Review Article

Legal problems faced by hospitals seeking to implement artificial-intelligence-based medical treatments in Taiwan

Shu-Lin Wang[1#], Ding-Kuo Chien[1,2,3,4,5#], Wen-Han Chang[1,2,3,4,5,6]

[1]Department of Emergency Medicine, Mackay Memorial Hospital, Taipei, Taiwan; [2]Department of Medicine, Mackay Medical College, New Taipei, Taiwan; [3]Mackay Medicine, Nursing and Management College, Taipei, Taiwan; [4]Department of Emergency, School of Medicine, College of Medicine, Taipei Medical University, Taipei, Taiwan; [5]Graduate Institute of Injury Prevention and Control, College of Public Health and Nutrition, Taipei Medical University, Taipei, Taiwan; [6]Institute of Mechatronic Engineering, National Taipei University of Technology, Taipei, Taiwan

Contributions: (I) Conception and design: WH Chang; (II) Administrative support: SL Wang, WH Chang; (III) Provision of study materials or patients: DK Chien, WH Chang; (IV) Collection and assembly of data: All authors; (V) Data analysis and interpretation: All authors; (VI) Manuscript writing: All authors; (VII) Final approval of manuscript: All authors.

[#]These authors contributed equally to this work.

Correspondence to: Wen-Han Chang. 92, Section 2, Chung-shan North Road, Taipei, Taiwan. Email: branden888@gmail.com.

Abstract: Since 1995, Taiwan's National Health Insurance (NHI) has tracked the healthcare data for Taiwan's entire population. As of July 2019, a total of 2.47 billion medical examination reports have been collected, and the amount of data is very large. To cope with these large amounts of medical expenditure data and move towards the goal of the accurate review, Taiwan's Ministry of health and welfare began to open its medical imaging database to biotechnology and healthcare firms, using artificial intelligence (AI) to help explain the patient's CT and MRI results, and take AI as a tool to review health insurance benefits. A rapid review of medical information through AI can reduce the waste of time, which is an important focus of Taiwan's health intelligence. In the implementation of medical intelligent services, many medical units often violate the law. Privacy protection is the basic human rights of patients and the core value supported by hospitals to regulate the use of personal medical information. Because intelligent medical technology and big data analysis need a lot of private information, medical departments should learn to follow relevant laws and regulations to properly implement, using patients' information legally ensures a perfect balance between privacy and medical intelligence.

Keywords: Artificial intelligence (AI); medical diagnosis; big data, health intelligence; law

Received: 29 May 2020. Accepted: 10 August 2020; Published: 30 December 2020.

doi: 10.21037/ht-20-21

View this article at: http://dx.doi.org/10.21037/ht-20-21

Introduction

Taiwan's Ministry of Health and Welfare announced plans to use artificial intelligence (AI) to assist in interpreting the results of computer tomography and magnetic resonance imaging tests for hospital outpatients from January to June 2019 (1,2). The ministry said that the time has come to develop AI as a review tool in medical diagnosis. Concurrently, the Health Insurance Department mentioned that it hopes to use AI to interpret healthcare information to reduce wasted resources, which is a widely-reported concern (3-5).

Most AI applications in medical treatments are still focused on correctly applying technology or exploring possible future uses. The recently proposed applications are, however, potentially problematic because public health insurance data is utilized to conduct research. Given the current evolution in AI usage, a large amount of personal medical data (i.e., big data) must inevitably be processed (6). In this context, those who use health data need to answer key questions. How are the data collected? Where do they come from? Do the data owners agree? These issues are

also extremely problematic for every country considering more extensive AI applications, so this topic needs to be highlighted and discussed more extensively (7,8).

Regarding AI's application to medical data analysis, most information comes from data obtained by medical personnel during routine medical treatments, such as health insurance data, medical records, or various examinations' (i.e., tests) images or data (9-12). The Personal Data Protection Act classifies this process as using information for a specific purpose. Medical experts are thus currently embroiled in a dispute over how to strike a balance between the reasonable use of personal data and the protection of data owners' privacy rights and personal autonomy (13-15).

Taiwan privacy laws

Taiwan's laws governing privacy include the maintenance of human dignity, individual expression, and the integrity of personal development. Additional basic rights involve the protection of personal living spaces from intrusion and control of personal data, which is protected by law (16-18). Individual patients can independently limit access to their private information and protect information on their decisions about whether to disclose their personal data, including to what extent, when, in which way, and to whom permission is granted. Protecting people's use of their personal data also involves preserving their right to know about and to correct this information (19-21).

Taiwan's Personal Data Protection Law clearly regulates the collection, processing, and use of personal data by medical institutions (22). Due to the sensitivity of personal medical data, unless an exception needs to be made, these data should not be collected, processed, or used. The relevant parties' consent is a standard part of studies' provisions, without which data cannot be collected or disclosed except for to serve various specific purposes and to satisfy express exceptions provided for by the law. If statistics or academic research needs protected data, the competent authorities must determine whether their use is necessary based on the public interest, and the data cannot be identified with individuals after the information is collected and processed. Thus, AI-based medical research should meet the standard criterion for whether or not the parties can be identified, applying "de-identification" as needed (23-26).

De-identification comprises making individual clients' identity unrecognizable in order to avoid any infringement on their privacy (27,28). In human body research regulations, de-identification is achieved by blocking any links to names, which ultimately requires the target population's personal data to be permanently impossible to connect to individuals and to screen on a personal level in any way (29,30). In other words, data and specimens will no longer be traceable to specific identities and have attributes connected to individuals (31). However, in AI medical research and development, de-identification is not enough to resolve the current dilemma. Regarding information autonomy, most patients are willing to contribute to medical research, but they still have many doubts about the use of routine medical data without further notice (32-34).

Various studies of this issue have concluded that medical information involves the human body, so the content is quite complicated and privacy issues cannot be easily or quickly addressed (35). Taking medical records as an example, the information available is necessary for compiling medical big or AI-generated data (36,37). If this information is de-identified, it can diminish the accuracy of medical analyses. In addition, how to de-identify data completely and cleanly is a common problem. Taiwan's current laws and regulations do not contain specific instructions on how to identify individuals in data sets. European regulations on personal data processing could thus provide a reference point for Taiwan's future identification guidelines (38-41).

From a medical perspective, requiring AI-based studies to practice de-identification may detract from the value of the data processed. However, effective ways to obtain the interested parties' consent is an issue that still needs to be addressed. In the use of medical big data, the question remains whether patients' consent should be obtained before use or whether researchers can adopt different methods of eliciting consent concurrently (42,43). Resolving the dilemma of personal data processing is an extremely important step in the development of AI or smart medical treatments. Each country tends to find different solutions to this problem, which is a significant topic to be discussed further in this article.

In terms of the systematic de-identification of personal data, the United Kingdom provides an interesting example. In 2017, after Google Deep Mind illegally accessed 1.6 million British patients' medical data, officials announced in July of that year that patients would be allowed to refuse to share their medical records. British health and social care institutions regularly refer patients to the National Medical Service System (i.e., the National Health Service), but these organizations also announced that their future patients would be withdrawn from national data sharing programs.

The relevant medical institutions must now cooperate with the complete removal of personal information, and they will no longer be able to re-identify data (44-47).

Development of medical intelligence and big data

All countries inevitably contribute to medical intelligence and big data. In this context, protecting personal data from infringements on individuals' privacy and using data rationally have become the most important goals. Based on a review of the relevant literature, this article examines smart medical information technology's impact on the future with reference to various countries' experiences. This analysis's aims are to promote the establishment of adequate laws and regulations, address patients and the public's doubts about data sharing, and eliminate unnecessary disputes about AI-based medical treatment (47).

The medical industry's global security and personal information legal practices have been actively using AI to implement innovations in recent years. As this is a new trend, the process of smart technology innovation and business and product development often have no precedents to follow, so these advances will inevitably trigger many medical disputes. If those involved can understand the relevant regulations before starting any smart product planning or medical process improvement, a clear legal compliance plan can be developed that should avoid many unnecessary problems in the future (48).

The European Union began implementing the General Data Protection Regulation (GDPR) on May 25, 2018, which provides standards for European citizens' rights regarding the collection and use of various types of personal data, including by the medical industry. The GDPR's more than 200 specifications can be roughly divided into eight principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability (49,50).

Initial determination of data collection's purpose to avoid repeated modifications

Regarding smart medical information technology applications, some countries or regions have relatively loose laws and regulations. Collecting data and developing new products create no problems involving privacy. However, if these business activities develop further so that the products are sold to Europe or other countries with strict regulations, the companies in question will have to consider the issue of personal capital and its effect on the products' promotion. When the AI-based applications' distribution becomes increasingly complicated, the original legal, business, or information processes often need to be modified, which often creates daunting challenges. Therefore, these companies must, as soon as they begin operating, incorporate privacy compliance regulations into their overall design considerations (51).

To accelerate cross-border information transmission, Taiwan's privacy laws must comply with European Union regulations so that Taiwan's medical intelligence technology industry can be globalized more smoothly in the future. An early introduction of the GDPR is not a stumbling block for innovation but rather a more solid foundation on which to base growing internationalization. With the adequate reform of global laws and regulations, this industry can expand and stabilize more quickly over time (52,53).

Precautions for hospital data collection

The GDPR has become stricter in terms of the standardization of patient consent. For example, the expected results of new biomedical product applications should be clear to rationalize patient data collection, collection methods, and machine learning algorithm records. In addition, if users have doubts, they should be able to request that the entities collecting information and developing applications delete their personal data, which is enough to show the GDPR that the AI applications have a considerable degree of control over their subjects' data (54,55).

Smart product start-up teams need to include "privacy by design" in their considerations at an early stage, and proper planning is required to save time, effort, and trouble. This process needs to follow seven basic principles: turning passive into active, presetting privacy protection, implementing privacy design, ensuring complete function, protecting security and data, maintaining visibility and transparency, respecting user privacy, and ensuring user-centricity. To ensure compliance with legal specifications, data collection must first be clear about how to use data, what data to use, and how much data is needed to avoid future information errors. Given the importance of protecting patient privacy in conformity with GDPR norms, personal privacy has to be expanded from merely regulating assets that can be disposed of by hospitals to include state of custody. Therefore, hospitals should pay attention to the need to collect only absolutely necessary information—as opposed to "the more

the better"—and, after a period of time, to destroy all data in order to avoid future problems (56,57).

Smart law compliance to save hospitals time and money and boost achievements

Under Taiwan's current laws, violations of any individual medical regulations carry a maximum fine of hundreds of millions of yuan, which may even negatively affect hospital operations. As a result, many hospitals have set up mechanisms to ensure they follow the law. Because of the increasing demand for data security and privacy protection, hospitals have also begun to acknowledge the importance of data protection.

Notably, the European Union's GDPR specifies that hospitals should carefully follow right to data portability regulations. When patients or clients ask for a referral to another medical unit, the original medical facility cannot refuse to release their medical records or hide their contents, and the information presented must also be in a format that the other party can interpret and analyze (58). This medical information transfer mechanism encourages each medical unit to focus on data integrity and security, privacy protection, quality improvement, and detailed medical records (59).

Smart medical technology regulations allow product innovations to develop rapidly while simultaneously providing more protection of personal information. If doctors do not comply with personal data maintenance guidelines and illegally collect and use patient information, such as medical conditions, the competent authorities can prohibit or order these physicians to delete the relevant information. This action can be taken in accordance with Article 25 of the Personal Information Law, and a fine of 50,000 to 500,000 yuan is stipulated in Article 47. If the intention to misuse patient information for unlawful interests is established, the maximum penalty is five years in prison in accordance with Article 41. When a personal privacy protection law is violated, the offender is punished by the central government and he or she must pay the victim, who can seek compensation in accordance with Article 29 of the Personal Protection Law and Article 184 of the Civil Law. The latter risk has had a considerable impact on doctors' behaviors in this area (60,61).

Steps to follow when using patient data

Personal information laws guarantee that patients have autonomy of information. Although doctors learn about patient information during medical treatments, they cannot use it without authorization. Patient data can only be processed further by observing the following guidelines:

(I) Public officials or academic entities needing data for research can use patient information but only after de-identification.

(II) Those who do not fall into the above categories must obtain patients' written consent in advance and only then can they use patients' information.

(III) When data is collected, patients should be notified in advance of the research's purpose, period, region, objective, method of collection, and use; patients have the right to query, supplement, correct, read, request to stop using, and delete personal data; and, finally, when patients refuse their consent, they need to know whether this will affect their rights as patients.

Personal information protection laws' impacts on the smart medical technology industry: AI and internet of things applications

When medical professionals do not understand privacy regulations, they quickly encounter problems as soon as their AI applications' development accelerate. In the process of improving smart medical technology, the Internet of Things and AI, among other tools, need to collect large amounts of data in order to analyze the innovative technology's efficacy and deal with conceptual aspects of computing processes. These operations lead to the most common violations of regulations (62-65).

For the previously mentioned reasons, users must be provided with ways to delete easily any personal identifiable information (PII) so that the next users of the instrument or application cannot access the previous users' information (66). Another approach is to provide clear information to users about how to handle these data and ensure these individuals know they have the right to stop at any time. Other methods are to confirm information flow management such as sensor capabilities and collected PII data and provide a secure information environment, including confidentiality, integrity, availability, and personal privacy. These measures can effectively reduce the data collection problems generated due to the Internet of Things or software applications (67).

Regarding AI data collection and processing—including AI-based decisions and actions—concepts such as privacy

and de-identification need to be reinforced as they have become extremely important issues. After de-identification, users must still avoid identifying personal information through iterative reasoning steps, even while searching for links. When de-identified, data are not personal information, with no obligation to involve individual patients. However, users should be especially careful that, if de-identification is only pseudonymization or abbreviation, these data are still considered personal information even after comparison and verification processes (68).

Conclusions

Privacy protection is a basic human right of patients and a core value of hospitals, so the protection of private information needs to be maintained in all future medical care. Both smart medical technology and big data- and AI-based analyses require a large volume of valuable private information. Medical units should thus follow the relevant laws and implement appropriate strategies. A judicious use of patient resources and application of smart medical technology can help maintain the perfect balance between privacy rights and medical treatments.

Acknowledgments

Funding: None.

Footnote

Conflicts of Interest: All authors have completed the ICMJE uniform disclosure form (available at http://dx.doi.org/10.21037/ht-20-21). WHC serves as an unpaid Editor-in-Chief of *Health Technology*. The authors have no other conflicts of interest to declare.

Disclaimer: Some of the materials cited in this article have not been peer-reviewed and cannot confirm their reality, nor can they replace the opinions of experts or increase their credibility. The opinions expressed in this article only represent the views of the authors and do not represent the views of government health institutions or health units. These opinions or suggestions cannot replace the medical policy.

Ethical statement: The authors are accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

References

1. Chang LC, Wang PX, Chen YY, et al. Prospect and vision of the Taiwan Ministry of Health and Welfare. J Formos Med Assoc 2013;112:505-7.
2. Serviceavdelingen informerer: omorganiseringen av Sos.dep./Helsedirektoratet Service department reports: reorganization of the Social Department/Bureau of Health. Sykepleien 1982;69:21-3.
3. Ayanore MA, Pavlova M, Kugbey N, et al. Health insurance coverage, type of payment for health insurance, and reasons for not being insured under the National Health Insurance Scheme in Ghana. Health Econ Rev 2019;9:39.
4. Rogers MJ, Penvose I, Curry EJ, et al. Medicaid Health Insurance Status Limits Patient Accessibility to Rehabilitation Services Following ACL Reconstruction Surgery. Orthop J Sports Med 2018;6:2325967118763353.
5. Frank M, Lange J, Napp M, et al. Accidental circular saw hand injuries: trauma mechanisms, injury patterns, and accident insurance. Forensic Sci Int 2010;198:74-8.
6. Auffray C, Balling R, Barroso I, et al. Making sense of big data in health research: Towards an EU action plan. Genome Med 2016;8:71.
7. Manrique de Lara A, Peláez-Ballestas I. Big data and data processing in rheumatology: bioethical perspectives. Clin Rheumatol 2020;39:1007-14.
8. Andersson N, Grinberg A, Okkels N. How personalized medical data could improve health care. Prev Med 2014;67:303-5.
9. Sege R, Preer G, Morton SJ, et al. Medical-Legal Strategies to Improve Infant Health Care: A Randomized Trial. Pediatrics 2015;136:97-106.
10. Reza Soroushmehr SM, Najarian K. Transforming big data into computational models for personalized medicine and health care. Dialogues Clin Neurosci

2016;18:339-43.
11. Fischer H, Kneifel B, Gellweiler A, et al. Personal medical data in public networks. Minim Invasive Ther Allied Technol 2002;11:41-7.
12. Thompson M. The Biographical Core of Law: Privacy, Personhood, and the Bounds of Obligation. In: Matthews D, Veitch S. editors. Law, Obligation, Community. UK: Routledge, 2018:183-216.
13. Data Protection Act--subject access to personal health information. Med Rec Health Care Inf J 1986;27:28-31.
14. Groenewegen WA, van de Putte EM. Algemene Verordening Gegevensbescherming General Data Protection Regulation and medical research: friend or foe? Ned Tijdschr Geneeskd 2018;162:D3308.
15. DoBias M. Fighting for privacy. Protect patients in rush to health IT: coalition. Mod Healthc 2006;36:14.
16. Rendina HJ, Mustanski B. Privacy, Trust, and Data Sharing in Web-Based and Mobile Research: Participant Perspectives in a Large Nationwide Sample of Men Who Have Sex With Men in the United States. J Med Internet Res 2018;20:e233.
17. Kisekka V, Giboney JS. The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. J Med Internet Res 2018;20:e107.
18. Blanquer I, Hernández V, Segrelles D, et al. Enhancing privacy and authorization control scalability in the grid through ontologies. IEEE Trans Inf Technol Biomed 2009;13:16-24.
19. Martinez C. Cracking the Code: Using Data to Combat the Opioid Crisis. J Law Med Ethics 2018;46:454-471.
20. Rippen H. e-Health Code of Ethics (May 24). J Med Internet Res 2000;2:E9.
21. Schaper E, Padwa H, Urada D, et al. Substance use disorder patient privacy and comprehensive care in integrated health care settings. Psychol Serv 2016;13:105-9.
22. Mahmoud R, Moody AR, Foster M, et al. Sharing De-identified Medical Images Electronically for Research: A Survey of Patients' Opinion Regarding Data Management. Can Assoc Radiol J 2019;70:212-8.
23. Patel VN, Kaelber DC. Using aggregated, de-identified electronic health record data for multivariate pharmacosurveillance: a case study of azathioprine. J Biomed Inform 2014;52:36-42.
24. Pesapane F, Volonté C, Codari M, et al. Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. Insights Imaging 2018;9:745-53.
25. Goodman D, Johnson CO, Bowen D, et al. A comparison of views regarding the use of de-identified data. Transl Behav Med 2018;8:113-8.
26. Snäckerström T, Johansen C. De-identified linkage of data across separate registers: a proposal for improved protection of personal information in registry-based clinical research. Ups J Med Sci 2019;124:29-32.
27. Kayaalp M. Patient Privacy in the Era of Big Data. Balkan Med J 2018;35:8-17.
28. Dernoncourt F, Lee JY, Uzuner O, et al. De-identification of patient notes with recurrent neural networks. J Am Med Inform Assoc 2017;24:596-606.
29. Prasser F, Kohlmayer F, Kuhn KA. The Importance of Context: Risk-based De-identification of Biomedical Data. Methods Inf Med 2016;55:347-55.
30. Naessens JM, Visscher SL, Peterson SM, et al. Incorporating the Last Four Digits of Social Security Numbers Substantially Improves Linking Patient Data from De-identified Hospital Claims Databases. Health Serv Res 2015;50:1339-50.
31. Phillips M, Knoppers BM. The discombobulation of de-identification. Nat Biotechnol 2016;34:1102-3.
32. Goodman D, Johnson CO, Bowen D, et al. De-identified genomic data sharing: the research participant perspective. J Community Genet 2017;8:173-81.
33. Tucker K, Branson J, Dilleen M, et al. Protecting patient privacy when sharing patient-level data from clinical trials. BMC Med Res Methodol 2016;16:77.
34. O'Neill L, Dexter F, Zhang N. The Risks to Patient Privacy from Publishing Data from Clinical Anesthesia Studies. Anesth Analg 2016;122:2017-27.
35. Kayaalp M. Modes of De-identification. AMIA Annu Symp Proc 2018;2017:1044-50.
36. Richter-Pechanski P, Riezler S, et al. De-Identification of German Medical Admission Notes. Stud Health Technol Inform 2018;253:165-9.
37. Zhao YS, Zhang KL, Ma HC, et al. Leveraging text skeleton for de-identification of electronic medical records. BMC Med Inform Decis Mak 2018;18:18.
38. Chevrier R, Foufi V, Gaudet-Blavignac C, et al. Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review. J Med Internet Res 2019;21:e13484.
39. Foufi V, Gaudet-Blavignac C, Chevrier R, et al. De-Identification of Medical Narrative Data. Stud Health Technol Inform 2017;244:23-7.
40. Xia W, Heatherly R, Ding X, et al. R-U policy frontiers

for health data de-identification. J Am Med Inform Assoc 2015;22:1029-41.
41. Plötz FB, Bekhof J. Zorgevaluatieonderzoek en de AVG The General Data Protection Regulation and clinical guidelines evaluation.. Ned Tijdschr Geneeskd 2018;162:D2915.
42. Pringle MB, Natesh BG, Konieczny KM. Patient information leaflet on mastoid surgery risks: assessment of readability and patient understanding. J Laryngol Otol 2013;127:1078-83.
43. Freer Y, McIntosh N, Teunisse S, et al. More information, less understanding: a randomized study on consent issues in neonatal research. Pediatrics 2009;123:1301-5.
44. Mavragani A, Ochoa G, Tsagarakis KP. Assessing the Methods, Tools, and Statistical Approaches in Google Trends Research: Systematic Review. J Med Internet Res 2018;20:e270.
45. Arora VS, McKee M, Stuckler D. Google Trends: Opportunities and limitations in health and health policy research. Health Policy 2019;123:338-41.
46. Ssendikaddiwa J, Lavergne R. Access to Primary Care and Internet Searches for Walk-In Clinics and Emergency Departments in Canada: Observational Study Using Google Trends and Population Health Survey Data. JMIR Public Health Surveill 2019;5:e13130.
47. Kolajo T, Daramola O, Adebiyi A. Big data stream analysis: a systematic literature review. J Big Data 2019;6:47.
48. Guérin A, Tourel J, Delage E, et al. Accidents and Incidents Related to Intravenous Drug Administration: A Pre-Post Study Following Implementation of Smart Pumps in a Teaching Hospital. Drug Saf 2015;38:729-36.
49. Chico V. The impact of the General Data Protection Regulation on health research. Br Med Bull 2018;128:109-18.
50. Sousa M, Ferreira D, Santos-Pereira C, et al. openEHR Based Systems and the General Data Protection Regulation (GDPR). Stud Health Technol Inform 2018;247:91-5.
51. Lea NC. How Will the General Data Protection Regulation Affect Healthcare? Acta Med Port 2018;31:363-5.
52. Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). Hum Genet 2018;137:575-82.
53. Shabani M, Borry P. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. Eur J Hum Genet 2018;26:149-56.
54. Rumbold JM, Pierscionek B. The Effect of the General Data Protection Regulation on Medical Research. J Med Internet Res 2017;19:e47.
55. Crutzen R, Ygram Peters GJ, Mondschein C. Why and how we should care about the General Data Protection Regulation. Psychol Health 2019;34:1347-57.
56. Spencer A, Patel S. Applying the Data Protection Act 2018 and General Data Protection Regulation principles in healthcare settings. Nurs Manag (Harrow) 2019;26:34-40.
57. Reddy S, Allan S, Coghlan S, et al. A governance model for the application of AI in health care. J Am Med Inform Assoc 2020;27:491-7.
58. Yuan B, Li J. The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. Int J Environ Res Public Health 2019;16:1070.
59. Kuntsman A, Miyake E, Martin S. Re-thinking Digital Health: Data, Appisation and the (im)possibility of 'Opting out'. Digit Health. 2019;5:2055207619880671.
60. Dailey AC. A developmental perspective on the ideal of reason in American constitutional law. J Am Psychoanal Assoc 2005;53:1175-204.
61. Judicial Yuan. Taiwan Code of Civil Procedure. Laws & Regulations Database of The Republic of China. Accessed November 28, 2018. Available online: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=B0010001
62. Protecting Yourself on Social Networks. Surveillance Self-Defense (SSD). Accessed October 19, 2019. Available online: https://ssd.eff.org/en/module/protecting-yourself-social-networks
63. Youn S. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. J Consum Aff 2009;43:389-418.
64. LaRose R, Rifon NJ. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. J Consum Aff 2007;41:127-49.
65. Cho H, LaRose R. Privacy issues in Internet surveys. Soc Sci Comput Rev 1999;17:421-34.
66. McLean I, Anderson CM. The security of patient identifiable information in doctors' homes. J Clin Forensic Med 2004;11:198-201.
67. Pron G, Ieraci L, Kaulback K, et al. Medical Advisory Secretariat, Health Quality Ontario. Internet-based device-assisted remote monitoring of cardiovascular

implantable electronic devices: an evidence-based analysis. Ont Health Technol Assess Ser 2012;12:1-86.
68. Liddy C, Dusseault JJ, Dahrouge S, et al. Telehomecare for patients with multiple chronic illnesses: Pilot study. Can Fam Physician 2008;54:58-65.

doi: 10.21037/ht-20-21
Cite this article as: Wang SL, Chien DK, Chang WH. Legal problems faced by hospitals seeking to implement artificial-intelligence-based medical treatments in Taiwan. Health Technol 2020;4:6.