TeraSci – HIPAA & GDPR Compliance

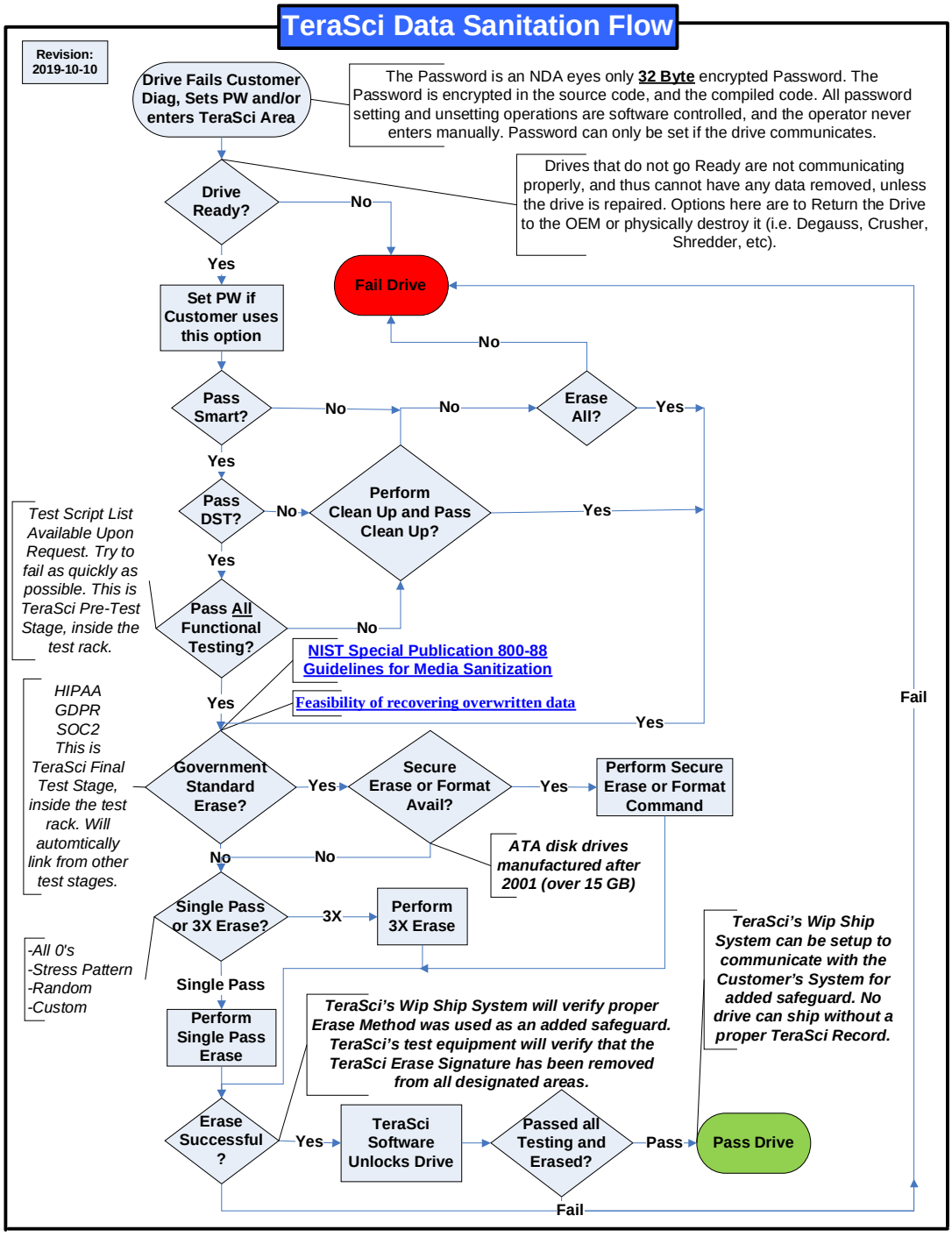
James Meece & Al Donnelly

1.) Purpose
   a. The purpose of this document is to explain TeraSci's role in HIPAA and GDPR compliance, in terms of erasing and handling of drives returned to our partners that may contain customer data.
2.) Scope
   a. The scope of this document is anyone currently using TeraSci equipment, or thinking about using it, to process drives.
3.) Definitions
   a. HIPAA - Health Insurance Portability and Accountability Act. This act is United States legislation that provides data privacy and security provisions for safeguarding medical information.
   b. GDPR – General Data Production Regulation. The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).
   c. NIST - National Institute of Standards and Technology. NIST 800-88, published by the National Institute for Standards and Technology, is known for its media sanitization categories of Clear, Purge and Destroy. Its principles can apply to magnetic, flash-based, and other storage technologies.
   d. SE – Secure Erase
   e. LBA – Logical Block Address
   f. NPI – New Product Introduction
   g. RTV – Return To Vendor
   h. RMA – Return Material Authorization
   i. OEM – Original Equipment Manufacture
   j. HDD – Hard Disk Drive
   k. SSD – Solid State Disk
   l. ATA – Advanced Technology Attachment
   m. NVME – Non-Volatile Memory Express
   n. SCSI – Small Computer Systems Interface
   o. SAS – Serial Attached SCSI
   p. FC – Fiber Channel

4.) References

a. https://www.hhs.gov/hipaa/index.html
b. https://eugdpr.org/
c. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
d. https://en.wikipedia.org/wiki/Data_remanence#Feasibility_of_recovering_overwritten_data

5.) Flowchart


TeraSci Data Sanitation Flow
Revision: 2019-10-10
Drive Fails Customer Diag, Sets PW and/or enters TeraSci Area
The Password is an NDA eyes only 32 Byte encrypted Password. The Password is encrypted in the source code, and the compiled code. All password setting and unsetting operations are software controlled, and the operator never enters manually. Password can only be set if the drive communicates.
Drive Ready?
No
Drives that do not go Ready are not communicating properly, and thus cannot have any data removed, unless the drive is repaired. Options here are to Return the Drive to the OEM or physically destroy it (i.e. Degauss, Crusher, Shredder, etc).
Yes
Fail Drive
Set PW if Customer uses this option
No
Pass Smart?
No
No
Erase All?
Yes
Yes
Pass DST?
No
Perform Clean Up and Pass Clean Up?
Yes
Test Script List Available Upon Request. Try to fail as quickly as possible. This is TeraSci Pre-Test Stage, inside the test rack.
Yes
Pass All Functional Testing?
No
NIST Special Publication 800-88 Guidelines for Media Sanitization
Feasibility of recovering overwritten data
Yes
Yes
Fail
HIPAA GDPR SOC2 This is TeraSci Final Test Stage, inside the test rack. Will automtically link from other test stages.
Government Standard Erase?
Yes
Secure Erase or Format Avail?
Yes
Perform Secure Erase or Format Command
No
No
ATA disk drives manufactured after 2001 (over 15 GB)
Single Pass or 3X Erase?
3X
Perform 3X Erase
-All 0's
-Stress Pattern
-Random
-Custom
Single Pass
Perform Single Pass Erase
TeraSci's Wip Ship System will verify proper Erase Method was used as an added safeguard. TeraSci's test equipment will verify that the TeraSci Erase Signature has been removed from all designated areas.
TeraSci's Wip Ship System can be setup to communicate with the Customer's System for added safeguard. No drive can ship without a proper TeraSci Record.
Erase Successful ?
Yes
TeraSci Software Unlocks Drive
Passed all Testing and Erased?
Pass
Pass Drive
Fail

6.) TeraSci Data Sanitation

a. TeraSci test software is fully compliant with all HIPAA and GDPR requirements. But to be fully compliant with all HIPAA and GDPR requirements your service providers must do additional steps.
b. First as to the TeraSci software, HIPAA and GDPR require that all HDD and SSD use an approved erase process. We use Secure Erase (SE) with ATA drives and the Format command with NVMe / SAS / FC / SCSI drives. These commands meet the HIPAA and GDPR standards (it is what they recommend). To insure that an individual drive properly executed the SE or Format command we have added additional code that writes a test pattern throughout the drive and after the command completes we verify that the test pattern we wrote has been erased. Before we stipulate that a drive has been erased we make sure that it "Passed" the SE or Format command and additionally we verify that the test patterns we wrote are erased.
c. There is an additional check that is TeraSci specific. We have worked with some of our customer's legal departments and there we agreed that the definition of an "Erased Drive" is that the drive will have all accessible LBA's written with all zero's. This is the same condition that a drive is delivered from the drive manufacturer. We bring this up because some Intel NVMe drives do not meet this requirement (all zero's) after the format command. So we have added a full write pass to the Intel Erase Process, for drives with this issue, to make sure all LBA's are set to zero. We have gone to great lengths to insure that there cannot be a data escape with our software, and that there is only a single definition of a HIPAA / GDPR compliant erased drive (this is a step further than HIPAA / GDPR specifies). HIPAA / GDPR allows the NVME drive to discard the "KEYS" and still be compliant. But this leaves the drive in an indeterminate state, and we decided that "legally" we want to always leave all drives in a single determinate state where all accessible LBA's are written to all zero's.
d. Additionally, we have an "audit trail" incorporated into our software. Every drive that enters the TeraSci Process is logged into our database by serial number. As soon as the drive enters

our process the erase flag in the database is set to N (NO it is not erased). Only after the drive completes the full test process and passed the erase step is the Erase Flag changed to indicate it passed the erase process. At the last point in the test process (our WIP Ship step) we check the Erase Flag and only drives that passed our process and with a proper Erase Flag will indicate a HIPAA / GDPR compliant erase and can then be routed to good material.

e. At this point out database has the capability to send a record to your customer shop floor control systems to indicate the state of an individual drive (Pass or Fail). We call this the "Link". The Link is an important step in being 100% accurate in the disposition of all drives. Manually transferring the test data and Pass / Fail indicators is full of uncertainty (e.g. operators make mistakes).
f. We will pause here to make an important statement. All of TeraSci's customers (Lenovo, HP, Dell, Cisco, Toshiba, Best Buy …) are very concerned about HIPAA / GDPR compliance and data escapes in general. This has been a serious subject for over 10 years in the industry. As we explained above we have had strict controls on data erasure for all of this time (and even further back). We have been audited many, many times over the years. Some of our customers do a full compliance check for every NPI, which includes an independent audit check for full erase. Because we always leave the drives that pass our process in a single determinate state we can be audited. We have never failed an audit, and we have been audited innumerable times. When all of our controls are fully implemented (that includes the Link) we have never had a documented data escape in the last 15 plus years. That is a span where we have tested over 25 million drives.
g. The next point in HIPAA / GDPR compliance is determined by your service providers, not by TeraSci. We have (or can) electronically updated their shop floor control systems to indicate the state of an individual drive (Pass or Fail). They must then insure that only drives with a TeraSci Pass record can be shipped out to the field as a replacement drive, or re-used in a repair operation.

h. But HIPAA / GDPR compliance is much more than erasing drives. Many drives cannot be erased, some because they did not go Ready, some because they are fails that won't write correctly and others for more obscure reasons. There can also be routing issues where some drives are not routed to the TeraSci test process, for various reasons and these drives must be treated as fails.

i. So ALL fails must be properly handled to be fully HIPAA / GDPR complaint. If a fail is "In Warranty" it can be sent back to the OEM and then the data on the drive becomes their problem. If a drive is "Out Of Warranty" it must be destroyed in a manner that makes extracting data from the drive impossible. Normally HDD's are degaussed and SSD's are shredded. But in effect all drives must have an audit trail to show the proper disposition. We provide an audit trail for the Passes that are sent back to the field as replacement drives. We also provide the start of the audit trail for most of the Fails. Your Service providers must show the final disposition for the fails be it RTV or destruction, and have a complete documented audit trail.

j. Feel free to contact us with any questions or concerns, via email at: engineering@terasci.com