Is Your Data Destruction Process Compliant?

TechR2's newly patented Tear-A-Byte® solution is not just data eradication of hard drives but a cradle to grave tracking method that is compliant to current US and world data security regulations for tracking, containing and destroying Data Bearing Devices (DBDs) inside the datacenter and enterprise. Most other data eradication methods do not meet the data security requirements.

What is not in compliance?

1.	Current methods where hard drives are thrown into a bin and not tracked	• **FFIEC II.C.5** Inventory and Classification of Assets Management should inventory and classify assets, including hardware, software, information, and connections. • **PCI 4.10** Destruction and Audit Procedures a) All waste components must be counted before being destroyed in-house and under dual control. A record of destruction by reel number and item count must be maintained for 24 months. • **HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)** Administrative Safeguard – Security Management Process (Risk Management functions) Physical Safeguard – Facility Access Controls Physical Safeguard – Device and Media Controls - Physical access to assets is managed and protected • **GDPR article 78** 'detailed logs of the processing of personal data, its movement and storage' • **NIST SP 800-88 R1 Section 4.8** Documentation of the Data Eradication Process
2.	Missing multiple layers of data security	• **U.S. Patented** Tear-A-Byte Data Eradication Method with 4 layers of security • **NIST SP 800-88 R1 Section 4.7 –** Minimal of two layers of security with verification
3.	Management oversight not present	• **FFIEC II.C.11** – End-of-Life Management Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. Maintaining inventories of systems and applications • **HIPAA Security Rule 45 C.F.R. §§ 164.306(a)** – Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with • **NIST SP 800-88 R1 Section 3** Roles and Responsibilities
4.	EOL Risk Assessment missing	• **FFIEC II.A** Risk Identification • **PCI DSS Requirement 12.1.2** Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. • **HIPAA Security Rule 45 CRF 164.308(a)(1)(ii)(D)** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. • **NIST SP 800-88 R1 Section 4**
5.	Loss of data ownership – offsite eradication	• **PCI 4.10** Destruction and Audit Procedures a) All waste components must be counted before being destroyed in-house and under dual control. A record of destruction by reel number and item count must be maintained for 24 months. • **NIST SP 800-88 R1 Section 4.4** Control of Media • **HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)** - Policy and regulations regarding the physical operating environment for organizational assets are met
6.	Organization not information security authorized to touch or wipe DBDs	• **ISO 27001** certified for Information Security • **ISO 9001** certified for QMS • **FFIEC / GLBA Security Requirement** - SOC 2 compliant
7.	Recycling is not compliant to ISO 14001 standards	• **ISO 14001** Certified • Third party affiliate is not ISO 14001 certified
8.	Training of personnel interacting with DBDs not present	• **FFIEC II.C.7(e)** – Training Training ensures personnel have the necessary knowledge and skills to perform their job functions. • **NIST SP 800-88 R1 Section 4.7.2** Verification of Personnel Competencies • **HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5) -** Security awareness and training
9.	Regulatory compliance	• **GDPR, HIPAA, FFIEC, NIST, PCI, NERC**
10.	Technology and tracking system is not current	• **NIST SP 800-88 R1 Section 4.8** Documentation of the Data Eradication Process • **GDPR article 84 and 94** • **PCI DSS 12.6**