Manual Removal of Data

If applicable, a manual process is to be in place to remove, at least on a periodic basis, stored data that exceeds business retention requirements or, alternatively, requirements for a review conducted at least on a quarterly basis to verify that stored data does not exceed business retention requirements. The manual process is as follows: [If used, describe your manual removal process. You can also describe the process in the tables below]

Data Retention Matrix

Type of Data	Format	Location	Retention Period	Disposal Process
Personally Identifiable Information (PII)	Electronic Records only.	PII is stored in column level encryption in various databases.	7 Years	Script is run to purge database and eventually hard drive is physically destroyed.
Credit Card Information	Both hard copy and electronic format.	Credit card information is stored in file cabinets from old invoices and also in column level encryption in various databases.	90 days	Script is run to purge database and eventually hard drive is physically destroyed. Old invoices are shred.
Protected Health Information (PHI)	Both hard copy and electronic format	PHI information is stored in file cabinets from old invoices and also in column level encryption in various databases	7 years	Script is run to purge database and eventually hard drive is physically destroyed.
?	?	?	?	?
?	?	?	?	?

Data Retention Matrix for [Enter information for a specific type of data and/or record relevant to your industry if you need a matrix that is more descriptive and detailed than the above item. Examples shown in RED below]

Description of Data/Record	ABC company is a provider of medical billing services, thus we keep various elements of Protected Health Information (PHI) on our systems, and also in hard copy format. The below referenced tables illustrate the various types of specific PHI data and records kept by ABC company, along with all necessary supporting information relating to retention and disposal of such data and records.			
Type of Data	**Format**	**Location**	**Retention Period**	**Disposal Process**
PHI: Consumer Medical Record Number	Electronic records only.	PII is stored in column level encryption in various databases.	7 Years	Script is run to purge database and eventually hard drive is physically destroyed.
PHI: Consumer Social Security Number and Date of Birth	Electronics records only.	PII is stored in column level encryption in various databases.	7 Years	Script is run to purge database and eventually hard drive is physically destroyed.
PHI: Explanation of Benefits (EOB)	Hard Copy records only.	Copies of EOB's are stored in file cabinets.	2 years	Physically destroyed with cross-shredder at Iron Mountain.

Records Retention Matrix for [Enter information for a specific type of record relevant to your industry if you need a matrix that is more descriptive and detailed than the above two (2) matrices. Examples shown in RED below]

Type of Records	Trigger Dates	Format of Documents	Retention Period	Legal Requirements	Disposal Process
Protected Health Information (PHI)	Date of receipt of information from consumer.	Hardcopy Format	7 Years	Per HIPAA	Physically destroyed with cross-shredder at Iron Mountain.
Protected Health Information (PHI)	Date of receipt of information from consumer.	Electronic Format	7 Years	Per HIPAA	Script is run to purge database and eventually hard

					drive is physically destroyed.

Obtaining Data

Data must be obtained in a secure manner so as not to compromise the information traversing public networks and internal company-wide networks. Appropriate security-hardening and configuration standards are to be utilized throughout the entire network, which include, but are not limited to the following information systems: any network component (routers, switches, firewalls, load balancers, etc.), server or application(s) included in or connected to information systems that store, process, and/or transmit data.

Due diligence must be exercised to ensure that other organizations associated with [company name]'s information systems that store, process, and/or transmit data, also have appropriate security measures, standards and safeguards in place.