed* to use Cliniko.

Formalised internal company policies

We've revised the processes of in-house policies around how we handle your data. This includes protocols for how we access any of your information if requested by you, how we communicate with one another, and how we handle any incoming requests that we might get from your patients regarding their data (we *always* send them straight to you!).

Data Protection Officer (DPO)

We've appointed our own in-house Data Protection Officer (DPO). The roles of our DPO include making sure that Cliniko is compliant with GDPR, serving as an advisor on data protection obligations, and acting as a contact point for data subjects and supervisory authorities.

Our DPO can be contacted at dpo@cliniko.com.

EU representative

As Cliniko has no physical presence in the EU, we've appointed a representative as a point of contact. This complies with Article 27 of the GDPR, and the reason is that a party who actually *lives* in the EU needs to be available to address any questions relating to privacy.

Our EU representative is a company called VeraSafe, and they can be reached via their website, at support@verasafe.com, or by postal mail at:

VeraSafe EU
Zahradníčkova 1220/20A
Prague 15000
Czech Republic

VeraSafe Ireland Ltd
Unit 3D North Point House
North Point Business Park
New Mallow Road
Cork T23AT2P
Ireland

Flagging EEA-zone accounts

Not everyone who uses Cliniko is located in the EU/EEA zone, so we've taken appropriate measures to "flag" those who are. This is purely for our internal knowledge, and will make it easy for us to communicate any GDPR-related information out to those who need to know it.

However, we cannot guarantee that we have captured everyone. **The flagging is based on the location of your Cliniko account**, so if you're physically *outside* of the EU but treating patients *in* the EU (for example, you practice in Australia, but you're doing phone sessions with a patient in France), your account would *not* be initially flagged.

If you're concerned that you may not have been flagged, please let us know and we can double-check!

Ensuring that third-party vendors meet compliance

In order for Cliniko to function, we may have to utilise certain third-party tools ("subprocessors"), and we have ensured that all of them are compliant with GDPR.

The role of these different third-party tools are to help Cliniko run efficiently, such as cloud-based data storage and cloud-based email delivery services. You can learn more about the subprocessors we use here.

CLINIKO AS A PROCESSOR OF DATA

As the *processor* of your data, Cliniko will help you to meet your needs as a *controller*—we provide you with the tools needed to comply with your patients' requests.

Below is a list of requirements related to your use of Cliniko, and how we help you comply with those requirements!

- Remove patients from marketing-related communications.
- Allow for double opt-in with the MailChimp integration.
- Modify patients' personal details.
- Provide patients with a copy of all their personal information.
- Delete all of a patient's information from Cliniko.
- Record whether or not a patient has consented to your clinic's privacy policy.
- Let patients consent to your privacy policy when booking online.

Remove patients from marketing-related communications

If a patient requests to *not* receive marketing-related materials from your clinic (such as marketing emails or SMS messages), you need to be able to *remove* them from any such communication. GDPR calls this the **Right to Object**.

You can customise your patients' preferences by unsubscribing them from SMS marketing, and when sending a group SMS message you can select whether it's "marketing-related" or "need-to-know". If you use the MailChimp integration, archiving or deleting a patient will automatically remove their details from MailChimp, so they'll no longer get marketing emails from you.

Double opt-in if using the MailChimp integration

Rather than automatically subscribe any new patient to your list in MailChimp, we'll be allowing for double opt-in—this means that before a patient will be on the receiving end of any email communications through MailChimp, they will need to first confirm that they wish to *actually be* subscribed to your list.

Double opt-in can be enabled within your MailChimp account. Learn how to set it up here!

Modify a patient's details

A patient may request that you make changes to their information, as it's stored in Cliniko. GDPR defines this as the **Right to Rectification**.

If a patient tells you that their details are incorrect, you can edit anything about that patient in Cliniko!

Provide patients with a copy of all their personal information

☝**This is currently in progress, and we'll update this section when it's fully available!**

A patient may come to you and request a copy of every piece of personal information you have (which is stored in Cliniko). GDPR calls this the **Right to Access**. The information must also be provided to them in an easy-to-read format—and it needs to be portable (meaning, it could easily be transferred/imported to another system). This is defined as the **Right to Portability**.

We'll be making a one-stop shop where you can obtain *every* piece of information for *just one* patient, so you can provide it to them if need be!

Delete all patient information from Cliniko

A patient has the right to request that you remove any and/or all of their personal information from Cliniko. This is what the GDPR defines as the **Right to Erasure** or **Right to Be Forgotten**.

You can *permanently* delete a patient from your Cliniko account. This is important for those who *don't* have a legal requirement to retain records, or if that legal requirement has lapsed. **If you are legally required to retain patient records, we do not advise permanently deleting any patient. You can archive them instead.**

Record patient consent to your privacy policy

If you have a privacy policy for your clinic, you would need to keep track of whether or not your patients have consented to it, and you need to make it clear and easy The GDPR requires that you obtain **lawful consent** from your patients in order to store their personal information

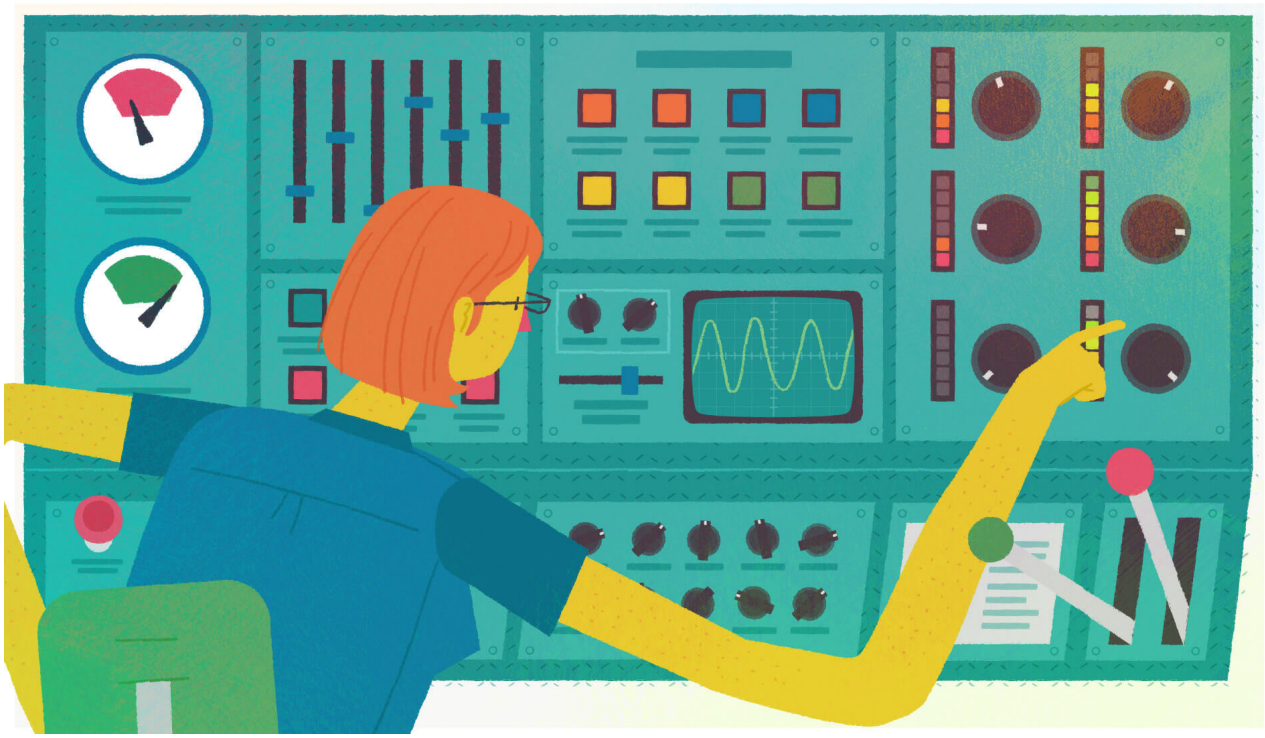
When adding a new patient or editing their details, you can mark off whether a patient has accepted, rejected, or not responded to your clinic's privacy policy.

Let patients consent to your clinic's privacy policy when booking online

Any patient who is booking an appointment through your online bookings page will be required to agree to your privacy policy, *if you include a link to it*.

When they agree to this, their record in your Cliniko account will also be updated to indicate that they have accepted your privacy policy.

CLINIKO AS A CONTROLLER OF DATA



We're also a *controller*, in that we control *your* information that you provide to us—like your email address, business details, and contact information, for example. As a controller, we have the same sorts of responsibilities that you have when it comes to your patients—except we're handling *your* information, not that of your patients.

The ways we comply with our job as a controller include:

- Full deletion of your Cliniko account.
- Allow you to opt out of any marketing-related communications from us.

Check out the specifics of how we help you with GDPR compliance, below!

Full deletion of your Cliniko account

If requested, we can *entirely* delete your Cliniko account. **This is irreversible.** We'll provide you with the tools to download all of your data prior to deleting (such as data exports) but if you do require a full account deletion, please note that it cannot be undone.

This is important for those who *don't* have a legal requirement to retain records, or if that legal requirement has lapsed. **If you are legally required to retain your records, we do not advise full account deletion.**

Allow you to opt out of any marketing communications from us

If you'd prefer to not receive emails from us that don't *explicitly relate to your account*, you can opt out of these. If you opt out, it means that you wouldn't receive any emails about new features we release, for example, but you would still receive an email if your account was past due, or if your SMS credits were low.

Note: this is different to your patients opting out of marketing-related communications *from your clinic*.

As always, if you have any questions about any of this, reach out to our support team via the chat bubble in the lower-right! We'll be more than happy to discuss things with you! 😊

Did this answer your question?