Short Article

Preventing Non-Authorized Access to Employee Medical Records at Worksites

Jefferelli SB,[a,*] Trauth B,[b] Abu Hasan S,[c]

[a] *Corporate Health Management, EHS Services Asia Pacific (AC/E), BASF Asia-Pacific Service Centre Sdn. Bhd., Level 25 Menara TM, Jalan Pantai Baharu, 59200 Kuala Lumpur, Malaysia.*
[b] *Corporate Health Management, BASF SE, Carl-Bosch-Strasse 38, 67056 Ludwigshafen am Rhein, Germany.*
[c] *Academy of Occupational and Environmental Medicine, Malaysia, Room No 11, 5th Floor, Bangunan MMA, 124 Jalan Pahang, 53000 Kuala Lumpur, Malaysia.*

*Corresponding author: jeff.bahrin@basf.com

Article history

Received 19/5/2021
Published : 21/12/2021

ABSTRACT : *Worksites may store medical records, and they may not be familiar with protecting medical data. An important aspect of medical data protection is the prevention of non-authorized access. Occupational health personnel are commonly responsible for this task. If they are not available, a suitable authorized person needs to be appointed. Types of medical data kept at worksites and measures required to prevent non-authorized access are described.*

Keywords - *Employee, Medical Records, Non-Authorized Access, Occupational Health, Worksites*

1.0 INTRODUCTION

It is common for worksites to store medical records of their employees to comply with local regulations or company procedures. As stated in the Department of Occupational Safety and Health, Ministry of Human Resource, Malaysia (DOSH) Guidelines on Occupational Health Services, one of the functions of Occupational Health Services would be to manage medical records (DOSH, 2005). Occupational Health (OH) personnel are usually familiar with medical data protection. However, many worksites in Malaysia do not have an on-site OH service. Therefore, an important aspect of medical data protection is the prevention of non-authorized access to medical records.

There are various types of laws or guidance on data protection. For example, in the European Union (EU), there is the General Data Protection Regulation (EU, 2016), whereas, in Malaysia, there is the Personal Data Protection Act 2010 (PDPA, 2010). The Malaysian Medical Council (MMC), which governs medical professionals in Malaysia, produced Guidelines on Confidentiality (MMC, 2011). BASF, a chemical company with approximately 110,000 employees in around 90 countries globally (BASF, 2020a), produced its guidance on medical data protection (BASF, 2020b). The BASF guidance document provides clarity to their sites globally on how to achieve the expected standards. In countries with higher national standards, the site must comply with the higher standard. We have used the BASF guidance as the main reference for this article.

This article aims to explain medical data and provide guidance on how to prevent non-authorized access to employees' medical records at worksites.

2.0 CONTENTS

2.1 What is Medical Data

Medical data is all information concerning the medical status of an individual, including medical history, physical examination findings, results of the mental status examination, medical test results, laboratory findings, diagnosis, and provision of medical health care which relates to past, present, or future physical or mental health or condition of an individual. Medical records are medical information physically recorded in any form, paper, or electronic form (e.g., medical files of patients, progress notes, consultations), also including particular media specific to the equipment or imaging study conducted (e.g., X-ray, ECG, audiometry or lung function print outs) (BASF, 2020b).

Medical records at worksites can either be generated on-site or off-site. For example, suppose a medical assessment is performed and recorded at the worksite. In that case, the document is generated on-site, whereas if the assessment is performed and recorded at an external facility, it is generated off-site. Medical records can also be stored either on-site or off-site. For example, if the medical assessment results are stored at the worksite, it is on-site, whereas if stored at an external facility, it is stored off-site.

2.2 How to Prevent Non-Authorized Access

Sites with or without OH personnel need to be familiar with medical data protection and take necessary measures to prevent non-authorized access to medical records. Given the lack of material and awareness at worksites on this subject, we share the recommendations from MMC and BASF.

2.2.1 Measures Recommended by MMC

Among the measures stated by MMC to prevent non-authorized access to medical records were enhancing physical and Information Technology security, limiting access to legitimate users, maintaining a log of access, antivirus protection, and proper hardware disposal (MMC, 2011).

2.2.2 Measures Recommended by BASF

BASF produced guidance on medical data protection to assist local management in ensuring good practices globally, including medical data protection.

2.2.2.1 Roles and Responsibilities of OH Personnel or Department

The BASF guidance emphasizes the role of OH personnel and department in medical data protection. Although not specified in the guidance document, it is understood that authorized persons would need to be appointed to this role if a site does not have OH personnel or a department. The criteria and responsibilities of authorized persons must be clearly defined. They need to be adequately trained on medical data protection and sign a written agreement to protect medical data. The guidance document does not state the necessary job level or title of the person performing this role. The manager of the OH department

is responsible for ensuring data protection (e.g., awareness, responsibilities of the supporting medical staff (physician, paramedic, nurse, assistant) signed acceptance of the data protection regulation), and regular information sessions must be held to inform and remind all members of OH department. The principles of medical data protection should be communicated to the staff members of the OH department. They should be made accessible to employees, patients (also non-employees), and clients (also non-patients).

All medical information that arises from or concerning the interaction between individual and OH personnel should be:

i. kept confidential, recorded, stored, and transmitted following the individual's rights;

ii. not visible or accessible to non-authorized persons;

iii. secured and locked away if not in use or required;

iv. labeled as "strictly confidential" when sent or transmitted;

v. transmitted by email or fax only with measures taken by the sender to assure that the intended person may only view the content: use encryption for email transmission; fax transmission, ensure that the recipient is present and can promptly remove the faxed document from the machine; and

vi. sent back to the responsible department if received by the wrong addressee.

In medical studies, annual reports, and publishing documents, personal identifiers of subjects and patients must be thoroughly obscured beyond feasible attempts at reconstruction.

2.2.2.2 OH Facilities

The OH facilities should be designed to enable adequate medical data protection (e.g., separate treatment and consultation room).

2.2.2.3 OH Service Provision by External Provider

If an external provider provides OH services, equivalent data protection measures should be defined in the contractual agreements between the provider and the company. Generally, medical records generated by external OH providers for company purposes and at company premises are the company's property. They must be provided upon request to an authorized company physician or an appointed person of the OH department. Procedures should be in place that explicitly states which data is collected, who will access it, and how to handle the information.

2.2.2.4 Protection of Medical Records Against Disclosure

Medical records are protected against disclosure without the explicit consent of the concerned patient or client or some other overriding legal reason justifying disclosure. In the first instance, the patient or client should be informed about the medical information disclosed to obtain his explicit consent. In addition, attention should be paid when confidential information needs to be disclosed on extraordinary grounds without explicit consent (e.g., a requirement by law, public interest, orprevention of a serious crime). In all these situations and disclosing confidential data, the applicable laws and regulations must be observed.

2.2.2.5 Storage of Medical Data

Suppose storage of medical files on-site is mandatory according to legal requirements even without an internal OH department, and access for-authorities needs to be guaranteed at all times. In that case, there has to be a clear written procedure on how this access is managed and misuse is prevented. Proper measures should be reducing the number of person with an access to medical files; number of persons with access to medical files reduced to a minimum; persons with access must sign the confidential statement; storage must be-sealed, broken seal needs to be documented; four-eye-principle should be implemented; breach of confidentiality must be documented and reported. Medical records in all forms must always be stored securely and separately from the other personnel information. The head of the OH department should determine the media and the location for the storage of the medical records. The head of the OH department must authorize the destruction of medical records; the usual terms and conditions of data destruction apply (BASF, 2020b).

3.0 CONCLUSION

Various measures can be taken to ensure non-authorized access to employee medical records. Elements that need to be considered include the roles and responsibilities of OH personnel or department; OH facilities; OH service provision by an external provider; protection of medical records against disclosure; and storage of medical data. Those responsible for the medical records, i.e., OH personnel or authorized persons, need to be familiar with these measures.

REFERENCES

BASF (2020a). BASF Report 2020.

BASF (2020b). Medical Data Protection, G-GD-OCH 010

Department of Occupational Safety and Health (DOSH) (2005).

European Union (EU) (2016). Regulation EU 2016/679 (General Data Protection Regulation).

Guidelines on Occupational Health Services.

Malaysian Medical Council (MMC) (2011). Guidelines on Confidentiality.

Personal Data Protection Act (2010).