COSMOS
Navigate the Compliance Universe

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.

Sensitive information and personal data

In healthcare organizations, medical personnel (general practitioners, specialists, nurses, surgeons, clinic directors, etc.) might have access to electronic patient records, laboratory results, pictures (x-rays, brain scans, mammography tests, MRIs), communication between patients and medical personnel, summary reports with diagnosis, treatment plans, patient insurance details, consent forms, etc.

In addition to personal data, laptops can also contain secret or restricted information such as personnel records, payroll information, personnel evaluations, strategic plans, company financials, etc.

Healthcare professionals might have some of the previously mentioned records stored on laptops, so prior to the disposal of laptops, healthcare organizations should take extra care to ensure that all sensitive and personal data has been erased.

Best practices principles for disposal of media

The National Institute for Standards and Technology (NIST) has defined a Guidelines for Media Sanitization (NIST SP 800-80), a set of best practices for effectively "sanitizing" storage devices and electronic media.[4]

Media typically consist of hard copy media (paper printouts) and electronic media—i.e., devices containing bits and bytes such as hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices, and office equipment.

NIST standard defines the following best practices:

1. Media sanitization needs and media types should be identified before reaching the disposal phase in the IT asset management lifecycle. The type of storage media is a fundamental factor in determining the proper data destruction method and the overall sanitization duration.

2. IT asset(s) should be disposed of via a process flow using appropriate roles and responsibilities, and the organization must maintain different levels of security based on the data confidentiality level. Further, it recommends maintaining a mapping of the type of data, based on its confidentiality level, stored on the devices to facilitate effective and efficient media sanitization.

3. Before any media is sanitized, system owners are strongly advised to consult designated officials with privacy responsibilities (data privacy officer) and/or the local records retention office.

4. Maintain a documented certification for every unit of sanitized electronic media, particularly those containing sensitive and confidential data. Per NIST media sanitization guidelines, the certificate should include hardware and process details such as manufacturer, model, serial number, media type, source, sanitization method, the tool used and version, verification details, etc.

5. Many types of media containing data will be transferred outside the organization's control throughout an information system's life. This activity may be for maintenance reasons, system upgrades, or during a configuration update. The organization should consider the "chain of custody" risks and wipe the storage device before handing it over to a third party.

Sanitization methods

Commonly used media sanitization methods are data erasure (overwriting the media with zeroes and ones to destroy the available data), degaussing (elimination of the magnetic field from the storage device, thus rendering the data available on these devices unrecoverable), cryptographic erase (performed by sanitizing the cryptographic keys used to encrypt the data, as opposed to sanitizing the storage locations on media containing the encrypted data itself), shredding, data deletion, reformatting, and physical destruction. As magnetic media evolves, some of the previously mentioned techniques are no longer effective.

The NIST guidelines, therefore, created three different types of sanitizations.

- **Clear** – applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, noninvasive data recovery techniques; typically applied through the standard "read" and "write" commands to the storage device, such as by rewriting with a new value or using a menu option to

reset the device to the factory state (where rewriting is not supported).

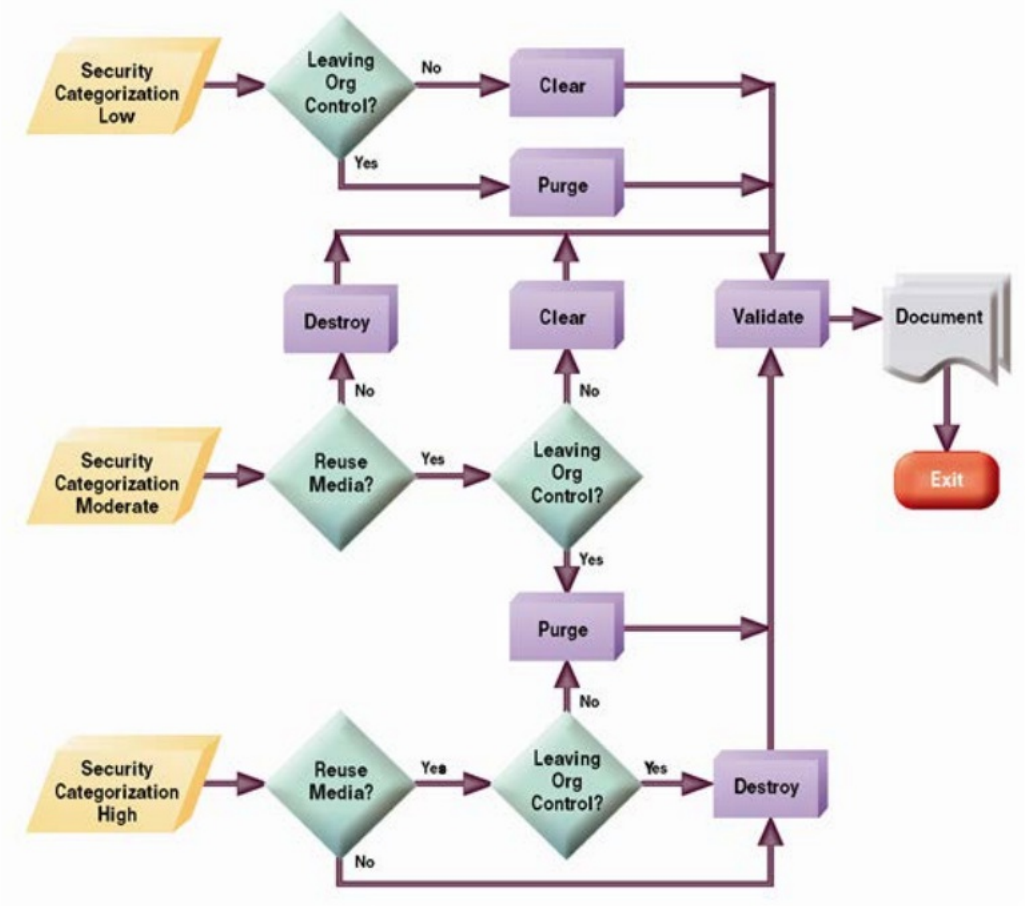
- **Purge** – uses physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques.
- **Destroy** – renders target data recovery infeasible using state-of-the-art laboratory techniques, resulting in the inability to use the media to store data.

The form of sanitization depends on:

- What types (e.g., optical non-rewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the confidentiality requirement for the data stored on the media?
- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media?
- What is the availability of sanitization equipment and tools?
- What is the level of training of personnel with sanitization equipment/tools?

The NIST standard has been defined in Figure 1.

Figure 1: Sanitization and Disposition Decision Flow[5]



Data privacy requirements

According to HIPAA, companies "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure."[6] This standard would of course also apply to disposal of laptops that contain personal data.

And according to General Data Protection Regulation (GDPR) Article 32 – Security of processing: "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."[7]

Conclusion

There are 2.5 quintillion bytes of data created each day.[8] Sensitive business and personal data is proliferated over a wide variety of media (paper, electronic devices, hard drives, RAM, ROM, disks, flash memory, memory devices, phones, mobile computing devices, networking devices, office equipment). Companies must proactively consider the disposal phase in IT asset management lifecycle to minimize reputational loss and prevent GDPR and/or HIPAA from failing to prevent unauthorized access, disclosure, or data loss.

Takeaways

- Laptops and other storage devices might contain sensitive data or medical records. Therefore, extra attention should be taken when disposing of such electronic devices, ideally following the NIST SP 800-80

Guidelines for sanitizing devices.

- An organization must maintain different levels of security based on the data confidentiality level. It is recommended to have a mapping of data, based on its confidentiality level, stored on devices to facilitate effective media sanitization.
- Before media (laptops, devices, tablets, etc.) is sanitized, system owners are advised to consult with a data privacy officer.
- The organization should consider "clear," "purge," or "destroy" sanitization techniques based on security categorization, whether the media (laptop, devices, etc.) will be leaving the organization and/or whether it will be reused.
- Companies must proactively consider the disposal phase in IT asset management lifecycle to minimize reputational loss.

1 Livingstone, "Data Leak Zurich Reached the Federal Palace," *24Instant News.com*, December 2, 2022, https://24instantnews.com/politics/29794.html. https://switzerlandtimes.ch/politics/zurich-data-leak-reaches-the-federal-palace/
2 "Medical records found on Brisbane road," *Sky New Australia*, accessed March 29, 2023, YouTube video, 1:16, https://www.youtube.com/watch?v=9vZ7Jjii0Ks.
3 "NHS Surrey fined £200,000 after losing patients' records," *BBC News*, July 12, 2013, https://www.bbc.com/news/technology-23286231.
4 Richard Kissel et al., *Guidelines for Media Sanitization*, NIST Special Publication 800–88, Revision 1, December 2014, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.
5 Richard Kissel et al., Figure 4–1: Sanitization and Disposition Decision Flow, 17.
6 45 C.F.R. § 164.530(c)(2).
7 Article 32 GDPR. Security of processing, GDPR Text, accessed April 11, 2023, https://gdpr-text.com/read/article-32/.
8 Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=3137eb1460ba.