Data Handling for E-Mental Health Professionals

Sandeep Grover[1], Siddharth Sarkar[2], Rahul Gupta[3,4,5]

ABSTRACT

Digital psychiatry and e-mental health have proliferated and permeated vastly in the current landscape of mental health care provision. The COVID-19 crisis has accelerated this digital transformation, and changes that usually take many years to translate into clinical practice have been implemented in a matter of weeks. These have outpaced the checks and balances that would typically accompany such changes, which has brought into focus a need to have a proper approach for digital data handling. Health care data is sensitive, and is prone to hacking due to the lack of stringent protocols regarding its storage and access. Mental health care data need to be more secure due to the stigma associated with having a mental health condition. Thus, there is a need to emphasize proper data handling by mental health professionals, and policies to ensure safeguarding patient's privacy are required. The aim of useful, free, and fair use of mental health care data for clinical, business, and research purposes should be balanced with the need to ensure the data is accessible to only those who are authorized. Systems and policies should be in place to ensure that data storage, access, and disposal are systematic and conform to data safety norms.

Keywords: Cyberpsychiatry, epidemiology, qualitative, review

The use of telemedicine and digital platforms by the mental health professionals has accelerated during the current COVID-19 pandemic.[1] Keeping in mind the need for such services during the pandemic situation, the Government of India has provided guidelines for running such facilities.[2]

Telepsychiatry is a field in its own right and has been gradually increasing in scope and application. The ecosystem of telepsychiatry has changed from being telephone-based to digital platforms. Telepsychiatry permeates marketing and listing of mental health services, booking appointments, conducting interviews and therapy, documentation, prescription generation, medication delivery, scheduling follow-up, and other activities. Various mental health sub-specialties can expand in scope and improve the delivery of services due to the potential of telemedicine.[3] The promise of psychiatric services in remote areas by using telepsychiatry has made it one of the important components of telemedicine services.[4] Digitalized medicine is another framework that includes using digital services and devices, whether connected to the internet or not, in the provision of medical services. This includes push toward moving to computerized records instead of handwritten ones and using digital devices in the processes of providing care to the extent possible.

Many countries are already moving toward a national health record for its citizens, which is assessable by health care providers irrespective of location.[5,6] There are considerable benefits in terms of streamlining health care experience, reducing the need for repeat investigations and assessments for the same conditions. Australia is a prime example of this. Most Western countries have well-defined standards and protocols in place for generating, recording, storing, and disposing of health care data. Similarly, specific legal statute are governing the same.

Expansion of telemedicine and digital services draws attention toward appropriate handling of the data. Digital health care data is particularly insecure as health systems are not designed with security in mind. At the same time, it is one of the most valuable data from the perspective of privacy[7] and health research.[8] There have been reports of health care data being hacked and then made available on the dark web.[9] The breach of mental health care data is more sensitive than a breach of several other health care conditions, as considerable stigma still applies to psychiatric disorders. Additionally, the same can have more extreme legal implications compared to the data from different specialties.[10] Thus, psychiatrists and other mental health professionals need to be aware of the issues related to data generation, handling, and disposal. This write-up aims to discuss topics related to data handling relevant to mental health professionals. This article does not intend to go into the depth of the technical and computational aspects of data handling and access. Still, it provides a pragmatic overview of the issues involved in the generation and storage of the data in general.

Definition

Telepsychiatry is "the delivery of health care and the exchange of health information for purposes of providing psychiatric services across distances,"[11] while digital medicine (of which digital psychiatry is a part) is "all the theory, knowledge, technology, and methodology which are involved in solving medical problems using modern digital technology in basic science, clinical medicine, preventive medicine, and so forth, to increase our understanding of life phenomena and the nature of disease as well as to improve clinical diagnosis and treatment."[12]

Data and its Facets

Data has been conceptualized differently by different experts[13] but one of the appealing definitions is that data are the primary individual items of numeric or other information garnered through observation. Still, in themselves, without context, they are devoid of information. Data from the perspective of digital psychiatry is any discrete information that is stored in a digital device and pertains to information about the patient, process of

care, research, or secondary analysis of this information.

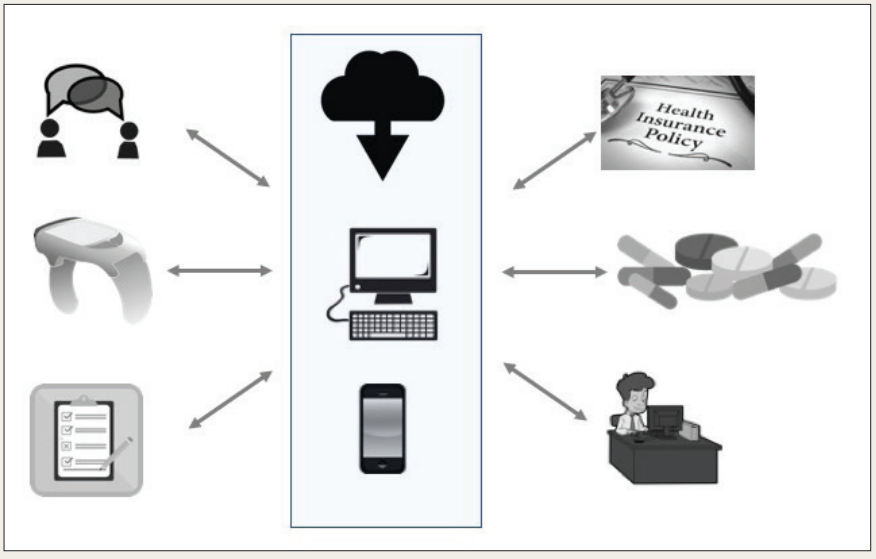
The potential sources of data of relevance to mental health professionals are depicted in **Figure 1**. The source of data can be the interview and assessment process, which can be audio or video recorded in a digital format. Data processing and extraction can be used to convert audio data into text. The information from the intake interview or subsequent mental health professional encounters may be coded into text either by writing the same information or using the audio into the text form by using various software. This process is similar to the notes prepared after an interview, which are stored in files. Current technologies also allow for recognition of handwriting, conversion into text, and textual digitalization of old records as the conversion of text into speech. This data is important as it provides information to other mental health professionals about what was the psychopathology, clinical concerns in a particular case, management plan formulated, and treatment offered. This information would be quite valuable to understand previous treatment approaches and what can be done in the future. Smartphone, wearable device, or computer-based applications can also be used for assessment of mood charting, administration of psychiatric rating scales, and momentary ecological assessment.[14,15] Nursing records also provide information on the physical and mental health conditions. Additionally, the advent of real-time data through sensors are emerging avenues of data collection. Hand movement ascertained through actigraphy, originally used for sleep research, has been used to look at conditions like attention deficit hyperkinetic disorder and delirium.[16,17] As the integration of sensors occurs more seamlessly with wearable devices, it is hoped that minimally obtrusive observation of many psychiatric conditions would occur in the natural home or work environment, and not just in the mental health professionals' "chambers." Other data sources include billing information linked to the mode of payment and other financial information; insurance information about the patient, including the diagnoses, sums reimbursed through insurance, and the reasons for declining claims; and management of inventory including medications (especially when stocking regulated medications like buprenorphine). The potential application of the digital data-based aspects of psychiatric health care is not limited to the above, and many other potential applications are being tried, tested, refined, and implemented in the current circumstances. As mobile phones have become ubiquitous, many research and commercial applications are now available to extract the data from the device sensors to study physiological functioning. For example, stress and nonstress conditions can be differentiated by monitoring electrocardiogram using a chest strap sensor and galvanic skin response using finger sensors and a wrist cuff. This data can be transmitted reliably to a server via Bluetooth.[18]

A related consideration in the mentioned scheme of things is the storage of the data. Traditionally, patient information has been stored in hardcopies of files, typically for at least five to ten years, with the ownership of the data resting with the patient. The digital revolution has allowed storage of data in the form of binary codes that is stored in disc drives. Texts, images, audio, and video are the common types of data from the health care setting that are stored. Localization of the stored data in disc drives in fixed computers and laptops and pendrives has given way to storage of data on mobiles, and access through the internet in remote locations. Uploading data in the "cloud" servers and accessing the data through intranet or internet has become commonplace. As the clinical data moves from paper files that can be physically locked to digital format across devices and often communicated via the internet, it becomes increasingly susceptible to unauthorized access and hacking. For example, electronic medical records got locked due to a ransomware attack on Grays Harbor Community Hospital and Harbor Medical Group.[19]

Data access (i.e., who has access to the digital information and by what means) is a crucial consideration for telepsychiatry and digital psychiatry. Ownership and access to the data within regulatory framework are some of the questions that are being deliberated upon. If the patient is the source of data, the health care provider is also a cocreator of the data. Many regulations over the world do recognize the privacy of the data of the patients, and unauthorized use is punishable. For example, the UK Data Protection Act of 2018 has a provision of penal fine of up to 17 million pounds

FIGURE 1.

Potential Sources of Data for Mental Health Care Practice



Note. Electronic data related to mental health can be generated from patient interviews; smart devices; nursing records, specialist referrals and consultations, and self-filled checklists (can be through mobile devices); insurance claims and information; medication inventories; and administrative, scheduling, and billing sections. Information can be stored in mobiles, computers, or in the cloud.

on the organization using patient data without consent after permission from Confidentiality Advisory Group for serious breach if there is a failure to comply with the provisions and guidelines of data handling.[20] Yet, the data curating and hosting services do have authorized access on as-needed basis. Similarly, health care providers have required access to the data for promoting the health of the patients and populations. Standards have been spelled out about data safety of electronic health records, both in terms of technical specifications and administrative requirements.[21] The individuals or entities that are likely to have access to the data are the patient, clinician, receptionist or administrative staff, computer professionals who have set up the system and maintain it, and those who have access to cloud servers if the data is stored in the cloud. Similar to the paper medical records format, health care regulating authorities and law enforcement agencies, including judiciary, may request for particular records. However, there needs to be a guidance for professionals and public, who are the main stakeholders. Hackers can gain access to the data when they mount an attack. However, data can become accessible to unauthorized personnel when nonencrypted files are available through lost or discarded pendrives, computers, and laptops; and when individuals have left their stations/devices without "logging out" of the health care data portal. Therefore, there is a need for individuals to understand the importance of such an act. Therefore, this needs to be part of induction training before getting involved in providing telepsychiatry services. Maintaining confidentiality of the data of patient information is everyone's responsibility and all professionals need to understand that there are different aspects involved.

The electronic data in mental health care, both online and offline, can have multiple potential uses.[22] The data can be of use to the patients to know the records, timelines, and appraisal of their mental health, especially when they need to switch between different health care providers. Such electronic data may be useful for the mental health professionals to know salient features of patient's history, management, and course of illness. It may also be helpful for researchers to gain insights into the determinants of health and diseases and outcomes of patients with different interventions. For example, the research data can be used for suicide prevention and research on the long-term course and outcome of psychiatric disorders.[23,24] The digital information is of use to insurers in actuarial sciences, in determining the risk of diseases, and the suitable premiums. Activity data may also be of relevance to engineers who would like to develop wearable devices for specific purposes, for example, having an indirect estimation of drug responses in depression.[25] The electronically generated and stored information might be of consequence to the regulatory authorities to understand the adverse effects of certain drugs or interventions. Hospital administrators and managers may use health data for benchmarking, service utilization, and revenues. The blended data can be used at the state and national levels to inform public health policy and for allocation of funding for specific conditions. The pharmaceutical industry (and the health care industry in general) may be interested in the real-time sales data to estimate the demand for particular medications or pharmaceutical products. The finance industry may find the data relevant (if such data is accessible) to determine the credit-worthiness for certain individuals, especially if they are suffering from specific disorders. Advertisers may look at the volume of electronically stored data from one particular demographic where they would like to promote a product. Thus, the value of the mental health care data would be different for different entities based upon their profile, goals, and directions.

Handling of Data and its Importance

The above discussion underscores why the handling of data has to be given due consideration in the field of mental health. Following are some of the issues that are relevant to data handling.

1. Determination of the storage medium: The storage of data can be on a laptop, desktop, local server, or the cloud, or any other medium. Using pendrive for data transfer can be unsafe as pendrives can get lost or accessed without authorization. Hence, such a transfer should be minimized and anonymized if possible. Discarding of the storage medium after use should also be paid attention to, as that can be a source of data leakage. For paper records, medico-legal statutes usually require the health care provider to maintain records for a fixed time period before they can be disposed of. Hence digital data, too, must be appropriately stored and backed up to ensure compliance. Similarly, as for paper records, any post hoc alteration must be suitably recorded by digital means.
2. Encryption of patient data (encoding of information) and other security protocols: Data encryption helps to protect the data even if it is lost in transit or is accessed by unauthorized personnel. Several encryption strategies are available[26] but efficient data encryption methods are required to make the data available and minimal time and computation power is needed for encryption and de-encryption process. Similarly, other security protocols should be in place for the secure transmission of data. Password protection of data is one of the most conventional ways of access controls which ensure security. End-to-end encryption has been provided in messaging and calling applications such as WhatsApp, Telegram, and Line. Telemedicine guidelines do mention WhatsApp as an application that can be used.[2] Ability to make voice calls, video calls to talk to the patient and their caregivers, and sending e-prescriptions as a document, along with the ability to have text conversations, makes it an appealing application for telemedicine. Secret chat in Facebook Messenger also provides end-to-end encryption.
3. Access control policies: This pertains to the legitimate access holders of the data. The more the number of individuals who have access to data, the more are the chances of it

being compromised. Access control policies should spell out who shall have access to the data (complete or partial) and in what circumstances. Such policies, when written and known in a health care organization, help to create an environment of trust and accountability regarding patient data. Also, different access categories can be given entry to various segments of the data. For example, mental health professionals may have information of mental health records, but not billing documents. In contrast, administrative staff may have access to scheduling and billing records, but not psychiatric care records.

4. Access loggings: This pertains to the access to the data by different individuals being logged. The log provides information about who all accessed the data (e.g.,, the doctor, nurse, secretarial staff), and when. This may be helpful to trace unauthorized access to data,[27] especially in the situations of data hacking.
5. Automatic logout: Patient data may be unknowingly exposed to third parties when the last session had not been logged out. Automatic logout after a defined period of inactivity may reduce the chances of such inadvertent access to the health care data.

The handling of data is ingrained in the process of online consultation and needs to be in accordance with the locally relevant guidelines. The telemedicine guidelines in India[2] have provided some clarity in the manner in which telemedicine services are to be provided and what measures are to be taken in the teleconsultation process. Some elements should be considered while providing services.[2] These apply to both treatment and prevention of diseases, and for research purposes. Additionally, it is recommended that log or record of telemedicine interaction and patient records, prescriptions, reports, documents, images, diagnostics, and data (both digital or nondigital) should be retained by the registered medical practitioner. The invoice of the appropriate fee charged by the practitioner should also be provided. Prescriptions, when issued, should not be in contravention of the provisions of the Drugs and Cosmetics Act and Rules. A photo, scan, digital copy of a signed prescription or e-prescription to the patient via email or any messaging platform can be sent, with explicit mention to the patient that he/she can get the medicines dispensed from any pharmacy of his/her choice.

Big Data Analytics

Big data has come up in health care in a significant manner, due to the collation of large patient databases, and advancement in the computational powers and techniques like machine learning.[28] Extensive data in the cloud and distributed systems offer an opportunity to access volumes of data to make consequential inferences. Machine learning algorithms on the more massive data sets have resulted in gaining insights about diagnostics and therapeutics. Deep neural networks can be used and tested with the voluminous merged data from different practices and health care institutions. Data mining from big data is another exciting field that entails getting data of interest from a plethora of data that has been collected. One of the essential steps in big data analytics is the de-identification of the data. This means that identifying details of the patients are coded or removed so that the condition in question is available for analysis without providing details, which may lead to a breach of privacy. The data which are generally de-identified are name, social security number (or Aadhaar number in India, PAN card number or bank details), pin code, and date of birth.

Different Data and Reconciliation

One of the main challenges in compiling and comparing data has been different architectures of data storage. Each of the data systems may have its own defined data capture fields, delimitations, access codings, compression algorithms, and supported operating systems. Automatic cross talk and data conversion across platforms are still a challenge. Hence, data of patients from different sources are reconciled first while aggregating across sources. This might require the use of dedicated software "middleware" for data exchange to occur.

Unique Situations Impacting the Handling of Data

There can be several circumstances when the handling of data may become challenging for mental health professionals. Therein, the usual protocols, means, mechanisms, and statutes may be called up into question. Some of these situations are discussed further.

TABLE 1.

Recommendations for E-Mental Health Professionals for Handling Data

Do consider what data are to be collected from patients, where would that data be kept, who all would have access to the data, and to what component(s)of the data?
Ensure that all the mental health professionals are provided induction training and are updated regularly on local policies and protocols, including data security, login and logout protocols, and data handling.
Separate traceable logins should be available for each individual who has access to the patient data.
Use software and data storage facilities that have data encryption facility and are adept in implementing data security protocols.
Data, when being used for other purposes like research, should be anonymized. Identifying data should be omitted at the time of copying the data. If the data is likely to be used for research, then it is better to inform the patient about it beforehand.
Transfer of the data to colleagues and authorities should be documented by electronic logs in terms of what data was shared, when it was shared, how it was shared, and with whom it was shared.
Automated logout after inactivity should be the norm at the data entry, and access terminals for that pilferage of data can be avoided.
Disposal of obsolete hardware/data storage devices should ensure that the data is wiped clean and securely disposed of.
Incidents of being hacked should be reported to law enforcement or proper regulatory authority.
Exercise reasonable degree of caution while hiring services/ individuals/ applications for technological solutions for telemedicine services, emphasizing on patient's privacy and confidentiality.

Emergencies

During the teleconsultation process, patients may demonstrate the need for emergency care due to a threat of harm to self or others. Such a situation may occur if the patient is suicidal or expresses violence due to psychotic symptoms. Therein, it is crucial to record the consultation appropriately for further necessary action. The subsequent step could be the encouragement of known acquaintances to seek treatment in an emergency setting, or involvement of local law enforcement to defuse the situation. The breach of confidentiality would need to adhere to the telemedical rules and regulations and the legal statutes. The teleconsultation may also serve as evidence in case there is legal fallout of the situation.

Psychotherapy

Online psychotherapy has also gathered steam to prevent the need to travel and physical infrastructure for face–to-face psychotherapy sessions.[29] While psychotherapy has been found to be effective when conducted online, caution has also been expressed about its uptake.[30] The data of the patient emanating out of online psychotherapy can be in the form of digital notes and audio/video records of the session. The documents are potentially instructive, may work well for reflections or teaching material for therapies, and also add-on the patient's mental health profile. However, safe-keeping of such data of the patient also needs to be emphasized to maintain anonymity and confidentiality. Psychotherapy is more appealing to clients when they feel secure and their privacy respected. Ensuring such concerns of the clients are honored would be essential for digital uptake in psychotherapy practices.

Access to Family Members

The Mental Healthcare Act of 2017 mandates that the nominated representative can seek information about the diagnosis and treatment of the patient. However, when the patient does not want the information to be disclosed to family members, then the support needs of the patient may need to be looked at. When there are high support needs of the patient or when capacity is lacking or when the patient is a minor, then the nominated representative would make decisions for the patient and would need information about previous diagnosis and treatment. In such situations, it might be prudent to provide information to the nominated representative. However, when the patient has low support needs, it is better to have consent from the patient (preferably audio-recorded, video-recorded, emailed, or texted) before disclosing information to the relative.

Access to Regulatory Authorities

As the digitalization of services increases, the data is also likely to be under the scrutiny of the regulatory authorities (as with hardcopy case records). Data appraisal and compliance might be required in health care, as has been becoming commonplace with financial data. Data systems would need to be compliant with regulatory standards. The Health Insurance Portability and Accountability Act[31] of 1996 of the United States is one of the initial such regulatory framework implemented to ensure the privacy and security of the digitalized patient data.

The Interface of Data of Different Disorders or Specialties

The internet of things[32] is expanding its footprint, and it aims to interconnect different devices and data streams to improve experience and output, health care in this case. As patient care improves with real-time monitoring of various physiological parameters, treatment decisions are being expedited for several diseases. Remote observation and intervention are becoming possible, with even robotic surgeries being performed by surgeons in a different location. Such real-time data capture and patient monitoring may become commonplace in mental health care, especially for patients who are violent or suicidal, and multimodal inputs, including vocal intonations, sudden jarring movements, and autonomic parameters may be used to develop predictive models and preemptive action protocols.

Data Breaches and Data Hacking

Data breach is an encompassing term that implies that data has been available to nondesignated individuals or entities. The data breach does not mean a malicious intent. It can occur due to data loss or improper data disposal, along with incidents of data hacking that are done with malicious intent.[33] Data hacking includes unauthorized access to the data or blocking the working of data management systems with the intent of obstructing work or getting ransom (ransomware). Over time, health care data breaches have resulted in the loss of data, exposure of identified data to unauthorized personnel, and disruptions in the functioning of the hospitals. Suitable exposure reduction, security enhancement, and organization access control features are likely to reduce the instances of such data breach and hacking. Guidelines and uniform policies would help to bring clarity and standard operating procedures for data handling. The concept of ethical hacking entails hacking with the intent of exposing vulnerabilities, so that corrective measures can be taken to enhance security systems in place, both in the software and in the procedural accesses.

Recommendations for E-Mental Health Professionals for Handling Data

In this section, we provide some recommendations for mental health professionals as they handle the data, from the perspective of telemedicine and digital psychiatry. These are summarized in **Table 1**.

Issues of Consent for the Generation and Use of Data (Clinical and Research)

Prescription—Requirements as per the Telemedicine Guidelines

Incomplete data has several problems associated with it. These can be legal, clinical, and research related. Incomplete data ascertainment can lead to suboptimal care, which may make a practitioner liable to negligence. For example, regularly conducting and documenting mental status examination for a patient with bipo-

TABLE 2.

Suggestions for Data Handling During Conduct of Mental Health Research

Conduct of Research Through Telemedicine

- Consider collecting anonymized data if possible, especially for cross-sectional studies (i.e., avoiding capture of IP address, name, Aadhaar number, date of birth, and pin code)
- Consider using end-to-end encrypted platforms for data collection.
- Consider taking consent using checkboxes developed as an online form. Multiple boxes can be used for different elements of data collection.
- Check the data collection process by dummy entries to check whether data capture is working properly.
- Consider whether the online mechanism of data collection would be used or asynchronous periodic data uploading. If data is not immediately sent, then there is a chance of data loss due to device malfunction, theft, and data corruption.
- Consider beforehand who all will have access to the data (preferably those who have access intimated in a mail).
- Electronic vaults can be used to store the data. Data should be securely deleted after conducting the analysis.
- In case emailing of data is required, or data has to be posted in a repository, then the de-identification of the data should be ensured.
- Consider having ethics committee oversight for the study.

Conduct of Secondary Data Research

- Consider collecting anonymized data, if possible, from the source. Consider minimal information being drawn from the sources.
- Consent might not have been taken from the participants beforehand. Consider having ethics committee oversight for the study.
- Consider beforehand who all will have access to the data (preferably those who have access intimated in a mail).
- Electronic vaults can be used to store the data. Data should be securely deleted after conducting the analysis.
- In case emailing of data is required, or data has to be posted in a repository, then the de-identification of the data should be ensured.
- Certified email systems should be used for the transmission of health data, making sure attachments are password protected. Corporate and subscription-based emails offer better security than free email service. Some health organizations (e.g., NHS) specifically certify their emails to communicate health data.

lar disorder frequently, especially when making decisions about changing medications or considering admissions, would be helpful, especially if adverse outcomes occur and patient's family would like to take to court. The capture of data is related to documentation of data, with the tenet that if it was not documented, then it was not asked (this being similar to hardcopy records). Thus, attempts should be made to provide reasonable comprehensiveness of data, that is, what an adequately trained professional is likely to record or proceed with. The clinical issue with lack or loss of data is that the management plan would be impeded if crucial information is missing. The inadequacy of data may not serve to assist in research and, therefore, policies.

Legal requirements while dealing with data for mental health professionals pertain to Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002, and with the relevant provisions of the IT Act and the notifications that are issued from time to time regarding the protection of privacy and confidentiality of the patient. The recent Indian telemedicine guidelines mention that registered medical practitioners will not be held responsible for breach of privacy provided that it was caused by technology or some other person, provided a reasonable degree of caution was taken for the hiring of such services. Willful compromise of patient confidentiality is not permissible, for example, misusing patient images and data, especially private and sensitive in nature, using telemedicine to prescribe medicines from the specific restricted list, and soliciting patients for telemedicine through any advertisements or inducements. It is important to be aware of of legal provision from the Information Technology Act (section 22) which provides that anyone who has secured access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document, or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.[34] The section 108 of Mental Health Care Act, 2017, mentions that any person who contravenes any of the provisions of this Act, or of any rule or regulation made there under shall for first contravention be punishable with imprisonment for a term which may extend to six months, or with a fine which may extend to 10,000 rupees or with both, and for any subsequent contravention with imprisonment for a term which may extend to two years or with fine which shall not be less than 50,000 rupees but which may extend to five lakh rupees or with both. This is relevant when considering provision of confidentiality under section 23 of the Act.

An expanding ambit would be the use of telemedicine for the conduct of research or the use of secondary data for research purposes. We offer specific suggestions for dealing with various issues about data handling in such circumstances (**Table 2**). However, there is a need to formulate guidelines for the same. It is important to develop guidelines about safeguards for the patient and families in terms of how their data may be used for research purposes. Several online questionnaire services are now available, such as SurveyMonkey and Google Forms.

Conclusion

As mental health professionals deal with voluminous amounts of data, attention is drawn toward proper handling of the data. Data and its collective analysis are useful for the current patient as well as other patients. Loss of data and its unauthorized access puts the privacy of the patients at risk. Efforts are required to improve the security protocols of data handling to ensure that confidence is retained in the e-mental health services. Continued efforts at improving data generation, storage, handling, and disposal are likely to improve the care, care processes, and outcomes of the patients.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

1. Portnoy J, Waller M, and Elliott T. Telemedicine in the Era of COVID-19. J Allergy Clin Immunol Pract 2020; 8(5): 1489–1491.
2. Board of Governors, in supersession of the Medical Council of India. *Telemedicine practice guidelines enabling registered medical practitioners to provide health care using telemedicine* [Internet], https://www.mohfw.gov.in/pdf/Telemedicine.pdf (2020).
3. Punnoose V and Sarkar S. Advances in IT and social psychiatry. Indian J Soc Psychiatry 2016; 32(3): 267–269.
4. Barnett ML, Ray KN, Souza J, et al. Trends in telemedicine use in a large commercially insured population, 2005–2017. JAMA 2018; 320(20): 2147–2149.
5. Hossack E. Australia's national health record-putting the PCEHR into perspective. Medicus 2015; 55(8): 33.
6. Suna T. Finnish national archive of health information (KanTa): general concepts and information model. FUJITSU Sci Tech J 2011; 47(1): 49–57.
7. Coventry L and Branley D. Cybersecurity in health care: a narrative review of trends, threats and ways forward. Maturitas 2018; 113: 48–52.
8. Casey JA, Schwartz BS, Stewart WF, et al. Using electronic health records for population health research: a review of methods and applications. Annu Rev Public Health 2016; 37: 61–81.
9. Conaty-Buck S. Cybersecurity and health care records. Am Nurse Today 2017; 12(9): 62–64.
10. Gooding P. Mapping the rise of digital mental health technologies: emerging issues for law and society. Int J Law Psychiatry 2019; 67: 101498.
11. Wootton R, Yellowlees P, and McLaren P. *Telepsychiatry and e-mental health*. London: Royal Society of Medicine Press Ltd., 2003.
12. Zhang S, Liao R, Alpert JS, et al. Digital medicine: emergence, definition, scope, and future. Digit Med 2018; 4: 1–4
13. Zins C. Conceptual approaches for defining data, information, and knowledge. J Am Soc Inf Sci Technol 2007; 58(4): 479–493.
14. Hassem T and Laher S. A systematic review of online depression screening tools for use in the South African context. South Afr J Psychiatry 2019; 25: 1373.
15. Bell IH, Lim MH, Rossell SL, et al. Ecological momentary assessment and intervention in the treatment of psychotic disorders: a systematic review. Psychiatr Serv 2017; 68(11): 1172–1181.
16. Maybrier HR, King CR, Crawford AE, et al; ENGAGES Study Investigators. Early postoperative actigraphy poorly predicts hypoactive delirium. J Clin Sleep Med 2019; 15(1): 79–87.
17. Faedda GL, Ohashi K, Hernandez M, et al. Actigraph measures discriminate pediatric bipolar disorder from attention-deficit/hyperactivity disorder and typically developing controls. J Child Psychol Psychiatry 2016; 57(6): 706–716.
18. Sun FT, Kuo C, Cheng HT, et al. Activity-aware mobile stress detection using physiological sensors. In: Gris M and Yang G (eds) *Mobile computing, applications, and services.* Heidelberg: Springer, 2012, 211–230.
19. Davis J. $185K Proposed Settlement Reached in Grays Harbor Data Breach Lawsuit, https://healthitsecurity.com/news/185k-proposed-settlement-reached-in-grays-harbor-data-breach-lawsuit (2020, accessed July 28, 2020).
20. UK Data Protection Act of 2018, https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (accessed September 14, 2020).
21. National Health Portal of India [Internet]. Data privacy and security [cited 2020 Jun 26], https://www.nhp.gov.in/data-privacy-and-security_mtl (accessed September 14, 2020).
22. Kumar MS, Krishnamurthy S, Gowda MR, et al. The dawn of e-mental health professional. Indian J Psychiatry 2019; 61(4): S730–S734.
23. Jing Y, Hu Z, Fan P, et al. Analysis of substance use and its outcomes by machine learning. I: Childhood evaluation of liability to substance use disorder. Drug Alcohol Depend 2020; 206: 107605.
24. Burke TA, Ammerman BA, and Jacobucci R. The use of machine learning in the study of suicidal and nonsuicidal self-injurious thoughts and behaviors: a systematic review. J Affect Disord 2019; 245: 869–884.
25. Vahia IV, and Sewell DD. Late-life depression: a role for accelerometer technology in diagnosis and management. Am J Psychiatry 2016; 173(8): 763–768.
26. Abouelmehdi K, Beni-Hessane A, and Khaloufi H. Big health care data: preserving security and privacy. J Big Data 2018; 5(1): 1.
27. Chernyshev M, Zeadally S, and Baig Z. Health care data breaches: implications for digital forensic readiness. J Med Syst 2019; 43(1): 7.
28. Pashazadeh A and Navimipour NJ. Big data handling mechanisms in the health care applications: a comprehensive and systematic literature review. J Biomed Inform 2018; 82: 47–62.
29. McDonald A, Eccles JA, Fallahkhair S, et al. Online psychotherapy: trailblazing digital health care. BJPsych Bull 2020; 44(2): 60–66.
30. Van Daele T, Karekla M, Kassianos AP, et al. Recommendations for policy and practice of telepsychotherapy and e-mental health in Europe and beyond. J PsychotherIntegr 2020; 30(2): 160–173.
31. Office for Civil Rights (OCR). Summary of the HIPAA security rule [Internet]. HHS.gov2009 [cited June 26, 2020], https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (accessed September 14, 2020).
32. Banerjee A, Chakraborty C, Kumar A, et al. Emerging trends in IoT and big data analytics for biomedical and health care technologies [internet]. In: Balas VE, Solanki VK, Kumar R and Khari M (eds) *Handbook of data science approaches for biomedical engineering*. Elsevier [cited June 26, 2020]. 2020, 121–152. https://linkinghub.elsevier.com/retrieve/pii/B9780128183182000052 (accessed September 14, 2020).
33. Dolezel D and McLeod A. Cyber-analytics: identifying discriminants of data breaches. Perspect Health Inf Manag 2019; 16: 1a.
34. Government of India. *The Information Technology Act, 2000*. New Delhi: Government of India, 2000.

[1]Dept. of Psychiatry, Postgraduate Institute of Medical Education and Research, Chandigarh, India. [2]Dept. of Psychiatry, All India Institute of Medical Sciences, New Delhi, India. [3]NMHEC-RAP Telepsychiatry Service. [4]Intermediate Stay Mental Health Unit. [5]Faculty of Health and Medicine, University of Newcastle, Callaghan NSW, Australia.

HOW TO CITE THIS ARTICLE: Grover S, Sarkar S, Gupta R. Data handling for e-mental health professionals. *Indian J Psychol Med.* 2020;42(5S):85S–91S

Address for correspondence: Sandeep Grover, Dept. of Psychiatry, Postgraduate Institute of Medical Education and Research, Chandigarh 160012, India. E-mail: drsandeepg2002@yahoo.com

ACCESS THIS ARTICLE ONLINE
Website: journals.sagepub.com/home/szj
DOI: 10.1177/0253717620956732