

Privacy Recognition by Nurses and Necessity of Their Information Security Education

Yukari NIIMI*

School of Health Science
FUJITA HEALTH UNIVERSITY
Toyoake, JAPAN
niimi@fujita-hu.ac.jp
*Corresponding author

Katsumasa OTA

Graduate School of Medicine
NAGOYA UNIVERSITY
Nagoya, JAPAN
kota@met.nagoya-u.ac.jp

Abstract— Because of advanced computerization, the number of hospitals in which nurses use computers to collect, check, input, and record patient information has increased. The expectation for subjective and responsible behaviors by individual nurses has increased along with changes in society. Clarifying nurses' recognition and security behaviors regarding patient privacy is important for patients and medical staff. The present study revealed that hospitals follow various information security measures, but some of the nurses working in the hospitals did not recognize any concrete security-maintaining measures; 40% of responding nurses answered that the range of information sharing could be restricted within each occupational group from the viewpoint of patients' privacy rights. In addition, some of the nurses were making efforts to hide a portion of patient information in their hospitals. In other cases, patients gave nurses concrete requests. Patients' knowledge of information privacy and their attitudes toward the privacy of patients may have begun to change. Because hospitals' electronization will continue to increase in the future, comprehensive information security education is important not only for nurses but for all other medical staff.

Keywords—*electronic medical records; confidentiality; nursing education; user behavior*

I. INTRODUCTION

In recent years, the handling of medical information using information and communication technology (ICT) has advanced significantly. Hospitals introducing ICT can receive many advantages including work optimization, cost reduction, promotion of information sharing, and improvement of medical safety. On the other hand, issues accompanying information sharing using ICT have become known, including handling of patients' personal information, privacy protection, and security. Needless to say, hospitals have vast patient data. Because the data include not only names and addresses but also private information of which even patients' family members may be unaware, from clinical history to family structure, financial problems, and psychological problems, the data need to be handled carefully. Inappropriate handling of patient information by a medical institution causes more significant damage to those concerned (patients) than in other general industrial fields and may result in significant damage to the reliability of the institution.

Nurses collect information for their ordinary care of patients not only from patients but also from divergent information sources including patients' family members, other medical staff, and medical records. From among such various information sources, nurses specify, record, and store information that is required for care, collected appropriately, and utilized for care. An issue of patient privacy protection exists here. We wonder if nurses sufficiently consider patients' privacy when they collect information from patients. We also wonder if nurses consider the ways in which patients desire their private information to be handled by medical staff.

This study aimed to investigate the way education for nurses in the handling of patient information should be conducted through clarification of the behaviors of nurses and thoughts of patients concerning privacy from the viewpoint of information privacy.

II. METHODS

A. Survey Subjects

The subjects of this survey were nurses working at 515 randomly selected hospitals in which electronic medical records or ordering systems had been introduced. These comprised half of all hospitals in Tokai and Hokuriku regions in Japan.

B. Survey Methods and Details

The survey was conducted between March and April of 2009 through a mailed questionnaire. The questionnaire was composed of questions addressing topics such as attributes and status of efforts for personal information protection by hospital and nurses and requests for handling of patient information. The answers were processed using the statistical software, SPSS Statistics 17.0.

C. Ethical Considerations

Consent for cooperation in the survey was requested by clearly expressing in a letter of survey request the purpose of the survey and that the questionnaire was anonymous, cooperation was arbitrary, acceptance or denial of cooperation would cause no advantage and disadvantage, and so on. This survey was conducted with the approval of our Ethical Review Board.

III. RESULTS

A total of 21 hospitals cooperated from which 432 of 736 nurses (recovery rate: 58.7%) provided answers. Among them, 417 nurses provided valid answers (valid response rate: 96.1%).

A. Attribute of Nurses

Regarding education background, 331 nurses (79.8%) had graduated from 3-year courses at professional training colleges or junior colleges, 29 (7.0%) from 4-year universities, and 55 (13.3%) from others. Regarding years of experience as a nurse, respectively, 69 (17.0%), 130 (31.9%), 109 (26.8%), and 99 (24.3%) nurses had 3 years or shorter, 4–10 years, 11–20 years, and over 21 years. As for current position, 33 (8.0%), 74 (17.8%), and 300 (72.3%) nurses were head nurse, chief nurse, and staff nurse, respectively. The period of use of electronic systems was 2.8 ± 2.0 years, on average.

B. Status of Efforts for Personal Information Protection in Hospitals

In response to the question about users' identification and certification methods when using electronic medical records, 379 (91.3%) and 333 (80.2%) nurses answered "password" and "ID", respectively. Others included "IC card" and "fingerprint certification," though they made up less than 10%.

In response to the question about the degree of effort for security measures taken in hospitals, 20 (4.8%), 262 (63.1%, the highest), 116 (28.0%), and 4 (1.0%) nurses answered "very eagerly," "eagerly to some extent," "not so eagerly," and "no interest," respectively. In response to the question about security measures actually taken in hospitals, 241 (58.1%) answered "regular password renewal", the most frequently taken measure, followed by "screen-saver function or forced logging off as a screen-closing process when leaving one's seat" by 224 nurses (54.0%), "anti-theft measures including wire-fixing of PC" by 220 nurses (53.0%), and "access right restriction" by 182 nurses (43.9%). On the other hand, some nurses answered "no idea."

C. Status of Nurses' Efforts for Patient Information Protection

Regarding efforts by nurses themselves for the protection of patients' personal information, nurses were asked multiple-choice questions about the kinds of efforts they were making. The most common answer was "no leakage of patients' secrets to the outside (third party)", answered by 384 nurses (92.5%), followed by "shredding output worksheets after use" by 308 nurses (74.2%), "no viewing of medical records, etc. unless necessary" by 250 nurses (60.2%), and "leaving one's seat after logging out" by 210 nurses (50.6%). The contents of "others" included not leaving medical records open in the hallway and other places and following a designated method of disposal and administration of worksheets.

D. Recognition of Nurses When They Manage Patients' Information Privacy

Nurses were asked about "the concept to hide temporarily a part of or categories of patient information by pixelation according to the intention of the patient" when the patient expresses to a nurse in charge that "he/she does not want to show the screen of his/her electronic medical record that the

nurse ordinarily uses (does not want the nurse to display it in the way everybody can see it)." In response to this, 122 (29.4%), 110 (26.5%), and 176 (42.4%) nurses answered "acceptable," "unacceptable," and "no idea," respectively.

Nurses were asked to choose options about how the range of occupational group and staff allowed to view patient information in electronic medical records should be determined. The most chosen answer was "it should be set using the unit of occupational group such as doctor and nurse", selected by 199 nurses (48.0%), followed, by "all staff can view all patient information as in the past" by 98 nurses (23.6%), "it should be set depending on the degree of relationship with the patient (such as whether the nurse is in direct charge of the patient)" by 63 nurses (15.2%), and "no idea" by 52 nurses (12.5%).

There were 16 nurses (3.9%) who had actually received some requests from their patients regarding the range of information that the medical staff share. The contents of the request included "limit to staff directly involved in the patient's treatment" by 4 nurses (25.0%) and "limit to the department the patient is hospitalized," "limit to professional medical groups," and "restriction in viewing by occupational groups not related with the patient" by 3 nurses each (18.8%). Among those who had received a request from their patients, 12 nurses had taken action to meet the requests by taking measures within their reachable range including explaining the current status of the system to the patients and contacting their nursing administrator or the information system division.

E. Nurses' Opinions on Handling of Patient Information

Classification and organization of the contents of the free writing exercise by focusing on their similarities resulted in classification into seven subcategories and three categories. The categories were successfully consolidated, and their subcategories are shown by [] and < >, respectively.

[Current status of handling of patient information] is composed of two subcategories. <Efforts for patient information protection> included minimization of entry items in electronic medical records and use of a single room when collecting information. <Status leading to leakage of patient information> listed leaving the screen of a medical record open, leaving a mobile terminal, etc. in the hallway and other places, situations in which all medical staff can view information of all patients as they want, and so on.

[Improvement of privacy consciousness] is composed of three subcategories. <Thinking with the standpoint of the patient> included the fact that patients have information they do not desire to be published and their anxiety concerning the exposure of their information to everybody. <Importance of staff education> included moral education for staff and making them conscious of which information is required when collecting patient information and how the collected information should be used in nursing. <Issue of recognition of patient information> listed the issue of consciousness and ethical view of individuals.

[Necessity of information in team medicine] is composed of two subcategories. <Troubles in work caused by management of privacy> listed that viewing restrictions make sufficient care and management impossible and that it is difficult to confirm

true will concerning the privacy of patients with a problem in cognition. <Information sharing and medical safety> included indications that information sharing can secure patient safety and that no information may lead to occurrence of medical accidents.

IV. DISCUSSION

This study focused on information security related to the behavior of nurses and their recognition of patient privacy. It was revealed that many of the electronic medical records introduced in the nurses' hospitals identify and certify access rights using a set of ID and password and take an information security measure through regular password renewal. Additionally, enhancement of the certification using biometrics including fingerprint and iris was also conducted, though at a low rate. Bardram [1] reported that user identification (user name and password) is a basic theme in computer security and is particularly important in the multiuser computer environment. However, the results of the present study revealed that the hospitals of approximately 40% of the nurses who were using a password were not making efforts for password renewal. This can be said to violate the most basic principle of information security. In spite of the fact that all the choices shown in this survey are related to the efforts hospitals should make aggressively as information security measures, 13% of the nurses answered that they had no idea, indicating a lack of sufficient education and training regarding information security. On the other hand, the presence of efforts for hiding a portion of patient information according to the intention of patients demonstrated a presence of hospitals that are aggressively making efforts for the protection of personal information.

The information security behaviors of nurses revealed that compliance with duty of confidentiality also stipulated in the Act on Public Health Nurses, Midwives, and Nurses [2] and the Code of Ethical for Nurses [3] is not thorough. On the other hand, according to the guidelines [4], notification of the purpose of use in obtaining personal information from patients can be omitted if the purpose is published beforehand. In this study, it was shown that 24% of the nurses explained the purpose of use of the information when obtaining personal information. This shows that the purpose of Act on the Protection of Personal Information [5] permeates, to some extent, through the site of medical practices, which is favorable given the protection of patients' information privacy rights. In addition, the behaviors that threaten information security included leaving a computer terminal that is logged on and leaving a PC to stand. Kobayashi et al [6] reported that the reasons for leaving one's seat include being called by nurse call, difficulty logging out, and the time consuming nature of opening the screen. Nurses need to strongly become conscious that their work using PCs is a constant series of logging on and logging off, and each session does not complete without logging off (unless they log off) [7].

Opportunities in which nurses have contact with patient information have significantly increased because of spread of the hospital information system. Nurses living in an information-oriented society are required to be able to safely and efficiently use information and information equipment in the site of medical practices. Ayatollahi et al [8] mentioned that

efforts should be appropriately made concerning information confidentiality in parallel with the enhancement of accessibility to information, and users should notice the possible seriousness of confidentiality infringement. Safety management measures have three perspectives: human, physical, and technical. Among them, the human measure is generally said to be the most important and difficult. We have been educated and trained to protect patient information by learning occupational ethics for medical staff. However, the rapid spread of electronic medical records requires us to have new knowledge. There are facilities that make efforts for information security education using the e-learning system to efficiently conduct information security education for all staff [9,10]. However, it has been shown that the percentage of nurses who attend the e-learning lectures is lower than that of other occupational groups. Education is expected to be more effective if a training session is conducted after securing the time and guiding how to participate in the session instead of expecting arbitrary participation of individuals. Albarrak [11] mentioned that users' consciousness of information security issues and their training are very important in addition to bringing information security to a reliable level in health care organizations. The handling of patient information revealed that nurses recognize the importance of restricting the viewing range of patient information and staff education. We consider it necessary to keep educating and enlightening not only nurses but also other medical staff to improve their consciousness. Particularly, for the consideration of information privacy, patient information managed by medical institutions must be recognized as the property of the patients and handled carefully by taking sufficient security measures.

No certified nurse specializing in nursing information has yet been generated in Japan. Although there is a qualification called "healthcare information technologist" authorized by the Japan Association for Medical Informatics, the content of the operation is development, running, and maintenance of hospital information systems. Collection and use of information based on the self-information control right of patients are not included. While interprofessional collaboration is promoted, it will be important to prepare for the successful instruction of medical staffs by establishing a program with which certified nursing candidates specializing in nursing information in the training can acquire knowledge of and techniques for privacy and security shown in the information literacy education.

V. LIMITATION

The survey results in this study may not reflect the current status, because the survey was conducted four years after Act on the Protection of Personal Information came into full force in Japan eight years ago.

VI. CONCLUSION

Electronization and computerization of hospitals will continue to spread in the future. Most of the large-scale hospitals have introduced hospital information systems. There is no doubt that hospitals that have not introduced the system currently will introduce it at some time in the future. Therefore, we consider it important to teach health care professionals the

most essential elements, such as reasons why patient information is converted to electronic form for handling and the advantages and risks of the conversion.

ACKNOWLEDGMENT

This research was funded by a Grant-in-Aid for Scientific Research (C), Proposal No.20592485, 23593128.

REFERENCES

- [1] E. J. Bardram, "The trouble with login: on usability and computer security in ubiquitous computing," *Pers Ubiquit Comput*, vol. 9, issue 6, 2005, pp. 357-367, doi: 10.1007/s00779-005-0347-6.
- [2] Japan. Act on Public Health Nurses, Midwives, and Nurses. (1948). <http://www.japaneselawtranslation.go.jp/law/detail/?id=2075&vm=04&re=01>
- [3] Japan. Japanese Nursing Association.(2003). The Code of Ethical for nurses. <http://www.nurse.or.jp/nursing/practice/rinri/pdf/rinri.pdf> (in Japanese)
- [4] Japan. Ministry of Health, Labour and Welfare. (2004). Guidelines for proper handling of personal information in medical care/nursing care service providers. <http://www.mhlw.go.jp/houdou/2004/12/dl/h1227-6a.pdf> (in Japanese)
- [5] Japan. Act on the Protection of Personal Information. (2003). http://www.japaneselawtranslation.go.jp/law/detail_main?id=130&vm=4&re=
- [6] M. Kobayashi, I. Morikawa, T. Inagaki, S. Hosono, "Questionnaire survey about leakage of personal information for users of information system in our hospital," 26th Joint Conference on Medical Informatics, 26(Suppl.), 2006, pp. 770-771(in Japanese).
- [7] K. Yamanouchi, "Manners for the nurse in the 21st century to master information and computer equipment," *Jpn J Nurs Edu*, vol. 38, no. 5, 2013, pp. 8-15, (in Japanese).
- [8] H. Ayatollahi, P.A. Bath, and S. Goodacre, "Accessibility versus confidentiality of information in the emergency department," *Emerg Med J*, vol.26, no.12, 2009, pp. 857-860, doi: 10.1136/emj.2008.070557.
- [9] I. Sumito, T. Fukuda, H. Tanaka, K. Yamanari, T. Sakaguti, "Integrated management system education using e learning system," 26th Joint Conference on Medical Informatics, 26(Suppl.), 2006, pp. 1211-1212, (in Japanese).
- [10] H. Nakanishi, E. Nakano, "Information security education using e-learning," *J Jpn Nurs Asso Kango*, vol. 61, no. 14, 2009, pp. 70-79, (in Japanese).
- [11] A.I. Albarrak, "Information security behavior among nurses in an academic hospital," *HealthMED*, vol. 6, issue. 7, 2012, pp.2349-2354.