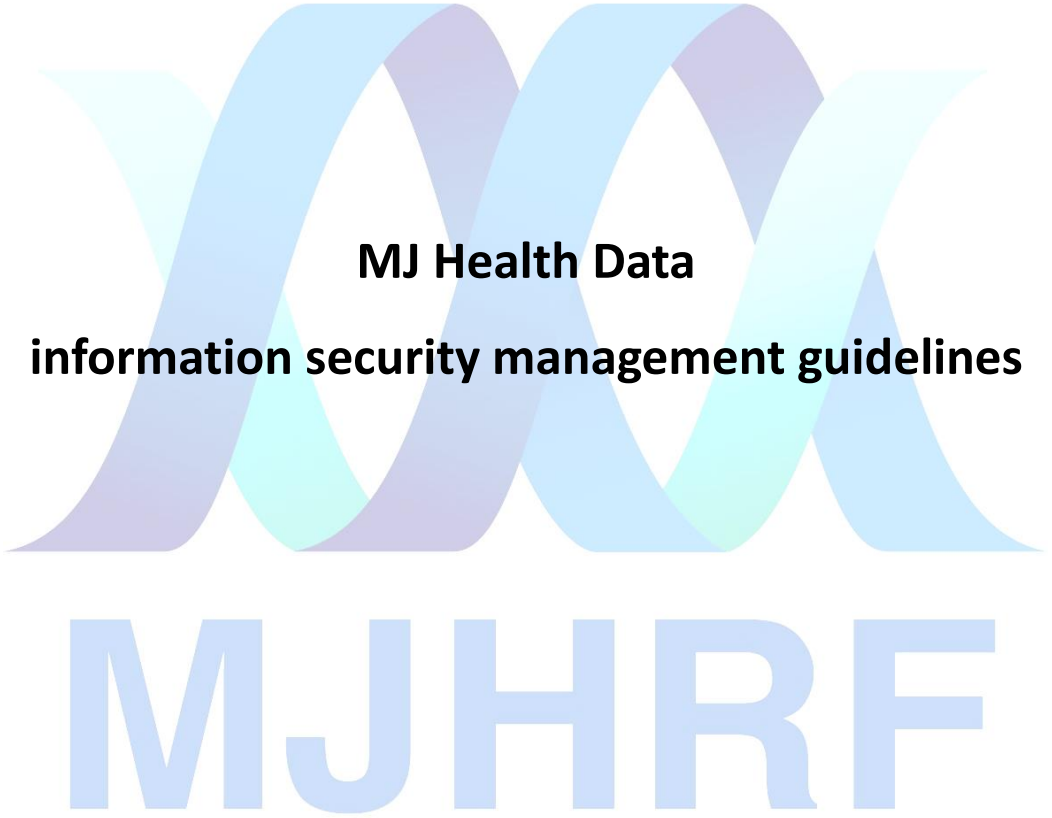
MJ Health Research Foundation

MJ Health Resource Center



MJ Health Data

information security management guidelines

Technical Report No. : MJHRF-TR-03

2016/04/12

Citation:

Yuan-Chieh Chuang, *MJ Health Data information security management guidelines*, MJ Health Research Foundation Technical Report, MJHRF-TR-03, April, 2016.

MJ Health Data information security management guidelines

I. Foreword

Due to the vast amount of personal data from participating members collected by the MJ Health Resource Center (hereafter the Resource Center), our Resource Center adheres to strict regulations regarding the protection of personal information. During the process of collecting and transporting data, we follow the Human Biological Database Information Security Specifications issued by the Ministry of Health and Welfare. Furthermore, we also refer to the Information Security Management System (ISO27001:2005) to establish systems relating to data security in order to protect personal information of participants. Such security systems are set to ensure continual operation for the Resource Center.

II. Information Security Management and Personnel Training

In order to implement an efficient information security management system, the Resource Center has established an Information Security Committee. Through the collaboration of Data Quality and Security, Biomedical Affairs, Ethics and Governance Council and Audit groups, the Resource Center aim to efficiently implement the information security policy.

To raise awareness on information security, we periodically hold workshops to educate and train our employees. These workshops aim to learn from the newest information security issues and to share the most up-to-date laws and regulations on the subject. The new employees also undergo security assessments along with signing confidentiality contracts regarding the information at hand.

III. Data Protection and Usage

We implement a physical isolation system for the storage of the personal data in the Resource Center. The data is stored in its own independent database, and is used only for identification purposes, not for research. Once the information is entered into the storage system, it will be identified only with an identification code, decreasing the risk of personal data exposure. As for information from health questionnaires and

physical examination data, they can only be provided for research purposes as de-identified data after the Ethics and Governance Council or related departments from the Resource Center have fully examined the research proposal. This is to ensure the utmost protection for the personal data of our participants.

Important data is stored and transmitted in secure methods according to the regulations. Data is transported either by reliable personnel or with the appropriate encryption after the confidentiality of the data is fully examined; this is done to prevent misplacement, blemish, forgery and tempering of data. Furthermore, backup of our data is also done periodically along with recovery simulation in case of blemished data causing irreparable damage.

IV. Management of Information Assets

The Resource Center has established a detailed list for our information assets, including the sorting of the items, owners and safety level of our assets. Also, we have established a standard for assigning information security levels and appropriate protection measures according to the The Classified National Security Information Protection Act, Personal Information Protection Act, The Freedom of Government Information Law and other related regulations. Each asset on the information asset list will undergo risk assessment based on its value, risk and weaknesses. To lower the possibility of high risk assets jeopardizing the information system, an improvement plan will be devised and periodically evaluated on its progress.

V. Computer System Safety Management

According to the regulations stated in the Computer system-related operational procedures, we are able to assure the proper functions of the information system through the information system operational documentations. Also, in order to efficiently handle information security incidents in our Resource Center, we have established proper procedures and records to handle such incidents and ensure accountability is addressed in the event such incidents occur.

As for the maintenance of our information system, the Resource Center keeps constant surveillance on the analytics system’s operating capacity to prevent our system from crashing due to overcapacity. We closely monitor the usage of system

resources, including the processor, main storage unit, file storage and others, while paying special attention to systems used for routine operations and information management. If new system is developed, it should meet the established operation standards before going online.

VI. Conclusion

With the advent of newer technology, although data acquisition has become much easier, the risk of information leak has also become much higher. Only through a constant update and adoption of information security knowledge and technology, can we provide the most reliable protection for personal information. Our Resource Center ensures that we will provide our members with the best personal information protection through establishing, planning, inspecting and implementing a robust information security system.