

## About The Author



**Matteo Colombo** is the Founder and President of Association of Data Protection Officer - ASSO DPO. He has a degree in Law at the University of Milan and in Political Science - Privacy Specialist - Data Protection Officer at Popular University of Milan. Colombo is a business consultant and trainer, expert in the field of privacy and labor law. After a few years of experience in a multinational company, leader in employment agencies sector, as Risk Manager and as a member of legal department, he became the founding member and CEO of Labor Project Srl, a company that for more than a decade has been working in the field of privacy compliance company liability. As Head of the consultants' team, he has been following, in these years, private companies and public administrations in the performance of Personal Data Protection Code. He is also an expert in corporate crimes and member of 'Compliance Committee'. Speaker at several events throughout Italy on topics Privacy and 231 and creator of E-Learning project 'Master DPO. Colombo is: the founder of LinkedIn group 'ASSO DPO Chief Privacy Officer Group', Privacy Consultant and Privacy Officer at TÜV Italia srl - TÜV SÜD Group according to the guidelines ISO/IEC 17024:2008, Data Protection Officer at Veritas Italia SpA - according to the guidelines ISO/IEC 17024:2008, and CIPP/E qualified.

E-mail: [matteo.colombo@laborproject.it](mailto:matteo.colombo@laborproject.it)

## Italy - Electronic Patient Dossier

Matteo Colombo

27 July 2015

### 1. Introduction

The Italian data protection authority (Garante) published, on 4 June 2015, new Guidelines on the Electronic Patient Dossier (EPD) aiming at providing a unified reference framework to ensure the correct treatment of all data included in the dossiers that private and public health care facilities have already established or will establish in the future.

### 2. What is the electronic patient dossier?

The electronic patient dossier is an instrument set up in each health care facility (hospitals, health authorities, health care centres, nursing homes), which is considered as the data controller and which collects information on the health of a patient, to record his or her medical history within that specific facility and to provide better care.

### 3. What are the risks that need to be evaluated?

There are many risks that the health care facilities in their role as data controllers, when set up the EPD, shall evaluate. In particular, when they have to choose the security measures to apply, an evaluation of the risks is necessary.

The main risks to which the personal data collected and processed by the data controller are exposed, when the EPD is being used by the data controller, are: data hacking, theft or loss - in whole or in part - of storage media or computer processing systems (whether fixed or portable), and unauthorised communication of these data. In addition to the above-mentioned risks, there is also the need to ensure legal certainty of the processed data, their accuracy, integrity, unchangeability, and availability; with regard to such issues, in addition to data protection, we must also take into account aspects related to professional responsibility and ethical conduct.