How Shall I Write to My Patient? Data Protection in Digital Communication

Georg W. Alpers a,b, Lisa Frey b, Stephanie Tessmer-Petzendorfer c, Anna Klingauf a, Silvia Schad b

 a Lehrstuhl für Klinische und Biologische Psychologie und Psychotherapie, Fakultät für Sozialwissenschaften, Universität Mannheim, Mannheim, Deutschland; b Psychologische Ambulanz, Otto-Selz-Institut, Universität Mannheim, Mannheim, Deutschland; c Landespsychotherapeutenkammer Baden-Württemberg, Stuttgart, Deutschland

Abstract

Digital communication is omnipresent. In everyday life, social messenger apps are very popular. Thus, for some patients it seems intuitive to use such media to correspond with their professional therapists as well. From a practical perspective, this seems to be advantageous for the therapists themselves. However, this should not lead us to overlook the problems of such platforms, especially issues with data protection. In spite of the legally binding rollout of a safe communication route for therapeutic and medical services in Germany (the so-called “Telematik-Infrastruktur”), so far, there is no unproblematic communication platform for therapists and their patients. Special messenger apps, which explicitly do not store metadata, seem to be the least problematic besides classic phone calls or letters. However, they are not yet widely used. This paper aims to sensitize psychotherapists for their responsibility and to demonstrate technical options, which need to be weighed carefully in order to maximize data protection of digital communication in therapeutic practice.

© 2020 S. Karger AG, Basel

Keywords

Datenschutz in der Psychotherapie · Digitale Kommunikation · Elektronische Kommunikation · Soziale Messenger-Dienste

Zusammenfassung

Digitale Kommunikation ist aus dem Alltag nicht mehr wegzudenken; im privaten Bereich sind insbesondere soziale Messenger-Dienste weit verbreitet. So scheint es für manche Patienten nahliegend zu sein, solche Kommunikationsmittel auch für die Kommunikation mit ihren professionellen Behaltern zu verwenden. Aus organisatorischen Gründen scheint dies auch für Psychotherapeuten Vorteile mit sich zu bringen; dies darf jedoch nicht unreflektiert dazu führen, die enormen Probleme solcher Plattformen, insbesondere mit Blick auf den Datenschutz, aus den Augen zu verlieren. Trotz rechtlich verpflichtender Einführung der Telematik-Infrastruktur in der ambulanten vertragspsychotherapeutischen/vertragsärztlichen Versorgung existiert bisher keine unproblematische

1 Patients and psychotherapists are referred to in this article by the generic masculine, which means all genders.
The new potentials of digital communication by e-mail or social media permeate our private lives; in Germany, 90% of the population currently have private access to the Internet [Statistisches Bundesamt, 2019]; e-mail and messenger services in particular are used by most citizens [Schlobinski and Siever, 2018]. As in many areas of life, expectations of uncomplicated and rapid digital communication between patients and their practitioners are increasing in the health care sector. This is shown, for example, in patient comments on rating portals, where most patients today take for granted the accessibility of their caregivers by e-mail, and a direct communication option via WhatsApp or SMS is praised as a positive feature of a practice [Czeschik, 2017]. The desire has obviously increased to be able to ask a question outside of regular therapy sessions or to make or postpone an appointment outside of office hours [Berliner Beauftragte für Datenschutz und Informationsfreiheit, 2015]. Many psychotherapists therefore find it reasonable to accommodate their patients’ communication habits. In view of the increasing bureaucratic burden on them, practitioners could also benefit from establishing faster communication channels with their patients. Digital media are obviously unbeatable in directness and speed compared to confidential communication by mail.

When the Kassenärztliche Bundesvereinigung (National Association of Statutory Health Insurance Physicians) surveyed a large stratified sample of medical and psychotherapeutic practice owners, they found that in recent years 54% of all medical and psychotherapeutic practices used e-mail and 16% used SMS or messenger apps to communicate with patients [Kassenärztliche Bundesvereinigung, 2018b]. The frequency of use of e-mail (69%) and SMS or messenger apps (32%) was particularly high in psychotherapeutic practices. Patients in psychotherapy also use digital media frequently [Kalckreuth et al., 2014]. The use of digital technologies has also grown explosively in psychotherapy in recent years [Mühleberger et al., 2009], and by the time you read this article, the numbers cited above will have certainly been long since exceeded.

Nevertheless, most users are aware that digital media have glaring gaps in their data protection [Mertz et al., 2016]. Especially against the background of the new General Data Protection Regulation (GDPR; Regulation [EU] 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data, on the free movement of data, and on the repeal of Directive 95/46/EC-GDPR), which has been in force since May 25, 2018, all users of digital communication media – but to an increasing extent psychotherapists when practicing their profession – must handle these media with particular care.2 It must be generally assumed that greater convenience is often bought at the expense of an enormous increase in the data protection risk.

Data protection risks are particularly problematic in the psychotherapist’s professional practice, because communication between psychotherapists and their patients is subject to special confidentiality obligations and particularly high data protection requirements must be met [Kassenärztliche Bundesvereinigung, 2018a]. In the offices of psychotherapists in private practice, it is usually easy to achieve the required confidentiality; arrangements or consultations by telephone are protected by the telecommunications secrecy law (§88 Telecommunications Act [TKG]). Anyone who also wants to offer their patients modern digital forms of communication must take additional precautions to ensure that the security and confidentiality of patient data are maintained [Jenkins, 2015].

Whether communication between psychotherapist and patient by e-mail, SMS, or Messenger is permitted under the data protection law and how secure these digital communication methods are has not yet been communicated sufficiently clearly in the training of psychotherapists [Vogel and Alpers, 2009], and there are published examples of the fact that the importance of data protection in the everyday life of health care professions is often glaringly underestimated [Ubel et al., 1995; Vigod et al., 2003]. In this article, we provide a general overview of the legal and technical foundations, point out the most important risks, and offer proposals for the practical implementation of data protection. The article deals with aspects of digital communication in conventional settings

2 Although this article presents considerations about legal principles – particularly about data protection – this is for general information only and does not constitute binding legal information. Of course, reading this article is no substitute for reflecting on your own professional actions. Our text is no substitute for binding legal advice either; liability is excluded to the extent permitted by law. In contrast to the considerations compiled here as a general overview, individual circumstances, new technical developments, legal publications, or the development of case law may lead to different assessments. The descriptions of apps and the data protection guidelines are not exhaustive and serve only as illustrations; they are not intended to be a comprehensive product description or critique.

DOI: 10.1159/000508713

2020 S. Karger AG, Basel
of outpatient psychotherapy. The potentials and limitations of Internet-based interventions [Alpers et al., 2014], which we have dealt with elsewhere [e.g., Winzelberg et al., 2003], are not discussed here. It must also be shown separately which security requirements have to be met for so-called remote treatment [Ärzteblatt, 2018]. Here we cannot go into the special research and therapy methods for outpatient assessment either that can benefit from modern digital technologies [Alpers, 2009; White et al., 2014]. Finally, it should be noted that the special requirements for data protection in research [Müller, 2018], as well as its special privileges [Schwartmann and Hermann, 2018], must be omitted here. For a comprehensive look at basic ethical principles, refer to more comprehensive texts [Tribe and Morrissey, 2015].

**Duties of the Psychotherapist**

The legal requirements for data protection in psychotherapeutic practice are clearly defined. The professional codes of the professional associations and chambers as well as the GDPR and the corresponding paragraphs of the German Criminal Code (StGB) are of particular importance in this context.

The professional codes are standardized for each state, taking into account the model professional regulations of the Federal Chamber of Psychotherapists or the German Medical Association. For example, the professional code of the State Psychotherapy Chamber of Baden-Württemberg (BO LPK BW) stipulates an obligation for all psychotherapists who are members to observe the applicable data protection laws. The same applies to the other state chambers of psychotherapy. Psychotherapists are required to take appropriate security and protection measures to prevent the unauthorized collection, storage, modification, transmission, blocking, and deletion of data that have come their way in connection with their professional practice. It should be especially noted that the fact that a person is undergoing psychotherapeutic treatment is a secret worthy of protection and is therefore subject to confidentiality requirements (§7 BO LPK BW). In digital communication between psychotherapist and patient, this means that not only the content of the communication, but also the fact that such a communication is occurring, deserves protection.

Psychotherapists are further obliged to document all essential therapeutic measures and their effects, as well as explanations given and consents received, in a complete written or electronic file (§11 BO LPK BW). Since SMS or Messenger texts are usually not printed out, it is not generally possible to ensure that they are documented.

The GDPR sets strict requirements for the processing of personal data, and the national data protection legisla-

of outpatient psychotherapy. The potentials and limitations of Internet-based interventions [Alpers et al., 2014], which we have dealt with elsewhere [e.g., Winzelberg et al., 2003], are not discussed here. It must also be shown separately which security requirements have to be met for so-called remote treatment [Ärzteblatt, 2018]. Here we cannot go into the special research and therapy methods for outpatient assessment either that can benefit from modern digital technologies [Alpers, 2009; White et al., 2014]. Finally, it should be noted that the special requirements for data protection in research [Müller, 2018], as well as its special privileges [Schwartmann and Hermann, 2018], must be omitted here. For a comprehensive look at basic ethical principles, refer to more comprehensive texts [Tribe and Morrissey, 2015].

**Duties of the Psychotherapist**

The legal requirements for data protection in psychotherapeutic practice are clearly defined. The professional codes of the professional associations and chambers as well as the GDPR and the corresponding paragraphs of the German Criminal Code (StGB) are of particular importance in this context.

The professional codes are standardized for each state, taking into account the model professional regulations of the Federal Chamber of Psychotherapists or the German Medical Association. For example, the professional code of the State Psychotherapy Chamber of Baden-Württemberg (BO LPK BW) stipulates an obligation for all psychotherapists who are members to observe the applicable data protection laws. The same applies to the other state chambers of psychotherapy. Psychotherapists are required to take appropriate security and protection measures to prevent the unauthorized collection, storage, modification, transmission, blocking, and deletion of data that have come their way in connection with their professional practice. It should be especially noted that the fact that a person is undergoing psychotherapeutic treatment is a secret worthy of protection and is therefore subject to confidentiality requirements (§7 BO LPK BW). In digital communication between psychotherapist and patient, this means that not only the content of the communication, but also the fact that such a communication is occurring, deserves protection.

Psychotherapists are further obliged to document all essential therapeutic measures and their effects, as well as explanations given and consents received, in a complete written or electronic file (§11 BO LPK BW). Since SMS or Messenger texts are usually not printed out, it is not generally possible to ensure that they are documented.

The GDPR sets strict requirements for the processing of personal data, and the national data protection legisla-
al service providers, with whom an order-processing contract in accordance with Art. 28 GDPR must generally be concluded, taking into account the unique features of psychotherapy. Of course, passwords should also be chosen carefully and changed regularly.

The next aspect is the encryption of messages, which ensures that the content of a message cannot be intercepted by unauthorized third parties. It is important to distinguish here which parties have the key that is needed to encrypt and decrypt the messages. With some encryption methods, the provider of the communication service has the key and can theoretically access the content of the messages. Only with so-called end-to-end encryption is this not the case, which is why it is recognized as secure [Bundesamt für Sicherheit in der Informationstechnik, 2019a].

In addition to the direct content of the message, the so-called metadata of a communication are also important, such as information about who is communicating with whom and how often. Such metadata may also contain personal data, such as the location and telephone number of the participants. The processing and use of these metadata are also important criteria with regard to data protection, since they provide information on the communicative exchange between psychotherapist and patient and thus on a possible treatment relationship. It might be argued that a visit to a psychotherapeutic practice reveals similar information, but such occasional observations are usually not documented and stored in databases indefinitely, which in turn constitutes a data protection problem.

Care is required for every digital communication between psychotherapist and patient, and there are multiple data protection risks encountered in daily practice. Since the mere fact that a person is undergoing psychotherapeutic treatment can be regarded as health-related information that may not be disclosed, special precautionary measures must be taken that many users ignore in their private contacts. In addition to the explicit disclosure of data, the implicit information about the treatment relationship is also relevant.

E-mail, SMS, and various social media apps differ greatly in their security and handling of personal data. Table 1 gives an overview of the methods presented, which are explained individually below.

The user frequency of messenger apps in particular is increasing rapidly, so WhatsApp, Signal, Telegram, and Threema are presented from a legal data protection perspective. There is also a number of other messengers (such as Hoccer, Wire), but to list all of them would go beyond the scope of this article. The Verbraucherzentrale (Consumer Advice Center) [2019] provides a general overview.

**Table 1. Security of some common digital communication channels**

<table>
<thead>
<tr>
<th>Method</th>
<th>Encryption</th>
<th>Storage of metadata</th>
<th>Disclosure of metadata</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unencrypted e-mail</td>
<td>none</td>
<td>yes</td>
<td>depending on the provider</td>
<td>no</td>
</tr>
<tr>
<td>Encrypted e-mail</td>
<td>end-to-end</td>
<td>yes</td>
<td>depending on the provider</td>
<td>limited¹</td>
</tr>
<tr>
<td>SMS</td>
<td>transmission only</td>
<td>yes</td>
<td>only to authorities</td>
<td>limited</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>end-to-end</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Signal</td>
<td>end-to-end</td>
<td>yes</td>
<td>unclear</td>
<td>no</td>
</tr>
<tr>
<td>Telegram</td>
<td>partly end-to-end</td>
<td>yes</td>
<td>unclear</td>
<td>no</td>
</tr>
<tr>
<td>Threema</td>
<td>end-to-end</td>
<td>no</td>
<td>only to authorities²</td>
<td>yes</td>
</tr>
</tbody>
</table>

¹ When both sides are using a secure e-mail provider that does not evaluate metadata. ² Since metadata are not stored permanently, their disclosure is virtually impossible.

**E-Mail as Digital Postcards**

When a regular e-mail is sent, it is usually transmitted over the Internet unencrypted. Several servers are usually involved, and the security of an unencrypted e-mail is thus more comparable to sending a postcard than to sending a letter [Bundesamt für Sicherheit in der Informationstechnik, 2019b]. Its content is not secured, and the service providers can read, process, and, if desired, pass it on to third parties as it makes its way over the Internet. Even more than with postcards, personal data can be stored indefinitely on untraceable servers – especially if the servers are located outside the EU. Unlike with telephone calls, it is often not evident who has access to a private e-mail account, since many private users adopt names other than their own (so-called aliases) and often several family members use the same PC.

Although in Germany the TKG says that providers may not pass on information about a communication to third parties, the regulations do not guarantee this aspect of data protection. Even though the communication be-
between patient and therapist mainly takes place in Germany, this territorial connection is not always the case in digital communication. Not all providers of e-mail services are bound by German law. For example, the prominent provider Google, with reference to the laxer data protection laws of the USA, reserves the right to evaluate and further process communication relationships [Google LLC, 2018]. In the case of servers located in the USA, American law (for example, the Patriot Act) makes it possible for the American authorities to access stored data without a court order. The writer often cannot determine what data protection precautions underlie which e-mail services. Unencrypted e-mails are therefore in principle not suitable for communication between psychotherapist and patient.

**Encrypted E-Mails**

It is possible to encrypt e-mails by additional processing steps [Bundesamt für Sicherheit in der Informationstechnik, 2018]. S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy), for example, are currently available for encryption of the entire information flow (end-to-end). According to the current state of knowledge, this type of encryption can be classified as secure [Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, 2019]. However, such e-mails can only be exchanged between people or devices if they use the same method.

In addition to these mostly fee-based offers, there are also free and open-source versions, e.g., OpenPGP as an open-source equivalent to PGP. The Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) [2019a] provides instructions on how to use these services; however, setting up such methods often involves a certain organizational effort, since additional software packages or plugins have to be installed [Bundesamt für Sicherheit in der Informationstechnik, 2018]. Therefore, this form of encryption is more suitable for frequent e-mail traffic with the same partners, such as referring physicians; it is not very practical for communication with patients. Furthermore, only the content of the e-mail can be encrypted with such methods, but not the connection data. These so-called metadata will continue to be transmitted in readable form and can be systematically stored by the service provider and analyzed accordingly [Wendt, 2014]. Given the background discussed above, that the fact that a psychotherapist (or doctor) is being consulted is itself confidential, this is particularly problematic if the psychotherapist’s e-mail address can be used to determine his function. The rules for storage, processing, and disclosure of the metadata are based on the terms and conditions of the particular e-mail provider. We can assume a high level of interest in health data on the part of the providers [Singer, 2018]. For this reason, this method is also only suitable for secure communication if both communicating parties use secure providers or can take special precautions to remain anonymous to their e-mail provider. This is hardly realistic on the part of the patient, but can, under certain circumstances, be arranged between two professionals — e.g., a supervisee and supervisor — and set up professionally in structured interventions with e-mail support [see, e.g., Svartvatten et al., 2015; Königbauer et al., 2017; Zagorscak et al., 2018]. Due to the effort involved, however, this seems to be of limited practicality for regular use.

**Short SMS Texts as a Compromise**

When sending a short text as an SMS (Short Message Service, via smartphone), the mobile operators have both metadata about the mobile phone number and identity of the sender and the recipient, as well as the entire content of the SMS. Compared to e-mail, however, it is advantageous that the mobile operators operating in Germany are subject to telecommunications secrecy regulations in accordance with §88 TKG. Although the SMS connection data are stored by the provider, they are not systematically analyzed or resold. They can only be passed on to authorities, in a separately regulated manner, in exceptional cases and under strict legal conditions (especially in a criminal prosecution).

Since there is no end-to-end encryption in SMS texts, they could theoretically be vulnerable and decrypted, although that requires a relatively sophisticated targeted attack on the data of the provider [Luchtmann et al., 2016]. The use of SMS for communication between psychotherapist and patient cannot therefore be recommended without reservation, but it does represent a compromise and can therefore be used sparingly, e.g., for appointment reminders or cancellations. The patient should refrain from mentioning the reason for the appointment when setting it up, however. Of course, the therapy-related content should never be communicated via SMS. It is noteworthy, however, that some practice management software includes the option of automatically sending appointment reminders via SMS. A prerequisite for this should be a declaration of consent from the patient.

**Data Big Differences among Messenger Apps**

**Messages Collection in WhatsApp**

Messages sent through the most popular messenger app, WhatsApp, have been encrypted end-to-end by default since 2016 [WhatsApp Inc., 2017]; the content of the messages can therefore not be read or evaluated by the
provider. However, WhatsApp systematically stores a lot of metadata in unencrypted form, such as the time of communication and the frequency and duration of the activities and interactions, and links this information of the communication partners [WhatsApp Inc., 2019]. The server is located in the USA, so it is possible for the US authorities to access the stored data (see above).

Users of the app give WhatsApp access to the entire address book of the smartphone being used and agree that the company or its partners (WhatsApp was acquired by Facebook in 2015) may synchronize data such as names and phone numbers. According to Art. 4 GDPR, this qualifies as processing of personal data and would be regarded as a data protection violation without the consent of all(!) those whose information is stored in the address book (just think of the enormous dimension of data protection violations that occurs when address books automatically collect contact information, e.g., from an e-mail program). Without the consent of all those listed in the address book, this could even lead to a warning to a WhatsApp user, who commonly illegally passes on the personal data of others from his address book without their consent [Verbraucherzentrale, 2018]. A psychotherapist should not make himself vulnerable in this way in his professional practice. WhatsApp is therefore not at all suitable for communication between psychotherapist and patient. We think it worth emphasizing that psychotherapists should not save the telephone numbers and contact information of their patients in the address book of a device with which they also use WhatsApp, even privately. Otherwise, patient data in the psychoptherapist’s area of responsibility that is worthy of protection would be automatically and illegally passed along to WhatsApp. For this reason, the use of WhatsApp in patient communications should not be considered a responsible professional ethical approach.

In addition to WhatsApp, there are similar services that explicitly distinguish themselves from the market leader in their handling of data.

**Transparent Signal**

Signal is a free messenger app from Open Whisper Systems, which developed the popular encryption “signal protocol” [Cohn-Gordon et al., 2017]. The communication is encrypted end-to-end with Signal as well; in contrast to most other messenger apps, Signal’s entire programming code is open source. This is relevant because it has enabled an independent assessment of the app’s security and, along with the protocol used, has been rated as secure [Cohn-Gordon et al., 2017].

One drawback of Signal is that the user must provide his mobile phone number for identification, which violates complete anonymity with respect to the provider. Signal also requires access to the address book during installation in order to find other users of the app and link them to the new user. But these address data are not stored unencrypted on the server as it is with WhatsApp [Open Whisper Systems, 2018]. Instead, the mobile phone numbers from the address book are encrypted and sent to the server in a form that is not directly usable, with checksums (so-called hashes) and not stored there [Open Whisper Systems, 2018]; the original mobile phone number could only be reconstructed with great effort.

It is an obstacle to communication with patients that Signal does not offer a German data privacy statement, nor does the official website provide any precise information about which metadata Signal collects and stores and how these data are used. The Verbraucherzentrale consumer advice center therefore points out that Signal reserves the right to disclose data to third parties under certain circumstances, and that the company is based in the USA and is subject to the laws of that country [Verbraucherzentrale, 2019], which means that there can be access by the US authorities. For these reasons, Signal is not recommended for communication between psychotherapist and patient.

**End-to-End Encryption Is Not Standard with Telegram**

Telegram Messenger is sometimes mentioned as a more secure alternative to WhatsApp. Contrary to this assumption, texts sent via this free messenger app are not end-to-end encrypted by default. Only so-called “secret chats” offer end-to-end encryption [Telegram, 2019a]. In order to use consistent encryption, the user must actively switch to another mode, but is not explicitly advised of this when installing the app. In such secret chats there is an additional function that deletes messages after a specified time. As with Signal, however, you must provide your own telephone number and first name, which does not allow complete anonymity with respect to the provider. As with WhatsApp, Telegram also requires access to the address book and stores the phone numbers and the first and last names of the contacts [Telegram, 2019a]. Such contact synchronization can be actively refused, but this makes the app unusable on some smartphones (e.g., iOS devices).

The originally Russian provider of Telegram is now based in Dubai, United Arab Emirates [Telegram, 2019b]. Unlike Signal, during installation Telegram offers a data protection guideline mostly translated into German [Telegram, 2019a], which initially makes the handling of data more transparent for German users. However, Telegram does not list all the forms of metadata that it stores [Telegram, 2019a], nor does it show how Telegram handles the metadata it collects. It should not be assumed that all users are so adept in using the medium that they reliably use only secret chats for communication. Therefore,
this messenger is not classified as suitable for communication between psychotherapist and patient either.

No Data Traces in Threema

The Swiss app Threema has a good reputation among data protection specialists. Besides end-to-end encryption, Threema offers the option of using the messenger anonymously [Threema, 2019a, b]. This means that it is not absolutely necessary for patients’ contact with a psychotherapist to reveal their treatment relationship to the provider of the app [Berliner Beauftragte für Datenschutz und Informationsfreiheit, 2015].

During registration, a random 8-digit ID is generated, which is used for identification and can be exchanged between the communication partners on their own initiative. An additional advantage is that the practitioner can avoid giving his (possibly private) mobile phone number to the patient. Synchronizing the address book is also optional with Threema, in comparison to WhatsApp and Signal. According to the company’s self-disclosure, it also refrains from permanently storing metadata [Threema, 2019c]. To ensure that the communication partner is actually who he appears to be, Threema offers authentication by scanning a barcode from the display of the partner’s mobile. If the practitioner uses the Threema Work variant to communicate with his patients, private and professional communication can remain separate and the risk can be minimized of inadvertently passing on private information to patients or patients’ confidential information to private contacts.

The headquarters of the company and its servers are located in Switzerland and are therefore subject to the Swiss federal law on the monitoring of postal and telecommunications traffic (BÜPF). Threema would therefore be obliged to release all available data to the authorities on request, but since the metadata of the communication processes are not stored permanently, it would not be possible to release them [Threema, 2019c].

A disadvantage of Threema is that the app is not open source, so the program code is not available for a security check by a third party. Furthermore, unlike WhatsApp, Signal, and Telegram, Threema is not free of charge, but there is a one-time cost of at least EUR 2.99, depending on the provider (as of February 2019). The points mentioned above regarding encryption and anonymity, as well as the renunciation of the storage of metadata, make Threema a user-friendly messenger app that is acceptable for communicating clearly limited content between psychotherapist and patient. Since the company is based in Switzerland, the provider must contractually undertake to comply with the GDPR in accordance with Art. 44 GDPR (General Principles of Data Transmission); the provider’s self-declaration says this is complied with [Threema, 2019a].

Special Instances of Digital Communication

Inquiries from Patients

Even if it has been explicitly agreed with a patient that digital communication may only be used, for example, to make an appointment, it still happens that patients send a confidential request by e-mail, SMS, or a messenger service. For example, in our experience, they ask therapy-related questions or provide information about their symptoms. Such an inquiry does not necessarily have to remain unanswered, since this can leave an unprofessional impression and strain the therapeutic alliance. Such inquiries should always be answered, however, with a note that you do not want to discuss any questions of content via this medium and asking for a phone call or inviting them to make a personal appointment. The patient’s (confidential) text should always be deleted in the practitioner’s reply.

Documentation Requirements for Psychotherapists

If a patient expands communication to include therapy-related content, psychotherapists are obliged to document and store essential treatment data in accordance with the relevant professional code (e.g., §11 for psychotherapists in Baden-Württemberg). Thus, when using SMS and messenger texts, it should be taken into account that the messages cannot be printed out and so the documentation must be retyped.

The same applies to the destruction of communication data, for example on the smartphone. If there is no obligation to preserve documentation and records, these must be destroyed properly so that the data cannot be reconstructed. This means that, for example, a smartphone would have to be destroyed by a certified specialist company according to DIN 66399 and the requirements of Art. 28 GDPR. The psychotherapist should take this into account when choosing his communication media.

Adolescent Patients

Adolescent patients, as digital natives, are often quite accustomed to using digital communication channels and at the same time are particularly vulnerable [Murray, 2014]. In our experience, schools and other institutions may lack awareness of the data protection problems posed by using digital technologies in a professional context. If relevant, special attention should be paid to explaining about potential risks. For minors who are unable to give their consent with regard to the right to informational self-determination, the consent of the parent or guardian is required. This is also required under Art. 8 of the GDPR; for information society services that are offered directly to a minor who has not yet reached the age of 16, the consent of the parent or guardian is required.
Table 2. Ten commandments of digital communication for practitioners

1. Comprehensive patient education about the risks of digital communication

2. Written consent of the patient to use a specific communication medium for a defined purpose (for minors who are unable to give consent, the consent of the guardian is required)

3. Keeping the operating system and secure virus protection program up to date on PC and smartphone

4. Encryption of the e-mail communication

5. On the smartphone: no apps like WhatsApp that read address books

6. Restriction of all digital communication to what is necessary, e.g., to make an appointment; if possible, no transmission of therapy-related content

7. Regular review of the communication media being used for changes relevant to data protection law (e.g., for updates)

8. All data-processing steps must be documented

9. Communicating to patients that psychotherapists cannot always be online and accessible

10. First think about data protection, then send

Consequences of digital communication

Within the scope of digital communication, there are always two sides: There is the excitement of e-mail, SMS, and messenger services in our everyday life. The Internet is regarded as a particularly convenient medium, but its use in psychotherapy requires consideration. For the psychotherapist and for the therapeutic approach, it is almost as old as the introduction of e-mail itself [Shapiro and Schulman, 1996; Bradley et al., 2011]. Although there are still no reliable data about this, it would of course not be possible for psychotherapists to guarantee their permanent availability.

Conclusion: Benefit versus Risk

Great caution is generally required in digital communication between psychotherapist and patient. Without claiming to be complete, the critical points can be summarized as 10 commandments of digital communication for practitioners (Table 2). Omnipresent services such as WhatsApp, which at first glance may appear reasonably secure due to their end-to-end encryption, can on closer inspection pose a significant data protection problem. Before using communication methods, psychotherapists should obtain information about their security, to effectively protect patients’ data and safeguard their rights. The services of the Federal Office for Information Security and Consumer Protection are reliable sources of information. It is also wise to carefully study the data protection statements of the services under consideration. Of course, there is no absolute security even with encrypted digital communication; a specialist journalist sums it up succinctly: “To be clear and concise: someone’s always watching” [Litman-Navarro, 2019]. However, digital communication media can be used if explanations, consent, and adequate encryption are provided. Due to the hurdles mentioned above, it should be carefully considered for each individual case whether and under what conditions digital communication is advisable.

Communication by unencrypted e-mail, WhatsApp, Telegram, or Signal is inadvisable in the psychotherapeutic context. Communication via encrypted e-mails (using a secure e-mail provider), SMS, or the Threema messenger app, on the other hand, can be regarded as comparatively secure for selected purposes. The content of the communication, however, should be limited to what is absolutely necessary and, if possible, no therapy-related information should be exchanged. There is no replacement for personally addressed letters and personal phone calls (not by voicemail), despite the rapid progress in digital technologies. In the medium term, it would be desirable to have a unified, rapid, and secure communication method for every type of content. Hope has been placed in the long-awaited telematics infrastructure for this reason. It will offer the possibility of encrypted e-mail communication between practitioners [the so-called “KOM-LE,” according to the GKV-Spitzenverband and Deutsche Krankenhausgesellschaft, 2019], but this will not improve the confidentiality of communication with patients, who, of course, cannot be part of the telematics infrastructure. Therefore, it remains the job of the psychotherapist to ensure secure communication.

While there are more and more important developments in Internet-supported therapy that can use specially protected communication platforms, there is still a considerable way to go before everyday forms of communication can also be used in conventional psychotherapy [Creaner, 2015]; therapists should be warned against hasty recommendations for use, particularly in therapy with adolescents [see Borg-Laufs, 2015]. Certainly, compliance with data protection regulations also requires a reasonable amount of effort when communicating with digital media; however, relying blindly on the popular communication services would be negligent.
Acknowledgment

The project received financial support from the state of Baden-Württemberg, digilog@bw (MWK, 2019–2023). We are grateful to Dipl.-Ing. Otto Martin (University of Mannheim) and Theresa Kruß, Ass. Jur. (LPK Baden-Württemberg), for important information. We thank Prof. Dr. Thomas Fetter (University of Mannheim) for his comments on the text.

Disclosure Statement

The authors have no conflicts of interest. They do not intend to promote individual products or services.

References

Google LLC. Datenschutzerklärung. 2018.
Litman-Navarro K. We read 150 privacy policies. They were an incomprehensible disaster. The New York Times. 2019 June 12.


