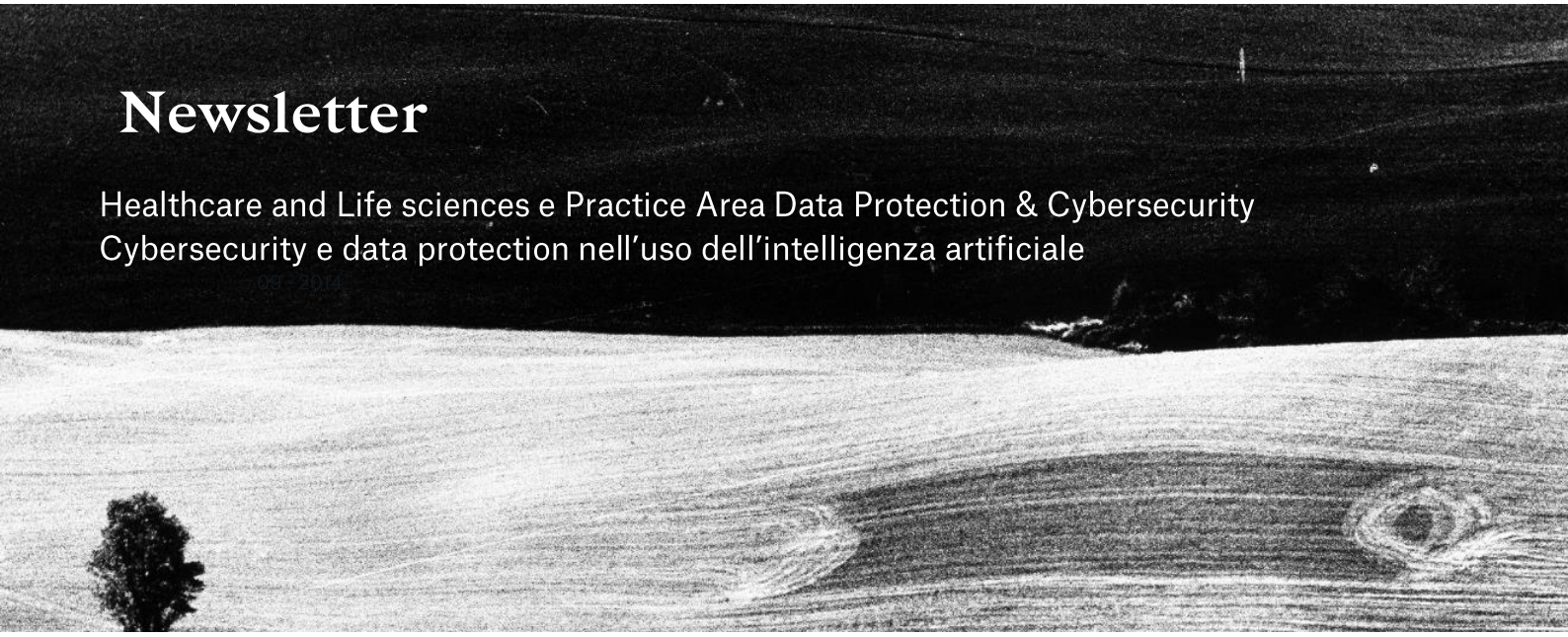
CHIOMENTI



Newsletter

Healthcare and Life sciences e Practice Area Data Protection & Cybersecurity
Cybersecurity e data protection nell'uso dell'intelligenza artificiale

Introduction

Artificial Intelligence (AI) is often employed to support processes and activities carried out by professionals and private and public entities operating in different sectors. However, its use does not come without risks, as it is often employed with little awareness and without adequate safety measures.

Considering the above, ENISA – the European Union Agency for Cybersecurity that aims at increasing the level of cybersecurity across the European Union – classified the artificial intelligence abuse among the emerging cybersecurity threats in the horizon of 2030.

For these reasons, ENISA has recently published the paper "Cybersecurity and privacy in AI – Medical Imaging diagnosis", that identifies the main security and privacy threats arising from the use of artificial intelligence. Moreover, the mentioned paper points out some controls that helps in mitigating the risks identified.

How to mitigate the risks arising from AI?

Among the main measures that shall be implemented in order to mitigate the risks arising from the use of artificial intelligence there are the following:

(i) Implement a security by design process

Implementing a security by design process means **strengthening the cybersecurity of the organization**, also by automating security controls and developing a robust AI

infrastructure. The goal is to ensure that the risks are mitigated before systems go live and appropriate security controls are implemented.

This helps in **increasing the overall level of cybersecurity and resilience** also by including it in **corporate governance processes**. This allows for greater asset protection and less business impact in the event of a cyber incident. In fact, the lack of security by design increases the likelihood of verification of the threats identified. This means that the medical practice shall ensure, from the development phase, adequate controls to limit the cybersecurity risks. To this aim an overall risk analysis may be helpful to identify all risks associated with assets identified. Following the risk analysis, the medical practice may try to reduce the "attack surface" (*i.e.*, the extent of exposed and potentially vulnerable services), for example by auditing its providers o a regular basis.

Moreover, adopting a security by design principle from the very early stages of a project requires **less effort** than adding security controls on top of existing one.

(ii) Ensure compliance with authentication, and access control policies

It is necessary to **draft an authentication policy** based on the current recommendations of public bodies such as ENISA and NIST.

Moreover, it fundamental to assess the **proper user authentication and access controls** on every device.

In addition, it is important to highlight that such authentication systems collect personal data concerning employees. Therefore, it is necessary to carry out a **data protection impact assessment**.

(iii) Data Protection Impact Assessment

This measure allows for an **in-depth analysis of the impact** of the processing on the privacy of users and to identify whether the associated risks are well addressed. It also helps to ensure that the purpose of the processing is well defined and that the actual use of the data remains within the scope.

The control under analysis may impact on the overall scenario of the processing carried out, because it may lead to a redefinition of the entire framework.

(iv) Identify data processors and perform control actions on their compliance

Where an artificial intelligence is used, data are manipulated and stored in resources provided by a cloud provider. Therefore, it is important that the medical practice controls the cloud provider, its actions and its compliance with data protection legislation and cybersecurity best practices.

To this aim it is important to **draft an audit plan and to identify their frequency**, also on the basis of a risk analysis.

(v) Call on ethical committee and external audits

The lack of review of processing by a specialised equity committee can lead to **unfair treatment**. The medical practice can find a solution by drafting a **Code of Ethics** and employing an **ethics committee and external auditors**.

Therefore, the medical practice must involve **independent entities** to review the inputs and outputs of the processing of data to determine whether the processing is unfair.

(vi) Pseudonymise data coming from patients

The medical practice may need a help in **identifying the best practices** to ensure a strong pseudonymisation of the data, replacing it with random IDs, and keeping the correspondence between these removed attributes and their IDs in a dedicated data base.

A different database could be used to store the correspondence composed of identification data.

(vii) Assessment of the severity of the impacts

For each impact and associated threats it is important to understand and classify the severity from both a data protection and a security standpoint.

The classification of the severity may help in defining a recovery plan and in understanding the main criticalities in order to implement appropriate safeguards.

Contatti

Luca Liistro
Partner – Head PA Healthcare & Life Sciences
T. +39 02 72157 322
luca.liistro@chiomenti.net

Pierluigi Perri
Of counsel – PA Data Protection & Cybersecurity
T. +39 02 7215 71
pierluigi.perri@chiomenti.net

Lucrezia Falciai
Associate – PA Data Protection & Cybersecurity
T. +39 02 7215 71
lucrezia.falciai@chiomenti.net