How to Write a Privacy Policy

Introduction

Preserving patient/customer privacy is key to running a trustworthy business. And, if you're a business based in Europe, it's the law.

When running a business, it's important to respect your patients'/customers' privacy rights and follow data protection laws. As a business owner and a podiatrist, you receive certain personal information about patients/customers when they attend an appointment or purchase something or contact you with a query, such as name, postal address, email address, phone number and medical information. The European General Data Protection Regulation (GDPR) and other local data protection laws guard how this kind of personal information is collected and used, and protect the privacy rights of the public. Under these laws, patients/customers are entitled to certain information, including when, why, how, by whom, and for what purpose personal information is collected, used, and shared.

If you are based in the European Union, the GDPR applies to you, which means you're required to have a privacy policy for your business. Read on to learn more about creating a privacy policy for your business — plus an example of what the privacy policy of a simple podiatry practice might look like.

Creating a Privacy Policy for Your Business

Giving your patients/customers information about how and why you're going to use their personal information is the heart of a privacy policy. Below is a guide to creating a privacy policy which has sample extracts which you can bring together to create your own privacy policy. Throughout, we'll point out which parts of the policy address requirements of the GDPR. Once you have created your privacy policy you should make it available in your podiatry practice on the wall and in a leaflet as well as on your website.

The specific needs and practices of each podiatry business are different, so you MUST customise the sample extracts to create your privacy policy so it reflects the needs and practices of your business.

Privacy Policy Guidance

The GDPR requires that you provide certain information to your patients/customers in your privacy policy, including:

- the personal information you collect;
- the legal bases you rely on to collect, use, and share personal information;
- the third parties with whom you share personal information;
- the length of time you keep personal information;
- your patients'/customers' rights regarding your use of their personal information; and
- how your patients/customers can contact you with privacy-related requests.

Based on GDPR requirements, here's how you might introduce your privacy policy to your patients/customers:

This Privacy Policy describes how and when I collect, use, and share information when you attend an appointment at my clinic, purchase a product from me, contact me, or otherwise use my services. This is to comply with the General Data Protection Regulations (GDPR) 2018.

You should then go on to include information on the following:

1. Personal information you collect

You should explain what information you collect from patients/customers, why you need the information, how you use and store it. Here's an example:

Information I Collect

To aid you treatment or as part of purchasing something from my business you will normally provide me with certain information, such as your name, email address, postal address, medical information and payment information. I will store you information on an electronic patient record and diary system which is fully password protected.

2. The legal bases I rely on to collect, use, and share personal information

The GDPR requires that you explain the legal bases you rely on to collect, use, and share personal information. The legal bases may include a patients/customers affirmative consent to receive marketing messages, compliance with legal obligations, and a podiatrist's use of the personal information in their legitimate interests (improving their services, for example). Throughout your privacy policy, you should be as clear as possible about where and why you are relying on these different legal bases. For example:

Why I Need Your Information and How I Use It

I rely on a number of legal bases to collect, use, and share your information, including:

- where it is necessary for the purposes of the provision of health care as needed to provide my services, such as when I use your information to fulfil your podiatry assessment and treatment, or to provide customer support;
- when you have provided your affirmative consent, which you may revoke at any time, such as by signing up for my mailing list;
- if necessary to comply with a legal obligation or court order or in connection with a legal claim, such as retaining information about your purchases if required by tax law;

3. Marketing I undertake for my business

There are a few things you should know before using email addresses to contact your patients/customers, such as sending a newsletter or advertising new products. Under the GDPR you will need prior "express consent" from your patients/customers to send them marketing or promotional messages. Express consent means that you can only

send marketing messages to a patient or customer if they have indicated their consent for you to do so through a clear affirmative action, such as ticking a box to receive marketing messages from you. Even if you get a patient's email address as part of the patient assessment you are required to get their express consent before sending them marketing messages. Remember that even once you have express consent to send marketing messages, you must respect requests to opt out of receiving further marketing messages from you, as consent can be revoked at any time.

If you do market to patients/customers then you should add a marketing section in your privacy notice which they need to fill in. You will also need to add an area for the patient to include their name. You should then keep a copy of this in their patient record. An example of this is:

Marketing

From time to time I may wish to send you direct marketing material which may include product offers and newsletters. If you are happy for me to do this please indicate in what forms you would like to receive this information:

Mail☐ Email ☐ Text ☐ Phone ☐ No Marketing ☐

4. The third parties with whom you share personal information

The GDPR requires that you disclose the details of any personal information you share with third parties. You should explain to your patients/customers why, when, and with whom you may share personal information. For example:

Information Sharing and Disclosure

Information about my patients/customers is important to my business. I share your personal information for very limited reasons and in limited circumstances, as follows:

- Medical professionals. With your consent I will share information with medical professionals such as your GP or consultant to allow continuity of care.
- Service providers. I engage certain trusted third parties to perform functions and provide services to my business, such as external reception services. I will share your personal information with these third parties, but only to the extent necessary to perform these services.
- Business transfers. If I sell or merge my business, I may disclose your information as part of that transaction, only to the extent permitted by law and with your consent.
- Compliance with laws. I may collect, use, retain, and share your information if I am legally required to.

5. The length of time you keep personal information

The GDPR requires you to disclose the period of time during which you will store personal information. You should consider how long the needs to retain information for business purposes and to comply with any legal or tax obligations, and keep in mind that data shouldn't be kept for any longer than necessary. For example:

Data Retention

I retain your personal information only for as long as necessary to provide you with my services and as described in my Privacy Policy. However, I may also be required to retain this information to comply with my legal and regulatory obligations, to resolve disputes, and to enforce my agreements. The retention of podiatry records is normally a minimum of 8 years, after the last appointment. For customers who are not patients but may have bought products from my business I will keep any data you may have provided for a minimum of 6 years in line with tax legislation.

6. If transferring personal information outside of Europe, how the transfer will be handled

GDPR requires you to disclose if you transfer personal information outside of the EU and the legal bases you rely on to do so, such as consent and contractual necessity. For example if you have a Cloud based server you need to check where the information is held as this may be outside the EU. Some Cloud servers are Privacy Shield certified, so you should explain that you rely on Privacy Shield as the legal basis for the transfer of his buyers' personal information outside of the EU. For example:

Transfers of Personal Information Outside the EU

I may store and process your information through third-party hosting services in the US and other jurisdictions. As a result, I may transfer your personal information to a jurisdiction with different data protection and government surveillance laws than your jurisdiction. If I am deemed to transfer information about you outside of the EU, I rely on Privacy Shield as the legal basis for the transfer, as X Cloud is Privacy Shield certified.

7. Your patients'/customers' rights regarding your use of their personal information and your contact details

Based on GDPR requirements, you should finish by explaining to your patients/customers their rights regarding the information they provide. You should also provide your contact details and explain that you are the data controller of their personal information. For example:

Your Rights

You have a number of rights in relation to your personal information. While some of these rights apply generally, certain rights apply only in certain limited cases. I describe these rights below:

- Access. You have the right to access and receive a copy of the personal information I hold about you by contacting me using the contact information below.
- Change, restrict, delete. You may also have rights to change, restrict my use of, or delete your personal information. In the case of health records these are normally exempt from change and deletion requests.
- Object. You can object to (i) my processing of some of your information based on my legitimate interests and (ii) receiving marketing messages from me after providing your express consent to receive them. In such cases, I will delete your

personal information unless I have compelling and legitimate grounds to continue using that information or if it is needed for legal reasons.
- Complain. If you wish to raise a concern about my use of your information (and without prejudice to any other rights you may have), you have the right to do so with the Information Commissioner www.ico.org.uk

How to Contact Me

For purposes of the GDPR, I, (enter name), am the data controller of your personal information. If you have any questions or concerns, you may contact me (enter email address). Alternately, you may mail me at:

(enter address)

Conclusion

This privacy policy is intended to be a guide to the information that should be included in a privacy policy. If you use this policy as a template for your own, you should customise it so it makes sense for your business. You can replace the details in this policy with yours, including your name, business name, email address, and newsletter settings (if you have an email newsletter). The sections entitled “Why I Need Your Information and How I Use It” and “Transfers of Personal Information Outside the EU” must be customised based on how you operate your business. Adjust the wording to reflect your practice set up and add or remove information to reflect specific facets of your business. For example, if you’re a joint business owner, you can change the pronouns from “I” and “me” to “we” and “us” to more accurately represent your business.

By creating a privacy policy for your business it will ensure that you comply with your obligations under the GDPR, and will signal to patients/customers that you take privacy seriously and have their best interests at heart.

Below is a full template of the sample extracts; however you will still need to amend it to suit your practice set up.

Sample Privacy Notice Full Template

YOU MUST AMEND THIS TO SUIT YOUR PRACTICE

This Privacy Policy describes how and when I collect, use, and share information when you attend an appointment at my clinic, purchase a product from me, contact me, or otherwise use my services. This is to comply with the General Data Protection Regulations (GDPR) 2018.

Information I Collect

To aid your treatment or as part of purchasing something from my business you will normally provide me with certain information, such as your name, email address, postal address, medical information and payment information. I will store your information on paper patient record which are securely locked away in my absence and electronic diary system which is fully password protected.

Why I Need Your Information and How I Use It

I rely on a number of legal bases to collect, use, and share your information, including:

- where it is necessary for the purposes of the provision of health care as needed to provide my services, such as when I use your information to fulfil your podiatry assessment and treatment, or to provide customer support;
- when you have provided your affirmative consent, which you may revoke at any time, such as by signing up for my mailing list;
- if necessary to comply with a legal obligation or court order or in connection with a legal claim, such as retaining information about your purchases if required by tax law;

Marketing

From time to time I may wish to send you direct marketing material which may include product offers and newsletters. If you are happy for me to do this please indicate in what forms you would like to receive this information:

Mail☐ Email ☐ Text ☐ Phone ☐ No Marketing ☐

Information Sharing and Disclosure

Information about my patients/customers is important to my business. I share your personal information for very limited reasons and in limited circumstances, as follows:

- Medical professionals. With your consent I will share information with medical professionals such as your GP or consultant to allow continuity of care.
- Service providers. I engage certain trusted third parties to perform functions and provide services to my business, such as external reception services. I will share your personal information with these third parties, but only to the extent necessary to perform these services.

- Business transfers. If I sell or merge my business, I may disclose your information as part of that transaction, only to the extent permitted by law and with your consent.
- Compliance with laws. I may collect, use, retain, and share your information if I am legally required to.

Data Retention

I retain your personal information only for as long as necessary to provide you with my services and as described in my Privacy Policy. However, I may also be required to retain this information to comply with my legal and regulatory obligations, to resolve disputes, and to enforce my agreements. The retention of podiatry records is normally a minimum of 8 years, after the last appointment. For customers who are not patients but may have bought products from my business I will keep any data you may have provided for a minimum of 6 years in line with tax legislation.

Transfers of Personal Information Outside the EU

I may store and process your information through third-party hosting services in the US and other jurisdictions. As a result, I may transfer your personal information to a jurisdiction with different data protection and government surveillance laws than your jurisdiction. If I am deemed to transfer information about you outside of the EU, I rely on Privacy Shield as the legal basis for the transfer, as X Cloud is Privacy Shield certified.

Your Rights

You have a number of rights in relation to your personal information. While some of these rights apply generally, certain rights apply only in certain limited cases. I describe these rights below:

- Access. You have the right to access and receive a copy of the personal information I hold about you by contacting me using the contact information below.
- Change, restrict, delete. You may also have rights to change, restrict my use of, or delete your personal information. In the case of health records these are normally exempt from change and deletion requests.
- Object. You can object to (i) my processing of some of your information based on my legitimate interests and (ii) receiving marketing messages from me after providing your express consent to receive them. In such cases, I will delete your personal information unless I have compelling and legitimate grounds to continue using that information or if it is needed for legal reasons.
- Complain. If you wish to raise a concern about my use of your information (and without prejudice to any other rights you may have), you have the right to do so with the Information Commissioner www.ico.org.uk

How to Contact Me

For purposes of the GDPR, I, Meeta Patel, am the data controller of your personal information. If you have any questions or concerns, you may contact me info@premierfootvlinic.co.uk. Alternately, you may mail me at:

Station Road wellness centre

12 Station Road

EPPING

CM16 4HN