

# Translational Issues in Psychological Science

## **Data Security in the Digital Age: A Consolidated Guide for Psychologists to Understand Health Insurance Portability and Accountability Act-Compliant Telehealth**

Jonathan G. Perle, William S. Frye, and Tyler McCoy

Online First Publication, June 27, 2024. <https://dx.doi.org/10.1037/tps0000403>

### CITATION

Perle, J. G., Frye, W. S., & McCoy, T. (2024). Data security in the digital age: A consolidated guide for psychologists to understand Health Insurance Portability and Accountability Act-compliant telehealth.. *Translational Issues in Psychological Science*. Advance online publication. <https://dx.doi.org/10.1037/tps0000403>

# Data Security in the Digital Age: A Consolidated Guide for Psychologists to Understand Health Insurance Portability and Accountability Act-Compliant Telehealth

Jonathan G. Perle<sup>1</sup>, William S. Frye<sup>2</sup>, and Tyler McCoy<sup>2</sup>

<sup>1</sup> Rockefeller Neuroscience Institute, West Virginia University School of Medicine

<sup>2</sup> Institute for Brain Protection Sciences, Johns Hopkins All Children's Hospital, St. Petersburg, Florida, United States


Despite the exponential increase in psychologists' use of telehealth, literature has highlighted variable degrees of preparation to guide their digital practices. Due to the many unique aspects of the use of technology in clinical care, a lack of evidence-informed knowledge can negatively influence psychologists and their organizations, as well as affect patient outcomes. One of the more unique considerations of telehealth use is the data security of electronic protected health information. To ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA), as well as updates presented through the Health Information Technology for Economic and Clinical Health (HITECH) Act, psychologists must be aware of specific methods to ensure data security in order to foster an ethical and legal practice, as well as mitigate issues. Due to the complex nature of data security, combined with limited graduate training or continuing education materials to guide psychologists in the use of telehealth, guides are needed to clarify recommendations for graduate-level trainees first becoming literate with telehealth, as well as for licensed psychologists, whether early career or seasoned. To address this gap, the current discussion provides a consolidated, psychologist-focused guide for data security recommendations that align with HIPAA and HITECH in efforts to support ethical and legal telehealth practices. Summarized topics include network controls, continuous data protection programs, data backup and recovery, passwords, encryption, business associate agreements, technological administrators, and data breach reporting methods.

## *What is the significance of this article for the general public?*

Ethical and legal practice of telehealth involves ensuring data security of protected health information stored or transferred. This consolidated summary details specific evidence-informed strategies psychologists should employ to foster adherence to Health Insurance Portability and Accountability Act (HIPAA), thus optimizing telehealth services and security for their practice. Considerations for a HIPAA-compliant practice include network controls, continuous data protection programs, data backup and recovery, passwords, encryption, business associate agreements, technological administrators, and data breach reporting plans.

**Keywords:** telehealth, data security, Health Insurance Portability and Accountability Act, psychology, digital

Jacklynn Fitzgerald served as action editor.

Jonathan G. Perle  <https://orcid.org/0000-0003-4118-4021>

Jonathan G. Perle served as lead for conceptualization, investigation, methodology, writing—original draft, and writing—review and editing. William S. Frye and Tyler McCoy

contributed equally to writing—original draft and writing—review and editing.

Correspondence concerning this article should be addressed to Jonathan G. Perle, Rockefeller Neuroscience Institute, West Virginia University School of Medicine, 930 Chestnut Ridge Road, Morgantown, WV 26505, United States. Email: [jonathan.perle@hsc.wvu.edu](mailto:jonathan.perle@hsc.wvu.edu)

Telehealth, or the integration of synchronous (i.e., live) and asynchronous (i.e., nonlive) telecommunication technologies (e.g., videoconferencing, telephone, email, texting, and messaging programs) with healthcare services, has dramatically changed the psychological healthcare landscape. While once restricted to a surrounding geographical area, telehealth has allowed psychologists to digitally extend their service offerings to reach a broader audience in need of mental healthcare. For example, within the United States, one in five, or 57.8 million adults experienced a mental illness within 2021 alone (National Alliance on Mental Illness, 2023). Telehealth allows for patients to receive the needed general or specialized mental healthcare while overcoming common barriers to in-person services, such as transportation difficulties, disability-related challenges, child-care considerations, and time-related issues (Lipschitz et al., 2023). Although the use of telehealth among medical specialties has fluctuated following the end of COVID-19 stay-at-home orders (e.g., Zocdoc, 2021), overall mental health-related telehealth service utilization post-COVID-19 has remained persistent and elevated when compared to pre-COVID-19 (Cantor et al., 2023). Further, a large number of surveyed psychologists have suggested intention of continuing to offer telehealth services in some capacity into the future (e.g., Lipschitz et al., 2023; Perle, 2022), with researchers citing the persisting popularity of the modalities (Mishkind et al., 2021).

Despite telehealth holding many unique benefits above traditional in-person methods, it also creates new challenges for psychologists. Among possible considerations, data security has repeatedly been identified as one of the more unique telehealth-related concerns faced by practitioners (Pierce et al., 2020, 2021). Transmitted data could be intercepted or sent to the wrong person, while stored data could be hacked or subject to malware (e.g., virus). The security of data can be considered both an ethical and legal requirement when a psychologist considers their applicable ethical guidelines and licensure standards. As an example, the American Psychological Association's (APA) Ethical Code (2017) highlights the importance of security of any private information collected, recorded, stored, or transferred.

While the mandate for data security is clear, literature has repeatedly highlighted the variable preparation among psychologists for the use of

telehealth in clinical practice (Baier & Danzo, 2021; Glueckauf et al., 2018; Perle, 2022; Sammons et al., 2020). Unfortunately, a lack of data security management strategies can lead to complications for psychologists, their organizations, and the patients. As an ethical and legal practice of telehealth requires a psychologist to adhere to state and country-wide data security requirements to meet the standards of their practicing jurisdictions, the question arises as to what these specific requirements are and how one can adhere. As no consolidated and universally accepted document of telehealth standards is recognized, the current discussion is meant to supply psychologists practicing within the United States with a readily understandable detailing of data security requirements for the use of telehealth (Table 1). Of particular note, this discussion is meant as a summary and not suggested as all-encompassing or legal advice. As a result, psychologists are suggested to seek additional guidance, as indicated, to ensure the most up-to-date materials and standards.

### U.S. Data Security Recommendations

The United States adheres to the Health Insurance Portability and Accountability Act (HIPAA). HIPAA focuses on the protection of "protected health information" (PHI), which includes, but is not necessarily limited to a patient's: (a) name, (b) location (e.g., address or equivalent geocodes), (c) birth date, (d) medical dates (e.g., admission, care, discharge, and death), (e) phone numbers, (f) fax numbers, (g) email address, (h) medical record numbers, (i) social security numbers, (j) healthcare plan numbers, (k) account numbers, (l) vehicle identification numbers and license plate numbers, (m) internet protocol (IP) address numbers, (n) web universal resource locators, (o) biometric identifiers (e.g., fingerprint, voice print, and eye print), (p) photographs or videos, and/or (q) uniquely identifying codes or characteristics (Office for Civil Rights [OCR], 2017, 2022). Originally published in 1996, HIPAA was updated in 2009 following the Health Information Technology for Economic and Clinical Health (HITECH) Act (OCR, 2017). The updated HIPAA involves four primary guiding rules: privacy rule, security rule, enforcement rule, and breach notification rule. Most relevant to data security is the security rule. This rule suggests physical, administrative,

**Table 1***Summary of HIPAA-Aligned Recommendations for Telehealth Practice<sup>a</sup>*

Factor	Brief description	Example
Network control	<ul style="list-style-type: none"> <li>Psychologist's employing of personal and network firewall systems to monitor incoming and outgoing network traffic to determine whether to allow or block specific traffic based upon a set of security rules.</li> </ul>	<ul style="list-style-type: none"> <li>Dr. Markman installed a cybersecurity firewall to his office network and devices used for telehealth services, which helped restrict unauthorized access to applications and systems on his devices and network.</li> </ul>
Malware software and continuous data protection	<ul style="list-style-type: none"> <li>Automated risk detection, prevention, and removal software to protect against malware that can include viruses and Ransomware.</li> </ul>	<ul style="list-style-type: none"> <li>Dr. Wade installed anti-malware software to all his devices to automatically protect against viruses and Ransomware, and automatically clean any files that the system believes may have malware.</li> </ul>
Data backup and recovery	<ul style="list-style-type: none"> <li>Creating data backups and replications of all important data (e.g., patient records, billing) as a recovery method in case of compromised, damaged, incorrectly edited, or deleted information.</li> </ul>	<ul style="list-style-type: none"> <li>A few months ago, Dr. Lou's office and computers were damaged as a result of a hurricane. However, Dr. Lou routinely backs-up her operating systems to a HIPAA-compliant off-site backup server. Thus, she continued to have access to patient records and billing files, which limited disruption to patient care.</li> </ul>
Passwords	<ul style="list-style-type: none"> <li>Authenticators known only to the psychologist and designated individuals to restrict access to programs and networks to only those allowed.</li> </ul>	<ul style="list-style-type: none"> <li>Dr. Young creates unique, strong passwords for all of his online programs and accounts. To keep track of the numerous passwords that vary by program, Dr. Young utilizes a password locker so he only has to remember one specific password to gain access to all his other passwords. Additionally, Dr. Young set up multifactor authentication for logging-in to the electronic medical record, which requires him to verify through an authentication app on his phone that he is the one entering his password to gain access to the electronic medical record program (i.e., once the password is put in, the app sends a message to Dr. Young's phone to indicate "I approve this login").</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>Using software that makes PHI unintelligible to others without a decryption key to ensure that it is not accessed and understood by non-designated individuals.</li> </ul>	<ul style="list-style-type: none"> <li>When choosing a telehealth platform, Dr. Hernandez found a telehealth platform that listed on their website that the platform offered 256-bit endpoint encryption to ensure that any information that may be intercepted is not decipherable by non-designated individuals.</li> </ul>
BAA	<ul style="list-style-type: none"> <li>A contract between the psychologist (or their organization) and a third-party company that has access to PHI from the psychologist (or their organization), and is acting on behalf of the psychologist. The BAA helps ensure that the third party is enacting proper HIPAA standards for data security.</li> </ul>	<ul style="list-style-type: none"> <li>Dr. Long uses a third party to send billing invoices to patients seen by telehealth. Dr. Long establishes a BAA with the third-party billing provider describing how PHI can be used, that the third party adheres to HIPAA, the liabilities of Dr. Long and the billing provider, and the steps to be taken in the event of a breach in PHI.</li> </ul>
Administrators	<ul style="list-style-type: none"> <li>Assigning administrators as security administrator, storage administrator, and security auditor. The security administrator establishes and manages accounts related to the telehealth service and PHI, as well as creating permissions for access,</li> </ul>	<ul style="list-style-type: none"> <li>The IT department was assigned to serve as the security administrator for the urban hospital where Dr. Thompson works. This department oversees data security and access auditing of the systems.</li> </ul>

*(table continues)*

**Table 1** (*continued*)

Factor	Brief description	Example
Reporting a breach	<p>policies for data security, and setting access controls, The storage administrator monitors and oversees the storage systems and ensures access to only those designated. The security auditor reviews security features and issues, verifies security protocols, and inspects audit logs to ensure that information is only accessed by designated individuals.</p> <ul style="list-style-type: none"> <li>• Complying with U.S. HHS guidelines for reporting breaches of more than, or less than, 500 individuals.</li> </ul>	<ul style="list-style-type: none"> <li>• Dr. Chin is the owner of a large psychology practice servicing more than 500 patients. Dr. Chin learned that electronic patient records were breached by internet hackers. Following HHS guidelines for notifying patients of a breach of more than 500 individuals, Dr. Chin provided written notice to all of his patients at their preferred method of contact within 60 days to provide a brief description of the breach, dates of the breach, description of PHI involved, steps the patients should take to protect against potential harm, the steps taken to investigate the breach incident and protect against further breaches, and his contact information. Additionally, Dr. Chin provided immediate notice to HHS of the breach, as well as provided notice to major media outlets in the geographical area. Dr. Chin also contacted APA's Office of Legal and Regulatory Affairs for assistance.</li> </ul>
Avoiding public networks	<ul style="list-style-type: none"> <li>• Avoiding the use of nonsecure public networks for internet when accessing PHI or conducting other business-related activities.</li> </ul>	<ul style="list-style-type: none"> <li>• Dr. Kim has several-therapy session notes she needs to write from sessions earlier in the day. She wanted to write her notes while enjoying coffee at a local coffee shop. However, Dr. Kim remembered that coffee shop public networks are not secure. Thus, Dr. Kim decided to order coffee to-go and completed her session notes at her office using the secure internet network.</li> </ul>
Use of a VPN	<ul style="list-style-type: none"> <li>• If public networks must be utilized, VPNs can help (although not completely) mitigate issues by enabling two or more parties to communicate securely across a public network by creating a private connection between endpoints.</li> </ul>	<ul style="list-style-type: none"> <li>• Dr. Lane frequently travels and she wants to be able to respond to patient emails while out of the office. Dr. Lane subscribed to a VPN service so she can more securely email while connected to her hotel Wi-Fi network.</li> </ul>
Monitor environment	<ul style="list-style-type: none"> <li>• Taking care to ensure that confidential information is not readily available on telehealth meetings (e.g., reflections of patient records from mirrors or glasses).</li> </ul>	<ul style="list-style-type: none"> <li>• Prior to starting a telehealth session with a client, Dr. Smith checks the camera view to ensure that no confidential information is visible on screen or reflected through his eyeglasses. Additionally, Dr. Smith uses the telehealth platform background filter to further limit visibility of his work environment.</li> </ul>
Cybersecurity insurance	<ul style="list-style-type: none"> <li>• Consideration of purchasing separate cybersecurity insurance to cover cyber-related issues, over-and-beyond general malpractice insurance.</li> </ul>	<ul style="list-style-type: none"> <li>• Dr. Rodriguez purchased cybersecurity coverage through a major vender prior to beginning telehealth services in her private practice to cover damages caused by such issues as hacking, and physical damage to computer hardware should an unexpected event occur (e.g., natural disaster).</li> </ul>

(*table continues*)

**Table 1** (*continued*)

Factor	Brief description	Example
Cross-country work	<ul style="list-style-type: none"> <li>Considering differences from HIPAA in terms of data security when practicing across country-based jurisdictions.</li> </ul>	<ul style="list-style-type: none"> <li>From his practice in the United States, Dr. Brown volunteers to provide psychotherapy services via telehealth to international refugees in Canada. Prior to providing psychotherapy services, Dr. Brown reviews the PIPEDA and the telehealth regulations for the specific province in Canada in which Dr. Brown will be providing telehealth services. Dr. Brown also clarifies with patients his obligations for data security and confidentiality for practice within both Canada and the United States.</li> </ul>

*Note.* HIPAA = Health Insurance Portability and Accountability Act; PHI = protected health information; BAA = business associate agreement; IT = information technology; HHS = Health and Human Services; APA = American Psychological Association; VPN = virtual private network; Wi-Fi = wireless fidelity; PIPEDA = Personal Information Protection and Electronic Documents Act.

<sup>a</sup> Psychologists are suggested to seek additional guidance, as indicated, to ensure the most up-to-date materials and standards.

and technical safeguard standards, which are directly applicable to a psychologist's telehealth work (Chandramouli & Pinhas, 2020; Perle, 2021). Physical safeguards involve psychologists ensuring the security of any physical components. More specifically, it suggests restricted access to not just the location in which the technology is stored for telehealth encounters and associated documentation, but limited physical access to the technology itself through locked doors and cabinets, key-card entries, and/or biometric devices (e.g., fingerprint scanner). Administrative safeguards focus on ensuring the competence of any psychologist or associated staff member who has access to the electronic PHI (ePHI). Such competence includes the use of, storage of, and legal reasons to disclose any of the PHI, with such competence developed through formal trainings, ongoing monitoring, and data audits. As part of this, organizations should appoint a data security officer to oversee these activities. Finally, technical safeguards include the cybersecurity measures applied to the ePHI by psychologist and/or the overarching organization of practice. While there are no universal guidelines for cybersecurity measures, the National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE) created U.S. government-approved stance papers on privacy and security risks applicable to telehealth practices (e.g., Chandramouli & Pinhas, 2020; Grassi et al., 2020; NIST, 2023). Adherence to these guidelines set by NSIT and NCCoE suggests several

specific security procedures. For more detailed information about any of the following recommendations, psychologists are encouraged to review: NIST Special Publication 800-209: Security Guidelines for Storage Infrastructure (Chandramouli & Pinhas, 2020), NIST Special Publication 800-63B Digital Identity Guidelines (Grassi et al., 2020), FIPS 197: Advanced Encryption Standard (AES; NIST, 2023), Protecting Data From Ransomware and Other Data Loss Events: A Guide for Managed Service Providers to Conduct, Maintain and Test Backup Files (National Institute of Standards and Technology and National Cybersecurity Center of Excellence [NIST and NCCoE], 2020), NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery (Bartock et al., 2016), and NIST Small Business Information Security: The Fundamentals (Paulsen & Toth, 2016).

### Network Control

It is suggested that psychologists employ a personal and network firewall for all systems. Firewalls are a form of network control that monitors incoming and outgoing network traffic to determine whether to allow or block specific traffic based upon set security rules (Cisco, n.d.). As such, firewalls limit who can access secure databases/networks, as well as what types of information they are allowed to view, modify, and save. Firewalls can be hardware, software, software-as-a-service, public cloud, or private cloud. Per Cisco (n.d.), firewalls have remained as a first-line

defense for network security for over 25 years. Many operating systems (e.g., Windows) provide built-in firewall capabilities; however, psychologists may also seek out additional business-focused firewall systems for their telehealth use. Similarly, psychologists should seek wireless access point (WAP) routers that give them or their organization full network control access (Chandramouli & Pinhas, 2020; Grassi et al., 2020). These routers provide wireless access to a wired network. Given that anyone could connect to these networks, psychologists can employ WAP routers with security features (also see Passwords and Encryption) to restrict access to only authorized individuals who should be on the network.

### Malware Software and Continuous Data Protection

To limit the potential for viruses, Ransomware, or other malware, psychologists should utilize automated risk detection and prevention software. Such programs should not only provide general ongoing monitoring for all data on the system/database, but also conduct scheduled scans of all the systems to ensure nothing has become compromised (Chandramouli & Pinhas, 2020; Grassi et al., 2020). As there is a multitude of free and paid malware software packages, psychologists are suggested to review each for specific features to meet their needs. More specifically, among other considerations, psychologists should strive for a program that offers ongoing updates to add new malware definitions to the database, has the ability to scan specific files or folders and full system, offers both file and network protection, uses the least amount of computer hardware (e.g., RAM) to reduce the potential for system lag, offers a built-in virtual private network (VPN, see Additional Data Security Considerations for Telehealth-Based Practice section), and is cost-effective for psychologists and their practices when considering the maximum number of systems the program is allowed to be installed on without additional charges.

### Data Backup and Recovery

Due to the possibility of data (e.g., ePHI) being compromised, damaged, incorrectly edited, or deleted, it is recommended that psychologists

and their organizations strive to have data backups and replications, as well as recovery strategies. As part of their data backup and recovery strategy, psychologists should have a plan or policy that is comprehensive and frequent enough to meet the needs of the organization and maintain the integrity of the data. More specifically, psychologists or their organizations should: (a) identify the files that require backing up (vs. a full database level copy), (b) determine the time required for a restoration/repair, (c) determine the relationships among systems to understand any dependencies required to repair or restore the files (e.g., one file is used by multiple programs), (d) determine what backup files need to be secured offline (e.g., encryption keys, passwords, digital certificates or other information needed to reestablish business operations quickly), (e) plan to save more than one backup file following the 3-2-1 rule (i.e., keep three copies of important files that includes one primary and two backups, keep the files on two different media types, and store one copy off-site/outside of the business facility), (f) develop response and recover procedures and determine the appropriate technical approach to generating backups (e.g., automatic vs. manual), and (g) test the plan (Bartock et al., 2016; NIST and NCCoE, 2020; Paulsen & Toth, 2016). Additionally, a full “point-in-time copy” (i.e., a copy of original data as it appeared at a point in time) of the entire database is recommended to occur on a set schedule (Chandramouli & Pinhas, 2020). Having such a system and plan can reduce disruptions to telehealth services that may arise from an impaired system/database.

### Passwords

To ensure that programs and networks are only accessed by designated individuals, passwords (also known as authenticators) must be employed. NIST guidelines by Grassi et al. (2020) recommend that the minimum password length should be based upon the threat model being addressed (i.e., more complex passwords as threats increase), but generally suggest that user-created passwords should be at least eight characters long, while autogenerated passwords should be at least six characters long (Grassi et al., 2020). Nevertheless, NIST guidelines by Chandramouli and Pinhas (2020) further indicate that a “good password” should be at least 15, but preferably 20, characters.



While historically, passwords have been recommended to include a mix of character types; such as at least one digit, uppercase letter, and symbol, analyses of breached databases have shown that such passwords are not as secure as originally thought (Grassi et al., 2020; Weir et al., 2010). Nevertheless, more complex passwords that psychologists will not forget should be used in favor of simpler or easily guessed passwords. For example, guidelines suggest that passwords should not be similar to usernames, include repeated or sequential characters (e.g., 1234), or utilize hints. Additionally, psychologists should set (or manually update) passwords based on an expiration timeframe that adheres to their practice and organizational requirements, while also avoiding the reuse of at least their previous four passwords. Further, psychologists should avoid merely adding an additional letter, exclamation point, or other single character after a previously used password. Finally, psychologists should avoid writing their password on a piece of paper, saving passwords for logins on their browser, and using default passwords that come with programs or computer systems. Due to psychologists likely having a large number of passwords across programs, password locker programs are encouraged. These programs allow an individual to have a singular password that unlocks the secure locker that contains a full listing of all of their passwords. As available, multifactor authentication (e.g., password followed by a text or email being sent to psychologists to verify that they are the ones attempting to access the system in question) is recommended (Chandramouli & Pinhas, 2020).

## Encryption

In efforts to protect digital data, including ePHI, psychologists are suggested to utilize telehealth programs offering at least 128-bit endpoint (i.e., on both ends of the technology) AES protocols (NIST, 2023). While 128-bit is recommended, 256-bit, sometimes referred to as military-grade, is better. Per NIST (2023), the AES algorithm is a symmetric block cipher that can encrypt (i.e., encipher) and decrypt (i.e., decipher) digital information. Related to telehealth, encryption makes PHI “unusable, unreadable, or indecipherable to unauthorized individuals” through “an algorithmic process to

transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (OCR, 2013a). In more simplified terms, the process of encryption takes information used or collected during telehealth encounters or documented postencounter (e.g., digital text, images, and video) and makes it unintelligible to those without the decryption key. As defined by the OCR (2013b), while the use of encryption is not specifically mandatory for the Security Rule if the regulation can be met without use of encryption, the use of AES is nonetheless highly recommended by both U.S. Department of Health and Human Services (U.S. HHS) and field experts to ensure that ePHI practices adhere to the Security Rule (NIST, 2023; Yellowlees et al., 2010). For those in doubt, software/product websites and manuals generally list the program’s level of encryption. If this information is not readily available, difficult to locate, or overly vague on what the encryption protocol is, psychologists would be wise to explore other options.

## Business Associate Agreement (BAA)

Psychologists and their organizations are encouraged to secure a signed/executed BAA when using any third-party programs for their telehealth services, including videoconferencing services, messaging programs, email clients, telephone services, call centers, electronic health records, billing services, and data sharing programs. A BAA is a contract between a covered entity (i.e., psychologists billing for clinical services and psychologists’ organizations) and the business associate (i.e., a person or organization other than a member of the covered entity who performs functions or activities on behalf of the covered entity and has access to the ePHI; OCR, 2013c). The BAA typically includes agreements describing how PHI can be used, the liabilities of each entity, and steps taken if there are breaches in PHI. In essence, the BAA provides psychologists a level of security and coverage should the third-party company have a breach of any PHI. While many telehealth companies have standard BAA contracts, a sample of a BAA can be found on the U.S. HHS website (OCR, 2013c). Psychologists are also suggested to consult legal counsel to ensure that the BAA fully covers their ePHI and liability.



## Administrators

To ensure comprehensive coverage of telehealth services, psychological organizations are suggested to assign administrators to cover three roles: security administrator, storage administrator, and security auditor. The security administrator holds the role of establishing and managing accounts related to the telehealth service and PHI (whether physical or digital related to the telehealth services), creating and associating roles and permission for all users and administrative operations related to the telehealth services and systems/databases, creating policies for passwords, managing certificate and data keys, managing encryption standards, managing auditing and logging of data and security, and setting access controls. The storage administrator monitors and oversees the storage system itself and ensures that no access is granted to security-related elements of data without their oversight. The security auditor allows for review of security features and issues, verifies security parameters and configurations, and inspects audit logs. Auditing ensures that nobody is granted access to the storage, configurations, or data without permission and oversight (Chandramouli & Pinhas, 2020).

## Reporting a Breach

Despite even the best preparation by psychologists, data breaches may occur. For such situations, the U.S. HHS provides guidance on steps a psychologist should take, varying by whether the breach affects more or less than 500 individuals (OCR, 2023). To further simplify, the American Psychological Association Practice Organization (2013) created a stepwise guide psychologists can follow. More specifically, this three-step plan suggests that psychologists first conduct a formal risk assessment if they discover or suspect a breach, even if the breached ePHI was secured through encryption or other cybersecurity measures. This evaluation considers: (a) the nature and extent of the PHI involved, (b) to whom the PHI may have been disclosed, (c) whether the PHI was actually acquired or viewed, and (d) the extent to which the risk to the PHI has been mitigated. Per the guide, should the risk assessment fail to clearly demonstrate that there is a low probability that the PHI has been compromised, a breach notification is required. If this occurs, the second step is for

psychologists and/or their organization to provide notice to the patient that is written in plain and understandable language and includes: (a) a brief description of the breach including dates; (b) a description of the types of unsecured PHI involved; (c) the steps that the patient should take to protect against any potential harm; (d) a brief description of steps that psychologists have taken to investigate the issue, mitigate any harm, and protect against further breaches; and (e) the psychologists' contact information should the patient need to contact their psychologist directly. If the five aforementioned points are unavailable, psychologists can provide a series of notices that fill in the information as it is learned. While first-class mail to the patient's last known address is suggested, email may be used if that was indicated as the patient's desired mode of contact. The notice should be provided to patients "without reasonable delay" and within 60 days after discovering the breach. Finally, in the third step, psychologists should make a formal report to the U.S. HHS. In addition to informing patients, for breaches of fewer than 500 patients, psychologists must keep a log of the breaches during the year and then provide notice to the U.S. HHS of all breaches during the calendar year, within 60 days after that year ends. Should the breach involve greater than 500 patients, psychologists should provide immediate notice to the U.S. HHS and send notifications to major media outlets of the state or jurisdiction in which the breach occurred for publication purposes. If psychologists are unsure of steps to take or the number of affected patients, additional instructions on how to provide notice can be found on the U.S. HHS website (OCR, 2023).

## Additional Data Security Considerations for Telehealth-Based Practice

In addition to the core recommendation to maintain data security in line with the HIPAA Security Rule, psychologists should also consider other technical, as well as less technical, considerations for data security of both physical and digital PHI related to their telehealth services. For example, psychologists are suggested to avoid using public networks (e.g., public Wi-Fi) when conducting telehealth services or accessing ePHI-hosting systems/databases, as public networks are generally unsecure with the potential for data transmission to be intercepted

or monitored by unauthorized parties, including for marketing purposes. Although public networks should likely be avoided when possible, if they are an only option (e.g., crisis events), psychologists are suggested to employ a VPN. VPN programs, of which there are numerous on the market, enable two or more parties to communicate securely across a public network by creating a private connection between endpoints. Although some have documented that VPNs are not without faults, and using a VPN over a public network does not necessarily preclude the possibility of data being intercepted by unauthorized individuals or companies, the use of VPN-related authentication and encryption has been suggested to significantly reduce the chances of such an occurrence (Dempsey et al., 2021). Additionally, psychologists should take care to monitor their own environment while conducting video-based telehealth services. For example, a psychologist leaving out confidential paperwork on a desk could be reflected by in-room mirrors, glass, or even their own glasses, thus making it visible to a patient seen via video (Simpson et al., 2016). Finally, given the potential for technological issues, psychologists can consider purchasing cybersecurity insurance over-and-above general malpractice insurance (HealthITSecurity, 2019). While varying by company and plan, this type of insurance will frequently provide coverage for data breaches, digital security issues, cybercrime, and hacking incidents through their coverage of damaged networks, software and hardware compromises, and legal fees associated with data breaches. While cybersecurity insurance does not preclude psychologists from ensuring their own data security, it may provide an additional level of protection for their practice should an issue occur (Leonard, 2016). Ultimately, psychologists are responsible for protecting patient PHI and taking the necessary safeguards to do so. Failure to protect PHI can result in civil monetary penalties (e.g., fines up to \$63,973 per violation) and criminal penalties (e.g., fines up to \$250,000 and 10 years imprisonment; OCR, 2022).

### Non-U.S. Countries

Although the current discussion is meant to focus on psychologists practicing within the United States, it is recognized that psychologists may also practice across province, territory, and country jurisdictions. While a full review of

such differences is outside of the scope of the current discussion, for psychologists wishing to practice across jurisdictional lines, they are encouraged to learn about each respective data security standards for both the location of the psychologist and their patient, as the two may differ.

For example, psychologists practicing within Canada must be aware of the Personal Information Protection and Electronic Documents Act (PIPEDA), which outlines Canada's data security regulations. Despite being a country-wide regulation, it should be noted that individual provinces and territories may have more specific adaptations of PIPEDA if deemed substantially similar by governmental bodies (Office of the Privacy Commissioner of Canada, 2018, 2020). As such, the psychologist must not only explore PIPEDA, but any additional specific regulations unique to the provinces or territories of practice. Related to data security, PIPEDA and HIPAA enforce similar physical, administrative, and technical safeguard standards, as both countries adhere to NIST recommendations (e.g., passwords, firewalls, network controls, at least 128-bit encryption). Finally, Canadian provinces and territories have specifics of how to report a data breach.

As another example, for those practicing within the European Union, General Data Protection Regulation (GDPR, 2016), should be explored. GDPR has been cited as the "strongest privacy and security law in the world" (Council of the European Union, 2022). Similar to PIPEDA, psychologists within the United States must explore specific regulations of where they are practicing, as not all countries in Europe adhere to GDPR. Rather, some countries (e.g., Switzerland) have similar, but more specific regulations (The Federal Authorities of the Swiss Confederation - Federal Data Protection and Information Commissioner, 2023). Related to data security, GDPR and HIPAA establish accountability for data security, regulate patient access, suggest implementation of safeguards, and have breach notification requirements. Differing from HIPAA, GDPR establishes the obligation of data controllers (i.e., those collecting, storing, and using personal data) to instill appropriate security measures that is regulated by the European Data Protection Board, an independent European body comprised of all participating independent supervisory authorities (Council of the European Union, 2022). Further differing

from HIPAA, GDPR suggests the application of encryption or pseudonymization (i.e., process of replacing personal data with artificial identifiers in the form of pseudonyms to conceal information), but does not provide universal guidance on the levels of security to implement, instead suggesting that the organization “should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risk and the nature of the personal data to be protected” (GDPR, 2016). To determine need, data controllers must carry out a data privacy impact assessment that allows them to clarify data security requirements. Finally, GDPR-following countries have specifics of how to report a data breach.

As PIPEDA, GDPR, and other country-specific regulations are broad yet nuanced, psychologists are recommended to review the province, territory, or country’s governmental websites, or their associated technology-focused organizations that govern technological use (e.g., Canadian Centre for Cyber Security). Further, psychologists can explore the APA’s Global Psychology Alliance, as well as the International Council of Psychologists, for contact information regarding international psychology boards and individuals.

### Barriers to Implementation

Despite considerable literature being available on general barriers to telehealth implementation, very limited empirical study has focused on barriers to implementation of data security as specifically related to telehealth for psychologists. Nevertheless, several barriers are believed to exist that can create challenges for implementation of outlined recommendations. These barriers can be categorized into two primary themes of (a) knowledge and (b) costs.

First a psychologist likely requires additional education related to telehealth and data security before they can properly employ the methods, or problem-solve arising challenges. This may also require education on different data security products to determine correct fit for one’s practice. As such, psychologists must make purposeful actions to not only educate themselves on current standards and products, but stay abreast of field changes through readings, listserv discussions, consultations, and trainings.

Supplementing education is the financial and time costs. It takes time to review current data

security practices and/or train others in how to effectively implement security protocols. It also takes time and resources to secure additional training and consultations. This can be important considerations for any psychologist, but becomes even more impactful if the psychologist is an independent practitioner and does not have a larger staff or significant extra revenue. To avoid becoming overwhelmed, the psychologist must not only determine current telehealth needs for their practice, but create ways to minimize disruptions to revenue and time that come from the continuing education and practice adaptation.

### Conclusion

To ensure an ethical and legal telehealth practice, psychologists must strive for data security of all PHI. The current discussion consolidated recommendations psychologists should aim for in order to maintain the integrity of telehealth-related data, mitigate possible issues, and address arising data breaches. These recommendations include utilizing firewall systems, automated risk detection and prevention software, data backup and recovery programs, complex passwords, data encryption, BAAs, and administrative roles to help safeguard patients’ PHI. Although this discussion is meant to help providers, each psychologist is suggested to conduct their own review of data security recommendations to ensure the highest level of understanding for their unique telehealth-based practice.

### References

- American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct (2002, amended effective June 1, 2010, and January 1, 2017)*. <https://www.apa.org/ethics/index.aspx>
- American Psychological Association Practice Organization. (2013). *The HIPAA final rule: What you need to know: Guidance and privacy notice updates for psychologists*. <https://www.apaservices.org/practice/update/2013/07-25/hipaa-final-rule.pdf>
- Baier, A. L., & Danzo, S. (2021). Moving toward a new era of telepsychology in university training clinics: Considerations and curricula recommendations. *Training and Education in Professional Psychology, 15*(4), 259–266. <https://doi.org/10.1037/tep0000359>
- Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *NIST Special*

- Publication 800-184: Guide for cybersecurity event recovery*. National Institute of Standards and Technology, U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>
- Cantor, J. H., McBain, R. K., Ho, P. C., Bravata, D. M., & Whaley, C. (2023). Telehealth and in-person mental health service utilization and spending, 2019 to 2022. *JAMA Health Forum*, 4(8), Article e232645. <https://doi.org/10.1001/jamahealthforum.2023.2645>
- Chandramouli, R. & Pinhas, D. (2020). *NIST Special Publication 800-209: Security guidelines for storage infrastructure*. National Institute of Standards and Technology, U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf>
- Cisco. (n.d.). *What is a firewall*. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- Council of the European Union. (2022, September 1). *The general data protection regulation*. <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/>
- Dempsey, K., Pillitteri, V., & Regenscheid, A. (2021). *NIST Special publication 800-47 Revision 1: Managing the security of information exchanges*. National Institute of Standards and Technology, U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-47r1.pdf>
- General Data Protection Regulation (GDPR), 2016/679. (2016, April 5). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Glueckauf, R. L., Maheu, M. M., Drude, K. P., Wells, B. A., Wang, Y., Gustafson, D. J., & Nelson, E. L. (2018). Survey of psychologists' telebehavioral health practices: Technology use, ethical issues, and training needs. *Professional Psychology: Research and Practice*, 49(3), 205–219. <https://doi.org/10.1037/pro0000188>
- Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2020). *NIST Special publication 800-63B: Digital identity guidelines*. National Institute of Standards and Technology, U.S. Department of Commerce. <https://pages.nist.gov/800-63-3/sp800-63b.html#policies>
- HealthITSecurity. (2019, February 5). *What is cyber insurance for healthcare organizations?* [https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations?eid=CXTEL000000439070&elqCampaignId=10874&utm\\_source=nl&utm\\_medium=email&utm\\_campaign=newsletter&elqTrackId=8a5fc9c33ec84bca962f8bba4fa87ef1&elq=27c63bceccff84063bf7bcbdef7a3b8ad&elqaid=11383&elqat=1&elqCampaignId=10874](https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations?eid=CXTEL000000439070&elqCampaignId=10874&utm_source=nl&utm_medium=email&utm_campaign=newsletter&elqTrackId=8a5fc9c33ec84bca962f8bba4fa87ef1&elq=27c63bceccff84063bf7bcbdef7a3b8ad&elqaid=11383&elqat=1&elqCampaignId=10874)
- Leonard, C. F. (2016). *Commission on enhancing national cybersecurity: RFI response*. [https://www.nist.gov/system/files/documents/2016/09/16/cyber\\_nance\\_rfi\\_response.pdf](https://www.nist.gov/system/files/documents/2016/09/16/cyber_nance_rfi_response.pdf)
- Lipschitz, J. M., Connolly, S. L., Van Boxtel, R., Potter, J. R., Nixon, N., & Bidargaddi, N. (2023). Provider perspectives on telemental health implementation: Lessons learned during the COVID-19 pandemic and paths forward. *Psychological Services*, 20(Suppl. 2), 11–19. <https://doi.org/10.1037/ser0000625>
- Mishkind, M. C., Shore, J. H., & Schneck, C. D. (2021). Telemental health response to the COVID-19 pandemic: Virtualization of outpatient care now as a pathway to the future. *Telemedicine and e-Health*, 27(7), 709–711. <https://doi.org/10.1089/tmj.2020.0303>
- National Alliance on Mental Illness. (2023, April). *Mental health by the numbers*. <https://www.nami.org/mhstats>
- National Institute of Standards and Technology (NIST). (2023). *FIPS 197: Advanced Encryption Standard (AES)*. Information Technology, Laboratory. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>
- National Institute of Standards and Technology and National Cybersecurity Center of Excellence. (2020). *Protecting data from Ransomware and other data loss events: A guide for managed service providers to conduct, maintain and test backup files*. <https://www.nccoe.nist.gov/sites/default/files/legacy-files/misp-protecting-data-extended.pdf>
- Office for Civil Rights (OCR). (2013a, July 26). *Guidance to render unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>
- Office for Civil Rights (OCR). (2013b, July 26). *Is the use of encryption mandatory in the security rule*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html>
- Office for Civil Rights (OCR). (2013c, January 25). *Business associate contracts*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>
- Office for Civil Rights (OCR). (2017, June 16). *HITECH Act enforcement interim final rule*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>
- Office for Civil Rights (OCR). (2022, October 19). *Summary of the HIPAA privacy rule*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/special-topics/summary-of-the-hipaa-privacy-rule/index.html>



- .gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- Office for Civil Rights (OCR). (2023, February 27). *Submitting notice of a breach to the secretary*. U.S. Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>
- Office of the Privacy Commissioner of Canada. (2018, January). *Summary of privacy laws in Canada*. [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02\\_05\\_d\\_15/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/)
- Office of the Privacy Commissioner of Canada. (2020, May). *Provincial laws that may apply instead of PIPEDA*. [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r\\_o\\_p/prov-pipeda/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/)
- Paulsen, C., & Toth, P. (2016). *NISTIR 7621 Revision 1: Small business information security: The fundamentals*. National Institute of Standards Technology. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>
- Perle, J. G. (2021). *A mental health provider's guide to telehealth: Providing outpatient videoconferencing services*. Routledge. <https://doi.org/10.4324/978103150473>
- Perle, J. G. (2022). Mental health providers' telehealth education prior to and following implementation: A COVID-19 rapid response survey. *Professional Psychology: Research and Practice*, 53(2), 143–150. <https://doi.org/10.1037/pro0000450>
- Pierce, B. S., Perrin, P. B., & McDonald, S. D. (2020). Demographic, organizational, and clinical practice predictors of US psychologists' use of telepsychology. *Professional Psychology: Research and Practice*, 51(2), 184–193. <https://doi.org/10.1037/pro0000267>
- Pierce, B. S., Perrin, P. B., Tyler, C. M., McKee, G. B., & Watson, J. D. (2021). The COVID-19 telepsychology revolution: A national study of pandemic-based changes in U.S. mental health care delivery. *The American Psychologist*, 76(1), 14–25. <https://doi.org/10.1037/amp0000722>
- Sammmons, M. T., VandenBos, G. R., & Martin, J. N. (2020). Psychological practice and the COVID-19 crisis: A rapid response survey. *Journal of Health Service Psychology*, 46(2), 51–57. <https://doi.org/10.1007/s42843-020-00013-2>
- Simpson, S., Richardson, L., & Reid, C. (2016). Therapeutic alliance in video conferencing psychotherapy. In S. Gross, K. Anthony, L. S. Stretch, & D. M. Nagel (Eds.), *Technology in mental health: Applications in practice, supervision, and training* (2nd ed., pp. 99–116). Charles C. Thomas.
- The Federal Authorities of the Swiss Confederation - Federal Data Protection and Information Commissioner. (2023, January 27). *Latest News*. [https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell\\_news.html#-2053438021](https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-2053438021)
- Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010, October 4–8). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM conference on computer and communications security* (pp. 162–175). Chicago, Illinois, United States. <https://doi.org/10.1145/1866307.1866327>
- Yellowlees, P., Shore, J., & Roberts, L. (2010). Practice guidelines for videoconferencing-based telemental health—October 2009. *Telemedicine and e-Health*, 16(10), 1074–1089. <https://doi.org/10.1089/tmj.2010.0148>
- Zocdoc. (2021, June 9). *A year in hybrid care*. <https://zocdoc-inc.medium.com/a-year-in-hybrid-care-8413da1252f6>

Received October 23, 2023

Revision received February 23, 2024

Accepted May 1, 2024 ■