

Compliance Today – June 2023



Patrick Wellens (patrickwellens@hotmail.com) is currently a Compliance Manager for a division of a multinational pharma company based in Zurich, Switzerland. He is a Board Member of Ethics and Compliance Switzerland and co-chair of the working group “life sciences.” Patrick is also an Executive Committee member of the Association of Corporate Investigators.

Is your sensitive data disposed of in a compliant way?

by Patrick Wellens, CCEP-I, CIA, CFE, CRMA, MBA

In Zurich, Switzerland, between at least 2008 and 2012, the Security Department disposed old laptops that still had very sensitive information (i.e., telephone lists of police agents, planning documents from police, psychiatric reports/assessments of inmates, personal evaluations from public prosecutors, etc.).^[1] When the government found out in 2020 about this leakage, they reported the incident to public prosecutors and cantonal data privacy authorities. The investigation is currently ongoing.

In Queensland, Australia, many medical records, transported from the hospital to a facility where such medical records would be destroyed, fell from a truck, and were then found on a busy road.^[2]

In the United Kingdom, the National Health Services (NHS) Surrey provided computers to a destruction company without checking whether any medical information on them had been securely deleted.^[3] One of the computers contained the health records of 2,000 children and 900 adults, plus NHS human resources records. Another 39 computers sold by a data destruction company were recovered during the investigation, with sensitive records found on three of the hard drives.

These examples show that if laptops or sensitive information are not properly destroyed, this might have severe consequences. First, the company is violating data privacy laws and might incur a substantial fine from the data privacy authorities. Second, the company would have to inform those individuals affected by the data loss/breach of personal data or medical records, which creates a huge reputational loss. Third, the company that showed negligence in properly disposing of sensitive information or personal data might have to pay compensation claims to affected individuals. Finally, the company might have breached official secrecy laws.

In this article, we will explore some best practices concerning the disposal of sensitive and/or personal data.

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member](#) [Login](#)