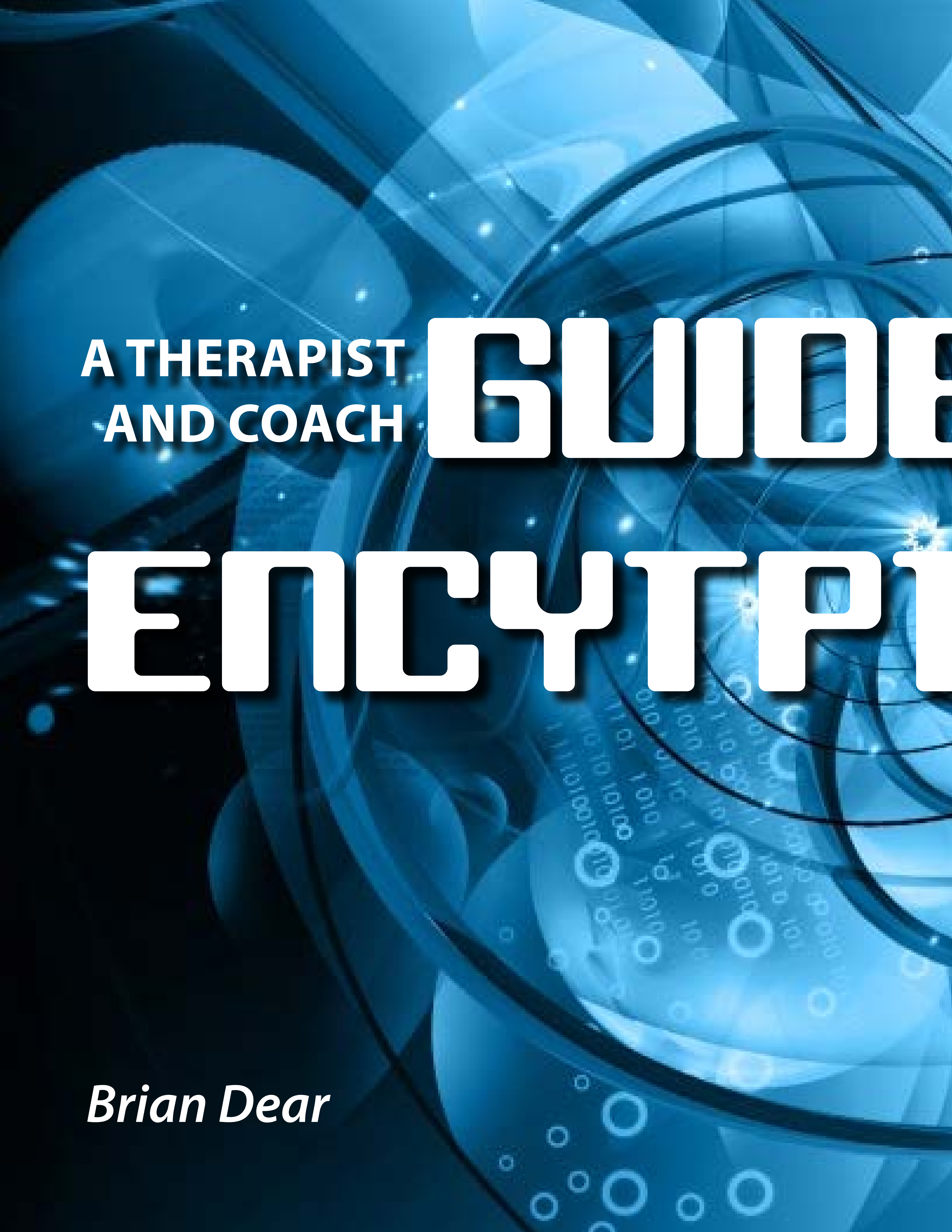

A THERAPIST AND COACH GUIDE ENCYTP

Brian Dear

E TO
TION

TRUE OR FALSE

If you use an encrypted email service to send emails to clients, you are in compliance with HIPAA.

□ True ☑ False

Skype is a HIPAA compliant video therapy solution because it uses encryption.

□ True ☑ False

Confused?

You aren't alone! Encryption, digital privacy and HIPAA are minefields. However, rather than pulling the plug on the wonderful tools that empower you to deliver better care to your clients, understanding the basic concepts behind encryption and digital privacy will give you the confidence to fully leverage technology to supercharge your productivity as well as improve the client experience. This guide is not meant to be legal advice; if you are uncertain about the laws in your jurisdiction, consult an attorney.

The exponential rise in digital communications and the seemingly endless digital tools for therapists and coaches brings both amazing opportunities to enhance client care but also serious consequences if misused. The digitally enabled therapy practice is the future. There's no escaping it; clients expect to interact with your business the same way they expect to be able to order books from Amazon. Land-line phones are disappearing. Phone calls are often viewed, especially by Millennials and the younger Generation X crowd, as intrusive annoyances. Mailing a check is as anachronistic as a house call. Telemedicine has gone mainstream with huge investments from Silicon Valley, insurers as well as governments. Welcome to the future.

There are two extremes of opinion regarding the digitally enabled therapy practice. There are the Luddites, the ones who still use paper schedules, telephone calls and don't even have an email address, web profile or other digital presence. Then, there are the early adopters. These are the therapists and coaches who were pioneering Second Life therapy, using video, as well as other tools like cloud-based practice management software. These will be the ones embracing virtual reality therapy. These techno-practitioners agree that the digital tools are worth the apparent risk because the benefit to the client outweighs downsides. The anti-tech constituency views the issue from either a position of fear, ignorance or tradition. Regardless of where you fall within the spectrum, the digital landscape for medical and behavioral health can be overwhelming.

Dispelling the Myths

"If I use an encrypted email service or if I have a Business Associates Agreement with my email provider, I'm HIPAA compliant."

This is the prevailing wisdom among many practitioners, however it's just not true. The problem isn't your end of the transaction, it's the clients side of things. To understand this, it's important to understand how encryption and email services work.

A Gentle Introduction to Encryption

Encryption is nothing more than converting a message into a secret code. Decryption is the opposite. Some of you might remember secret encoder rings in cereal boxes that let little kids code and decode messages. With digital information such as a computer file or email, encryption works the same way as those encoder rings. The bytes that make up the message are scrambled into a pattern that can later be unscrambled if you have the key.

Think of a needle. When you place it on your desk, it's easy to find. Anyone can walk over and view your needle. It's insecure. Now, place that needle carefully in a haystack, but create a precise diagram depicting exactly where it's located. Your needle is now "encrypted" and the map is the key. Without the map, that needle is lost forever.

If you keep the map locked in a desk drawer and the key to that drawer was sitting next to your keyboard, it would be very easy to simply open the lock, steal the map and find your needle. The weak link in this situation is the key to the desk lock, otherwise known as a password. The strength of the encryption (the massive size of the haystack,) isn't the problem, but the weakness in the password. Now imagine if you used the same key for all of your important hiding places!

Let's extend our needle in a haystack example to the situation where you need to transmit that needle, in this case an email to someone else. When you send the encrypted message, the entire haystack is sent to your recipient. However, what about the map? Without the encryption key, the recipient can't read your message. However, you can't send your map — then anyone could open your message. So what do you do? Using a system call Public Key Encryption, it's possible to send the message without revealing the "map."

Public Key Encryption

If Sandra wants to send an encrypted message to Dwight, Dwight provides Sandra something called a public key. This is digital file that describes how to encrypt something. It tells Sandra how to encrypt the message. This public key has a corresponding private key. Only Dwight has the private key. So Sandra can encrypt the message, but only Dwight can decrypt the message. The limitation to this approach is that it requires the participation of both people. Sandra would need to know Dwight's public key. Dwight would have to have a public key in the first place!

Encrypted email solutions solve this problem by handling this automatically — however, it only works if both people use the same service. It would be impractical to require all of your clients to use your particular email provider. So what you have is a situation where your "encrypted" email isn't actually encrypted at all. The storage of it might be encrypted, but once you've sent it — it's out there in the open. If it were encrypted, your client couldn't read it!

It Gets Worse...

If you're using an encrypted email service and you send a message to a client who uses the free version of Gmail (which is the vast majority,) then when that message arrives on Google's servers, it's scanned and harvested in order to provide contextual and target advertisements — not just within the Gmail application, but among the entire Google ad network! If you sent a client an email reminding them to take their lamotrigine or sent them an email mentioning hospitalization options, then suddenly as they're surfing the web, targeted advertising appears relating to hospitals, depression, bipolar disorder and treatment facilities. Imagine if their spouse or friends used their computer… This all happens regardless of how "secure" your particular email account happens to be. Imagine if you were counseling the client about a sexually transmitted disease or some other potentially sensitive issue.

Some types of Gmail accounts, specifically Google Apps for Business do not use this email scanning system. However, unless the client is the administrator of that business, their emails might be subject to monitoring by their employer.

What Can You Do?

While communicating with clients by email shouldn't be eliminated, there are ways you can ensure your obligations both ethically and under HIPAA.

If a client emails you, they are the furnisher of the health information. You aren't held responsible for what they send you until you receive it. If you are using a free Gmail account, it's strongly encouraged that you not use it for client communications, ever. If you are using Google Apps for Business, they do offer a BAA, however, that only extends to the storage of your email on

BUSINESS ASSOCIATES AGREEMENT

A **Business Associates Agreement** is simply a document provided by a technology provider that guarantees their compliance with HIPAA and other related laws. This document essentially states that they represent that they comply with the relevant laws. By having this document, you are not responsible if their system has a failure that violates the law. However, you are not protected if your misuse of the system resulted in a privacy violation. For example, if you shared your password — you'd still be on the hook for a health privacy law violation since it was your negligence that resulted in the data being improperly exposed.

their servers. There are several great providers of encrypted email providers, use one, but remember that only the email stored within your account is covered, not what you send to clients.

Email is an important tool for therapists and coaches, however don't be seduced into a false sense of security simply because your provider claims encryption. For email encryption to work, both parties of a message must use it. However, encrypted email services are valuable because you always want to ensure your messages are encrypted when in your possession (i.e. on your email provider's servers.) Be cautious of what you email to clients and never include their original message when you reply to their email since once you send the message, you are now the provider of the information. When they send the message, they are the provider.

What About Video Therapy?

Video therapy is one of the most important technological innovations in therapy. The benefits are well researched and documented, however the privacy and security implications are muddled.

Video therapy is generally very secure. Nearly all platforms use encrypted connections and the video stream itself is encrypted during transmission across the internet. However, there are still some significant concerns, not with the video itself, but with the platform itself.

Skype is Not HIPAA Compliant

Skype has been a therapist and coach favorite for several years. Cheap, nearly ubiquitous and generally reliable. However, Skype is not HIPAA compliant. The first indicator is that Microsoft (the owner of Skype) does not include Skype within its BAA. Since there is no way to obtain a Microsoft BAA for Skype, it is not compliant. Microsoft is effectively saying that they will not guarantee Skype's compliant with the security practices and data encryption requirements of HIPAA. If they won't guarantee it, then any therapist or coach using it would be willfully violating the law.

Another problem with Skype is that, despite claimed encryption, chat transcripts

WHAT IS HIPAA?

The **Health Insurance Portability and Accountability Act of 1996** is an American law that protects health insurance coverage for workers who change jobs as well as dictates administration standards for health care administration. Title II of the law concerns the Privacy Rule which is the section of the law that regulated the use and disclosure of Protected Health Information. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is a companion law that was passed in 2009. The HITECH app expands on the privacy protections of the HIPAA privacy rule. It sets requirements for notifications in the event of a data breach among other significant privacy protections. It also includes expanded provisions for Electronic Health Records implementation and meaningful use.

Secure Therapy.
Simple.

iCouch is an amazing HIPAA compliant therapy platform. With a set of simple and powerful tools, iCouch makes running your online and in person therapy practice easy.

iCouch

Video sessions
Manage clients and documents
Accept credit cards and Bitcoin
Encrypted, secure client inquires
SMS and email appointment reminders
In person and online appointment scheduling

Special offer for TILT readers!

$20 per month

icouch.me/tilt

Your therapy. Your couch. Since 2010

are stored on Skype servers. By looking at your own Skype conversations, you can see months of chat history — all stored on a platform that isn't HIPAA compliant. There are records of who you talked to and for how long — all egregious violations of patient privacy since that information isn't guaranteed secure, nor do you have a BAA protecting you from legal exposure in the event of a Skype data breach.

However, the good news is that there are a variety of HIPAA compliant video therapy platforms available that will sign a BAA. The best ones require no downloads and can work with a wide range of connection speeds. Do your homework when choosing a platform. The most important thing is that your provider be willing to provide a BAA and the platform be easy to use to ensure the widest accessibility for your clients.

Looking Forward

The digitally connected therapy practice is a reality that is improving client outcomes, improving your business and making quality treatment more accessible. However, with great power comes great responsibility. Be aware of the limitations of your tools. If you're interested in formal training on digital therapy, as recommended by most professional organizations, the Online Therapy Institute offers this through their various courses designed to suit you.

About the Author

Brian Dear is a software engineer and the cofounder and CEO of iCouch, Inc., a digital platform for therapists. He has been involved with the digital therapy community for the past 5 years creating iCouch.me with his therapist wife and cofounder Jessica Dear.