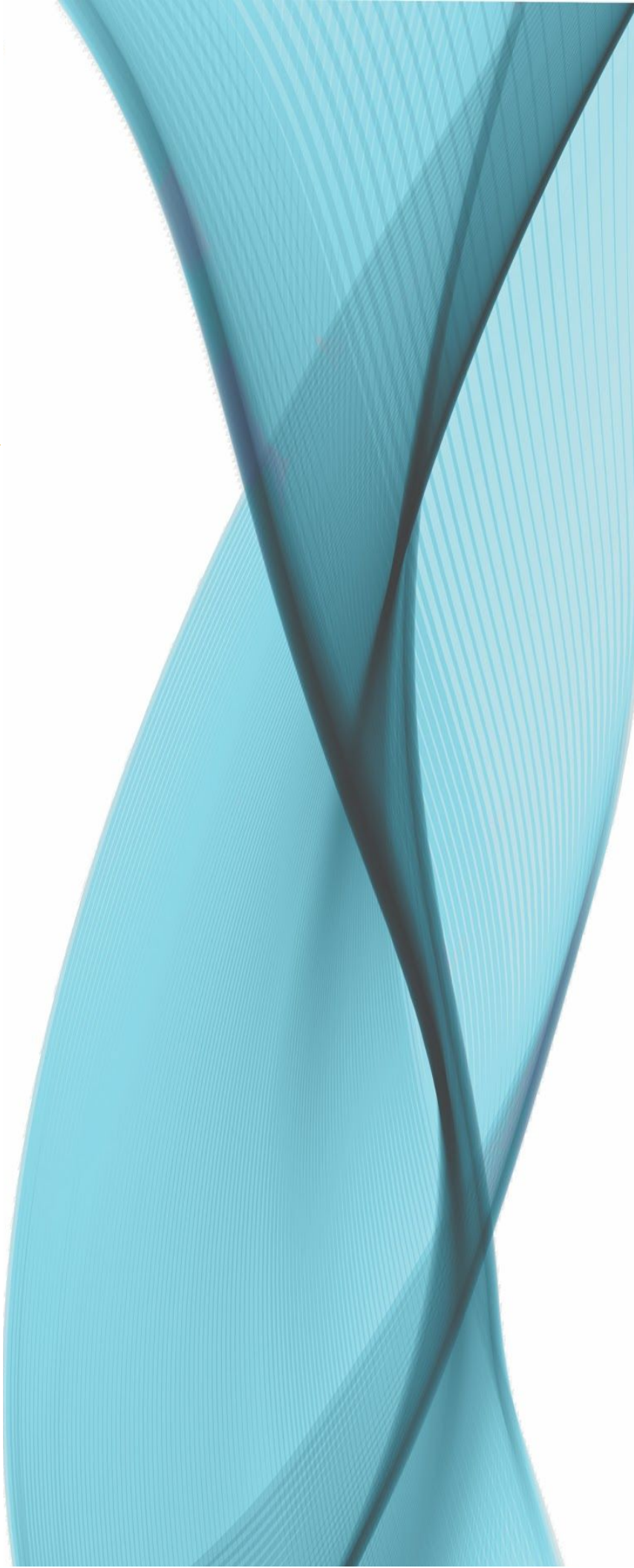
TELEBEHAVIORAL HEALTH™
INSTITUTE
21st Century Behavioral Health Strategies

EMAIL AND PRIVACY
HIPAA-COMPLIANCE CHECKLIST



Email and Privacy
HIPAA-Compliance Checklist

TELEBEHAVIORAL HEALTH
INSTITUTE

TBHI Checklist

Telebehavioral Health Institute www.telehealth.org

Email Privacy (HIPAA) Compliance Checklist

- ❏ As a healthcare practitioner or entity, obtain written consent from all patients before communicating with them via email or any other technology. This article that explains how and why.

- ❏ Include an automatic email signature statement to remind clients/patients that email is not secure. That same message can remind them to delete email not meant for them. See these samples of templates to consider when creating your email practice signature statement.

- ❏ Assure that the connection between all computers, smart devices and the email server are encrypted. To achieve this goal, conduct a regular *Risk Assessment* of all your devices to make sure they are in compliance with security standards. Use the US Government tool described here. The Security Risk Assessment tool is the result of a collaborative effort by the HHS Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR). The application, available for downloading at Health IT also produces a report that can be provided to auditors.

- ❏ Refrain from transmitting diagnoses and sensitive personal health information (PHI) via email or text messaging. When engaged in telehealth of any type, communicate diagnoses and other PHI via telephone or surface mail.

- ❏ To increase email privacy and security when transmitting sensitive medical information, consider email programs that literally offer email security. (Such systems can log in and out of separate software, which interrupts the normal flow of email exchange.) For examples of email programs, look at the "Resources" tab at the Telebehavioral Health Institute (TBHI) website. Other programs build the security features into the software, negating the need to log in and out of separate software to check patient email. See Google, Gmail for Work, or Office 365 from Microsoft for programs that do so. Some practice management and videoconferencing platforms build email functions into the interface, so that all exchanges with the client or patient are conveniently found in one place.

- ❏ Always use an email service that provides a HIPAA Business Associate Agreement (BAA). See this TBHI blog post for details of the Business Associate Agreement and how Google has handled it. Many other companies offering BAAs also exist. If in doubt, write to your vendor to inquire.

- ❏ Create unique email passwords and store them in a password manager, such as these:
  - ❏ Keepass
  - ❏ Dashlane
  - ❏ LastPass

- ❏ Enable settings in all email software to block emails that may have viruses.

- ❏ Without exception, use two-factor authentication for email. Such authentication prevents hackers from accessing your email. Such a feature is available at no cost in programs such as Gmail for Work.

- ❏ Have a written privacy and security policy. Document that all staff members have received and understand it.

- ❏ Organize a formal training session for staff to know what is allowed to be sent via email and SMS. Document time and location of training for such HIPAA compliance policies. For example, among other topics, train your staff about phishing with online training sites such as these:
  - ❏ Quiz for whether or not you can spot a phishing scam
  - ❏ OpenDNS Phishing Quiz
  - ❏ McAfee Phishing Quiz

- ❏ Always update software to the newest version. HIPAA violations have occurred and led to much negative publicity and fines when outdated software has been used in healthcare settings and hackers have accessed PHI.

Email Privacy and Security Checklist Disclaimer and Caution

The above checklist is used at TBHI for consulting clients and professional training to improve security and compliance with HIPAA and other state or provincial privacy laws. It is not legal advice, nor is it meant to represent all actions required by healthcare practitioners for compliance. Recommendations above are intended for informational purposes only, and are not meant to replace a legal opinion or review from a qualified privacy and/or security expert. Despite implementing all the above recommendations, you may suffer a security breach or violation of a privacy law.

By using this checklist, you agree that neither the Telebehavioral Health Institute, nor any of its directors, officers, shareholders, agents, servants, employees, including their heirs, successors, and assigns are to accept any liability for or will be liable for:

1. Any lack of compliance with the HIPAA Security Rule, the HIPAA Privacy Rule, HITECH, PCI, any state laws which may be applicable to Client, or any other federal or state legal authority
2. Any legal action against the user (you)
3. Any disclosures of sensitive data, or similar breaches of security, privacy, and confidentiality, or
4. Any legal liability or responsibility of any kind for any actions or omissions arising from the voluntary use of any third-party vendor products or services recommended in this checklist or related resources.

In summary: Ignorance is no defense in the face of the law. Data protection and legal compliance are 100% your responsibility. TBHI strongly advises you to hire a local telehealth attorney in your state or providence for a thorough document and telehealth process review. If you cannot afford such a service privately, TBHI encourages you to approach your state or national association and ask them to hire an attorney for this purpose on behalf of their entire membership. You may be delighted to learn that some of the more progressive professional associations already have undertaken such efforts, and make the documents and services available at an affordable rate. Take advantage of these resources, and share them with your colleagues at TBHI through our community HUB.