Medical Confidentiality

in the Era of Digital Health

Text by Dr T Thirumoorthy

> *Whatever, in connection with my professional practice or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.*
>
> – Hippocratic Oath

The tenets of medical confidentiality were first enunciated by Hippocrates more than 2,500 years ago,[1] and still remain an important pillar of building trust and confidence in the profession and the healthcare system. The doctor-patient relationship is a special relationship of trust and confidence. Information received in such a relationship is privileged information, to be used only in ways that are consistent with the understanding of the original disclosure, with the expectation that it will not be divulged to others inappropriately. In medical practice, such confidential information is to be used for the primary purpose of therapeutic benefit and promoting the welfare of the patient.

The duty to uphold medical confidentiality, which has been enshrined in professional codes of conduct, is one of the fundamental duties of all healthcare professionals. The professional's obligation of confidence extends to all patients, whether they are children, elderly or persons with diminished mental capacity.

However, the practice of medicine has rapidly evolved over the years, with advances in science and technology alongside changes in societal structures, relationships and expectations. Today, a large part of patient interaction and delivery of healthcare is moving into the realm of digital health, which involves the use of information and communication technologies to build relationships, communicate, make medical decisions for illness management and deliver care. Medical care is often delivered by multidisciplinary teams using shared electronic medical records (EMRs), and in consultation with non-clinical professionals in administrative and social work agencies, and even family members who have become caregivers.

The era of digital health has shaped new challenges in promoting and preserving the tenets of medical confidentiality. Let us first understand the ethical and legal basis for maintaining medical confidentiality in medical practice.

Ethical basis for preserving medical confidentiality

The fiduciary nature of the doctor-patient relationship is based on trust and mutual respect, and includes principles of consent, fidelity and truth telling. Confidentiality is the bedrock of trust which enables patients to freely share their medical and personal information with their doctor without fear of inappropriate disclosure. This free sharing of information not only helps the doctor to arrive at an accurate diagnosis and develop an effective management plan for the patient's benefit, but also has value for public health disease management.

The preservation of medical confidentiality is guided by the ethical principle of respect for patient autonomy. Mentally competent patients have the right to control the use of information pertaining to them (ie, informational privacy). Patients have the right to determine the person, time and manner of disclosure of their sensitive information. This right is limited by the obligation to not harm others and/or wider public health, legal and societal interests.

When healthcare professionals disclose confidential information to others without the patient's consent or knowledge, or against the patient's wishes, that is considered a lack of respect for or disregard of patient's autonomy. Even when it is justified to share confidential information with others against the patient's wishes, respect for patient autonomy still requires that all practical attempts must be made by the professional to appropriately inform the patient.[2]

Legal basis for preserving medical confidentiality

The legal basis of confidentiality is embedded in common law and supports the public interest of protecting the public and public health.[3] It is in society's interest that the public and patients have trust in the health system so that they will seek treatment for illness. A trusted and effective healthcare system promotes a healthy society, social security, social cohesion and harmony within a society, which are of public interest. The management of infectious disease outbreaks and epidemics requires the public to share accurate and timely information about their health, contacts and travels. Unless patients are certain that no harm will befall them for their disclosure, they are unlikely to divulge all that is necessary for managing the epidemic and their medical condition. It is in the public's interest that persons with infectious diseases seek early treatment, so as to limit its spread. Public interest in medical confidentiality thus lies in the preservation of the public's trust in the healthcare system and the medical profession.

The law, through statutes and regulations, stipulates specific obligations to preserve medical confidentiality (eg, Termination of Pregnancy Act and Infectious Diseases Act) and when confidential information is legally authorised to be released to appropriate persons (eg, Infectious Diseases Act, Enlistment Act, Immigration Act, Misuse of Drugs Act, Workplace Safety and Health Act). Two other statutes of importance for digital health are the Personal Data Protection Act – an act which governs the collection, use, protection and disclosure of personal data by organisations – and the Computer Misuse Act, which makes legal provision for securing computer material against unauthorised access or modification and preventing abuse.[4]

The Ministry of Health is proposing to introduce the Health Information Bill (HIB) in the first half of 2024. The HIB will make it mandatory for all licensed healthcare providers to contribute data to the National Electronic Health Record, and in return will provide them access to patients' summary medical records for patient care. There is a provision in the bill for a subset of "Sensitive Health Information" which will not be readily accessible compared to other key health information.[5]

Multidisciplinary teams and medical confidentiality

Let us now look at two important aspects of digital health that can provide challenges to preserving the tenets of medical confidentiality. A New Zealand study in 2007 estimated that an average patient admitted to a hospital for inpatient care would be attended to by between 17 to 26 healthcare professionals.[6]

Hospital-based multidisciplinary teams are essential to deliver good quality care and prevent errors. The teams often comprise several healthcare professionals, including patient-aides, nurses, physical therapists, social workers, specialist doctors and attending physicians. Clear, effective and unhindered communication channels are essential for sharing information, conducting handovers, exchanging ideas and making informed decisions. This enables all team members to work collaboratively towards the same goals. It is not an uncommon practice for physicians to text other physicians about work on their mobile devices, and even send relevant images. However, keeping the information in these exchanges secure is a major concern. Encrypting mobile devices used to transmit confidential information is of the utmost importance.[7]

Sharing of medical and personal information is acceptable between medical teams for the patient's therapeutic benefits. There is implied consent in addition to explicit consent when patients enlist in EMRs. Nevertheless, all healthcare workers and institutions are under professional obligation to keep their patients' information confidential.

The team, hospital and healthcare systems must ensure that information shared remains within the team for patient care-related purposes only. Licensed healthcare professionals are under oath and governed by the profession and hospitals' codes to maintain confidentiality. Healthcare professionals' ethical and legal obligations require them to achieve a delicate balance between unhindered sharing of confidential information within the treatment team and protecting patient confidentiality, embodying the principles of beneficence and autonomy, respectively.

EHRs and medical confidentiality

EMRs are a central feature of the diagnostic and therapeutic process and a permanent feature of healthcare systems. The electronic health record (EHR) is contemporaneous and interactive, with multiple stakeholders, contributors, reviewers and users of the documentation. The data and information contributed originate from the doctor-patient clinical relationship, is confidential and must be protected.

A potential vulnerability of EHRs is that large amounts of personal and critical medical data may be accessed by a wider audience rapidly and also widely exchanged between and among organisations, clinicians and healthcare providers.[7] Storage, transportation, reproduction and retrieval of the medical data are also possible with small portable devices.

Another threat to EHRs is that data can be hacked, manipulated or destroyed by internal or external parties. A single lapse in security can lead to catastrophic and damaging effects. The integrity of the electronic information holders and the security of the data itself are key factors in preventing breaches. Preserving confidentiality

is achieved by making sure that only authorised individuals have access to the data, and by preventing cyberattacks and cybercrimes.

Going forward

It is clear that in the era of digital health, preserving medical confidentiality is no longer just the individual healthcare professional's responsibility. The responsibility is spread among the medical-clinical teams and the leadership of teams, hospitals and healthcare systems responsible for providing healthcare services.

Individuals and teams

At the level of the individual and medical teams, proper education and skills enabling must occur in handling electronic records and devices where inadvertent errors may breach patient confidentiality. Healthcare professionals should not access a patient's electronic records unless they are part of the patient's therapeutic team or are doing so clearly for the benefit of the patient's welfare. Healthcare professionals should not be tempted to access confidential information for personal gain, social reasons, curiosity or other frivolous or vindictive intent. This includes attempting to access the records and information of relatives, friends or colleagues, even if they seemed to have consented to such access. Comprehensive confidentiality policies that clearly outline the responsibilities of all healthcare team members should be developed, and confidentiality agreements should be signed by all relevant parties internal and external to the organisation.

When sharing confidential information via email, fax, phone and/or hard copy printouts, there is a potential for inadvertent or purposeful data intrusion by unauthorised persons. The use of personal mobile phones for accessing patient data is strongly discouraged as these devices can be easily lost or compromised, posing a risk to confidentiality. Instead, special corporate mobile devices with appropriately secure enterprise solutions could be provided.

All digital systems are potentially vulnerable to cybersecurity lapses and attacks. Healthcare professionals should be educated and held responsible for upkeeping healthy cybersecurity habits, using these systems responsibly and complying with all security protocols. All patient-related information received from electronic records or otherwise should be handled with the standards of the profession's duty of confidentiality.

Organisations and leadership

In the era of digital health, healthcare organisations and leadership have an even greater responsibility and an active role in preserving medical confidentiality. Healthcare organisations need to have a robust system for the preservation of data confidentiality, integrity and availability. EMRs are susceptible to cybercrimes such as hacking, phishing and malware attacks. Healthcare systems must prioritise cybersecurity, train personnel effectively, and implement robust access controls to prevent breaches.[7]

Healthcare organisations must formally develop a comprehensive data protection policy. They must also designate a data protection officer to work with a team of health information technology (IT) experts who can not only monitor users and technologies, but also identify the system's security weaknesses and threats and remedy them.

Healthcare organisations should develop effective educational modules that enable all their healthcare professionals to understand the legal and ethical aspects of medical confidentiality and cybersecurity, and to develop good habits to meet professional standards. Clinician leaders will need to meet clinical, ethical and technological standards of competence, and thus be given the opportunity to achieve higher knowledge and qualifications in health informatics. Creating useful and accurate EHR systems will require the expertise of physicians, other clinicians, information management and technology professionals, lawyers, and administrative personnel led by healthcare leaders.

Conclusion

Collaboration among multidisciplinary therapeutic teams is considered a key factor in achieving high quality patient outcomes and preserving medical confidentiality. Likewise, collaboration among healthcare organisations, IT experts, clinicians and health professionals is essential to preserving medical confidentiality, by prioritising the confidentiality, security and integrity of EMRs. ◆

References

1. The Editors of Encyclopaedia Britannica. Hippocratic oath. In: Encyclopaedia Britannica. Available at: https://bit.ly/3OQFAIW. Accessed 20 February 2024.

2. General Medical Council. Confidentiality: good practice in handling patient information. Available at: https://bit.ly/49iHHgR. Accessed 20 February 2024.

3. W v Egdell. (1990) 1 All ER 835.

4. Government of Singapore. Singapore Statutes Online. Available at: https://bit.ly/3T7NnVn. Accessed 20 February 2024.

5. Ministry of Health. Public Consultation on the Health Information Bill. In: REACH. Available at: https://bit.ly/3uNiHzq. Accessed 19 February 2024.

6. Whitt N, Harvey R, McLeod G, Child S. How many health professionals does a patient see during an average hospital stay? N Z Med J 2007; 120(1253):U2517.

7. Harman LB, Flite CA, Bond K. Electronic Health Records: Privacy, Confidentiality, and Security. Virtual Mentor 2012; 14(9):712-9.

Dr Thirumoorthy has been with the SMA Centre for Medical Ethics and Professionalism (SMA CMEP) since its founding in 2000 and has most recently been given the responsibility of being the SMA CMEP Academic Director.