Remote Patient Management: Balancing Patient Privacy, Data Security, and Clinical Needs

Peter Choi^a · Rachael Walker^b

^aDepartment of Nephrology, John Hunter Hospital, New Lambton Heights, NSW, Australia;

^bSchool of Nursing, Eastern Institute of Technology, Napier, New Zealand

Abstract

Remote monitoring of dialysis offers significant clinical benefits to patients and healthcare providers. However, the collection, transfer, and storage of large amounts of health data involved in remote monitoring require a careful consideration of privacy and data security concerns. Failure to adequately balance clinical utility with privacy has the potential to reduce patients' confidence in remote monitoring and could represent ethical and medicolegal risks for clinicians. We provide 3 case vignettes that illustrate the real-life balance of utility and privacy in patients who received peritoneal dialysis with remote monitoring. We review the principles of health data privacy, confidentiality, and security with respect to remote monitoring as a guide for clinicians.

© 2019 S. Karger AG, Basel

Introduction

Patient A is a 75-year-old lady, with end-stage kidney disease (ESKD) due to hypertensive nephrosclerosis. She had a medical history of labile hypertension and depression with anxiety. At the point that she developed ESKD, she was functionally independent and living with her husband in a private home. Following education and counselling for her ESKD treatment, patient A elected to initiate overnight automated peritoneal dialysis (APD). Patient A performed her own

dialysis, but found it reassuring and helpful to have her husband in attendance. For 2 years, she managed well, with no peritonitis episodes and good clinical status.

When patient A's husband became unwell with a chronic illness, the couple moved into a monitored retirement village, where patient A continued her APD. Shortly thereafter, her husband died. This triggered a severe depression and a crisis of confidence for patient A, such that she believed that she would be unable to continue to perform her APD. Patient A was strongly supported by the knowledge that remote monitoring of her APD cyclers was reviewed regularly by her PD clinicians and continued with her dialysis. Two years after the death of her husband, she continues with remote monitored APD, is in good clinical condition, and has still suffered no peritonitis episodes. She is thankful for the role that remote monitoring has played in maintaining her quality of life.

Patient B was a 35-year-old lady with CKD due to biopsy-proven IgA nephropathy. She was morbidly obese, actively smoking, and suffered from hypertension and obstructive sleep apnea. She elected to perform overnight APD when she developed ESKD. Patient B was unemployed, and lived in a socially complex environment with young children and extended family. Clinical assessment of patient B suggested under-dialysis with serum urea >30 mmol/L and creatinine $>1,000$ $\mu\text{mol/L}$. Her weekly PD clearance was calculated to be mathematically adequate (total Kt/V 2.3, total creatinine clearance 88 L per week) but remote monitoring of her overnight cycler revealed that she frequently did not perform PD. Patient B was reluctant to agree with this assessment and elected to convert to hemodialysis. Before establishing hemodialysis, she presented to the emergency department with chest pain and died suddenly. Coroner's post-mortem examination revealed pulmonary congestion and coronary artery disease. Remote monitoring revealed that patient B had hardly performed dialysis in the week before terminal presentation. This information was provided to the coroner but clinicians were conflicted about whether this information should be shared with the grieving family.

Patient C is a 26-year-old man with ESKD, secondary due to IgA nephropathy who had been receiving peritoneal dialysis (PD) for 18 months. Clinical assessment of patient C indicated that he was under-dialyzed and there was concern amongst his clinicians that he was "failing" PD, with a serum creatinine of $>1,000$ $\mu\text{mol/L}$, serum urea of >35 mmol/L. His clinical status was reviewed as part of the assessment for kidney transplantation. Although patient C admitted to missing "the odd treatment," remote monitoring indicated that he had missed up to 4 overnight cycler sessions each week. Acknowledgement of remote monitoring enabled re-education about the risks of inadequate dialysis and allowed the reasons for missed treatments to be explored. His non-adherence with PD

was identified as an adverse risk factor for transplant outcome. It was agreed with patient C that he would remain actively listed for transplantation due to improved clinical status with adequate dialysis, but that remote monitoring would be reviewed as part of the ongoing assessment of his commitment to transplantation. Patient C continues to perform his dialysis regularly, is clinically well and remains listed for transplantation.

These 3 patient stories represent different aspects of the spectrum balancing the clinical utility of remote monitoring with an individual's right to health data privacy. For patient A, the clinical benefits of remote monitoring were self-evident and she never entertained questions about data use and privacy. For patient B, benefits of remote monitoring were mitigated by exercise of autonomous self-determination and information from remote monitoring was not openly shared because of privacy concerns, despite being an important clinical consideration. Patient C represents the most carefully balanced example of remote monitoring to improve patient care. With the patient's agreement, remote monitoring enabled his inadequate dialysis to be addressed and became the basis of an informal patient-provider contract to ensure the best possible outcome from transplantation.

Health data usually contains sensitive information that needs to be protected to maintain patient privacy. Increasing demands on the healthcare system and advances in technology have seen healthcare providers adopt data management systems in an attempt to provide efficient, affordable, and accessible care. Digitizing medical records has seen a paradigm shift in the healthcare industry with more complexity of data transfer and need for increased timeliness in data transfer, such as remote monitoring. Potential conflict may arise from balancing a patient's right to have access to his or her own data, while also preserving the right for a patient to keep health data private if he or she so wishes. It is increasingly important for clinicians to understand their ethical and legal responsibilities in balancing clinical benefit with a patient's rights to privacy relating to that data. Failure to understand these responsibilities may lead to clinical or legal misadventure. We examine these issues with respect to the use of remote monitoring for PD.

Ethical Considerations in Remote Monitoring

In determining the balance of clinical utility and right to privacy in remote monitoring, clinicians essentially make judgments about potentially conflicting ethical claims. The four commonly accepted principles of medical ethics are respect for autonomy, non-maleficence, beneficence, and justice [1]. Clinicians have a

prima facie duty to uphold these principles as part of their clinical practice. However, when 2 or more of these principles are in conflict, clinicians should balance the merits of each principle, acknowledging the non-hierarchical standing of each of the four ethical principles. How do the principles of medical ethics apply to remote monitoring?

Respect for autonomy is encompassed by the granting of informed consent for remote monitoring. An individual patient is required to provide informed consent for remote data collection, transmission, and reporting to occur and should provide this permission specifically, voluntarily, and with mental capacity to understand the consequences of their decision.

Non-maleficence in remote monitoring is primarily concerned with confidentiality and data security and the obligations of responsible parties to avoid data loss either inadvertently or as a result of hacking. Patients can reasonably expect for their data to be treated confidentially as part of their informed consent. Because overall data security involves a complex interaction between manufacturers, telecommunications, and clinical IT systems, the issue of non-maleficence in remote monitoring must be carefully considered.

Beneficence considerations of remote monitoring relate to the primary benefit of the intervention for the individual patient. Different aspects of the benefits of remote monitoring are considered in separate chapters of this book, and we do not discuss this further, other than to acknowledge the ethical importance of beneficial effect in justifying an intervention that could have coincidental detrimental effect.

Justice in healthcare requires that each individual is treated fairly and has equal access to healthcare as their peers. Justice in healthcare must take into account that most resources are not infinite but that the criteria for distribution are fairly applied to all individuals; in other words, distributive justice is upheld. When considering remote monitoring, this may mean that clinicians need to clearly define who may benefit from remote monitoring and ensure that all such eligible individuals receive remote monitoring and access to their data at reasonable cost.

Data Privacy and Confidentiality

As stated by the US National Committee on Vital and Health Statistics, “Health information privacy is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate” [2].

Although there are no universally agreed standards for health data privacy and confidentiality, certain principles can be distilled. These principles incorporate ethical considerations and include:

- 1 Consent for data collection and an individual's right to review and access their information.
- 2 Specific consideration for what information will be shared; with whom; and for how long.
- 3 Transparency about how failures of privacy and confidentiality will be managed.

Most countries have enacted privacy laws that protect patient data, but significant variability exists between jurisdictions. In the United States, the Health Insurance Portability and Accountability Act governs the privacy and security of health information. The European Parliament developed the “Regulation of the European Parliament and of the Council on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data,” also known as the General Data Protection Regulation. In Australia, health information is governed by the Privacy Act 1988, whilst in New Zealand the Privacy Act 1993 applies. One important consequence of worldwide data movement is that a situation could arise where a patient may receive dialysis in New Zealand, using remote monitoring infrastructure provided by a company incorporated in Australia, which warehouses data in Ireland. Such scenarios create ethical and legal complexities.

Principles of Data Security

Data security is different from data privacy and confidentiality and can be defined as “physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure” [2]. Security is one of the most important aspects of any healthcare system, and it must be effective to ensure that privacy and confidentiality can be guaranteed. Put another way, ineffective data security has the potential to reverse the clinical benefits that result from remote monitoring.

Individuals and organizations may have different perspectives regarding security, and hence it may be defined in many ways. Security implies data are protected from unauthorized users when being transferred, collected, processed and remains safely stored to protect identifiable health data from unwarranted access or disclosure. Remote monitoring devices are wireless devices, and therefore may result in various security threats. Some risks involve the potential to track the location of a patient and use private data to harm the person. However,

healthcare applications, such as remote monitoring are similar to other wireless sensor networks, and most of the security issues are comparable and have already undergone much refining and development to improve security.

Data security breaches may also arise from user error when handling data rather than inadequate security systems. Clinicians should recognize that they have a significant personal responsibility and ensure that they work within the guidelines and procedures relevant to their practice. Institutions must provide adequate training for clinicians and administrative staff about their individual privacy obligations and configure suitable audit systems. One key to preventing user error security breach is the limitation of authorized access to information. This starts with authorizing users and their level access based on pre-established role-based privileges. A delegated administrator determines the level of information to be shared and each user is assigned individual and frequently updated usernames and passwords.

To counter the major threats to information, 2 broad level security measures can be applied – encryption and authentication. Any communication of personal health information and data over the networks must be encrypted.

Data Encryption

The data are encrypted so that they are not disclosed whilst in transit from patient to server. Data encryption service provides confidentiality against eavesdropping attacks. All communications over wireless networks and Internet are required to be encrypted to protect the user's privacy. Some countries have also added this type of clause in their existing legal acts or enacted new laws.

Data Authentication

Authentication consists of the process of confirming the origin and validating the integrity of data. It is an efficient method against impersonation attacks.

The risks of inadequate security should not be underestimated. Despite many assurances of secure data management in healthcare, major health insurance companies have experienced data breaches involving millions of customers [3]. Both the Office of the Australian Information Commissioner [4] and the UK Information Commissioner [5] reported that healthcare providers were a major source of data breaches in 2018. Specific to the dialysis context, there has even been a reported incident where cyber-attack compromised a dialysis machine [6].

Finally, clinicians and institutions should be aware of their obligations for reporting breaches of health data security. Procedures will differ by context and institutional or legal requirement, but review of security breaches are required to identify patterns of failure and improve ongoing security implementation.

The Patient's Perspective

Individual patient's perspectives on the balance between data privacy and clinical utility in remote monitoring will differ according to their own personal priorities and needs, but how can these individual differences be incorporated into the configuration of clinical systems underpinning remote monitoring?

First, individual consent with appropriate understanding is critical. Patients must provide informed consent before data collection for remote monitoring commences. Patients should understand the purpose of data collection and the monitoring and storage of this data. Patients should also understand what data will be collected, who will be looking at this data, how often and what it is being used for. These issues may be unique to the specific patient-healthcare provider relationship. Patient understanding of remote monitoring is particularly important in PD to avoid the misunderstanding that real-time clinical review is taking place. It is important that patients are aware that remote monitoring is a tool that does not replace normal clinical process or clinical consultation, and in particular, that remote monitoring does not remove the requirement for vigilance relating to emergency situations, such as peritonitis.

In the absence of informed consent, or a surrogate decision-making process for individuals who do not have the capacity for consent, healthcare providers should consider whether remote monitoring for dialysis is appropriate.

Second, the expressed wishes of patient communities for remote monitoring can be explicitly considered in setting up remote monitoring systems. Several researchers have analyzed patient perspectives of remote monitoring and these have been recently reviewed [7]. Evidence suggests that patients are keen to receive the clinical benefits of remote monitoring, particularly to improve the quality of care received, track changes in their clinical status, and enhance their own engagement and confidence in care provision. Patients also express concerns about remote monitoring, although these were not always expressed as concerns about data privacy and security, but often related to issues of loss of interpersonal contact, general lack of trust in technology, and worry about out-of-pocket expenses. It is interesting to speculate whether patients' relatively low level of expressed concern for health data privacy in remote monitoring reflects suboptimal health literacy or high levels of trust in data security.

Ownership of Health Data

The ownership of health data is a critical but complex issue in considering the balance between access and data privacy. Clinicians should consider that ethically the patient rather than a healthcare provider or manufacturer is the original owner of his or her own data. In this context, patients must be enabled to determine the parameters for data use, storage, and dissemination of their own health information, and these issues should be discussed as part of the consent process. Most countries acknowledge the status of individuals in the ownership of their own health data.

However, health data must be recorded to be useful, and the ethical and legal status of ownership of the physical record becomes important. Historically, many jurisdictions have ruled that a healthcare provider legally owns the physical health record of a patient, usually with safeguards to protect an individual's right to access the contents of that record. Such precedents were established when health data were recorded on hard copy paper files, and the transfer and disposal of health records was simple and trackable. Distinction between *content* and *record* of health information in the digital healthcare era becomes more difficult and it is possible to imagine that provisions covering the actual record of health data may run counter to provisions for the intent of the data content. In this rapidly changing scenario, the concept of health data *custody* has been proposed as a mechanism for preserving an individual's ownership of data, whilst maintaining accountability of clinicians and healthcare organizations for data confidentiality and security. Presently, the operational requirements to implement data custodial considerations in healthcare have not been clearly articulated.

An additional issue relating to ownership of data is the balance of the rights of an individual patient versus the rights of wider communities. Some experts have advocated that all health data should be considered as a public health good [8]. In this scenario, the overall benefit to society of aggregated health data carries equal weight as an individual's right to regulate access to his or her own data. This consideration also applies to the use of individual patient data in research analyses, particularly in the context of database linkages and research data sharing. Another critical example is the consideration of data ownership for indigenous people given the right to indigenous data sovereignty in many countries. Effective governance of indigenous data requires: “(1) that indigenous people have power to determine who should be counted among them; (2) that data must reflect the interests and priorities of indigenous people; and that (3) tribal communities must not only dictate the content of data collected about them, but also have the power to determine who has access to these data” [9].

Concluding Considerations

The balance of rights to privacy and need for access to health data is fundamental to the delivery of all healthcare. This balance is particularly evident in the developing area of remote monitoring of dialysis delivery. Remote monitoring has the potential to improve patient experience and clinical outcomes, but enthusiasm for these concrete benefits should not result in failure to consider fundamental rights to privacy of individual patients. Clinicians, who may not consider themselves to be technologically adept in their personal lives, must nonetheless be aware of the principles of data privacy and security in their clinical practice. Clinicians should seek education on data privacy and security and ensure that they are up-to-date with available training.

The technological, ethical, and legal contexts of data privacy are rapidly changing and differ in different healthcare situations. Finding the best balance of clinical efficacy and patient privacy for a specific remote monitoring scenario ultimately requires individualized consideration by clinicians acting in the best interests of their patient. Understanding the patient's perspective and obtaining transparent patient consent provide the best means to achieving this balance.

References

- 1 Beauchamp T, Childress J: Principles of Biomedical Ethics (ed 7). New York, Oxford University Press, 2013.
- 2 Cohn SP: Functional Requirements Needed for the Initial Definition of a Nationwide Health Information Network. Hyattsville, National Committee on Vital and Health Statistics (US), 2006. Retrieved from <https://ncvhs.hhs.gov/wp-content/uploads/2014/05/061030lt.pdf> on 31/01/2019.
- 3 New York Times (February 5, 2015). *Millions of Anthem customers targeted in cyberattack*. New York Times. Retrieved from <https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html> on January 31, 2019.
- 4 OAIC Annual Report 2017–2018. Canberra (Australia): Office of the Australian Information Commissioner; 2018 September. Retrieved from <https://www.oaic.gov.au/resources/about-us/corporate-information/annual-reports/oaic-annual-report-201718/oaic-annual-report-2017-18.pdf> on January 31, 2019.
- 5 Information Commissioner's Annual Report and Financial Statements 2017–2018. Wilmslow (United Kingdom): Information Commissioner's Office; 2018 July. Retrieved from <https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf> on January 31, 2019.
- 6 Filkins B: Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon. North Bethesda, SANS Institute, 2014. Retrieved from <https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735> on January 31, 2019.
- 7 Walker RC, Tong A, Howard K, Palmer SC: Patient expectations and experiences of remote monitoring for chronic diseases: systematic review and thematic synthesis of qualitative studies. *Int J Med Inform* 2019, in Press.
- 8 Murdoch TB, Detsky AS: The inevitable application of big data to health care. *JAMA* 2013;309:1351–1352.
- 9 Snipp CM: What does data sovereignty imply: what does it look like; in Kukutai T, Taylor J (eds): *Indigenous Data Sovereignty*. Canberra, Australian National University Press, 2016, pp 39–56.

Dr. Peter Choi
Department of Nephrology, John Hunter Hospital
Lookout Road
New Lambton Heights, NSW 2305 (Australia)
E-Mail Peter.Choi@hnehealth.nsw.gov.au