Lionbridge

Policy for Protected Health Information, Personal Information and Personal Data

Policy Owner: **Lionbridge World Wide Vendor Management Team**

Effective Date: **18 June 2014**

Last Revision Date: **18 June 2014**

PURPOSE: This Policy provides guidelines and procedures regarding the handling of Protected Health Information, Personal Information and Personal Data that may be found in source documents and files which are the subject of the services provided by Lionbridge to its customers.

APPLIES TO: All Lionbridge suppliers of products and services

POLICY:

Lionbridge has determined that any Protected Health Information, Personal Information or Personal Data which is the subject of the services provided by Lionbridge to its customers must be fully de-identified. De-identification is the removal of any information that can be used alone or in combination with other information to identify an individual, such as names, addresses, identification numbers, contact information, dates (e.g. date of treatment), etc. (See complete list below.) The information removed could be Protected Health Information, Personal Information or Personal Data.

What this means for you as you perform services:

If Lionbridge determines that a source document or file received has not been properly or completely de-identified, then Lionbridge will interrupt further access, distribution and use of the source document or file until the issue has been discussed and resolved with the applicable customer. This means that you must immediately stop performing any services with respect to these source documents or files, and must wait for instructions from Lionbridge. If a project deadline is affected or may be affected as a result of you stopping to perform such services, then the Lionbridge project team will take into account any such deadlines and provide you with appropriate instructions. You must comply immediately and fully with any instructions received from Lionbridge. Examples of methods used to resolve the issue of complete de-identification include use of a replacement source document or file, or application of an exception or authorization to resume work on the original source document or file.

These are the guidelines to which each Supplier must comply:

1. **By accepting the Lionbridge SLA, you confirm that you have read and understood this Policy.** You must remain aware of and sensitive to the confidentiality and privacy of records that could potentially identify patients, subjects or any individuals. Even in authorized cases, access, distribution and use should be restricted to the minimum necessary to perform the contracted task.

2. **You must comply immediately and fully with any instructions received from Lionbridge to interrupt access, distribution or use of a source document or file.** Instructions may include the deletion or destruction of any copies of the source document or file with confirmation of such deletion or destruction.

3. **If you become aware of any source documents or files that have not been properly de-identified, then immediately interrupt access, distribution and use of the source documents or files, and notify your Lionbridge contact as soon as possible, and no later than 48 hours after detection of the issue.** You must wait for instructions from Lionbridge regarding these source documents and files. You must comply immediately and fully with any instructions received from Lionbridge.

Any questions regarding this Policy and related instructions may be directed to your Lionbridge Vendor Manager. Project specific questions may be addressed to your Project Manager or other project team contact.

Other References:

De-identification List (provided for illustration purposes only)

A fully de-identified record will remove the following 18 standard de-identification identifiers:

1. Names
2. Addresses or geographic location (smaller than a state)
3. Dates directly related to an individual, including date of birth, admission date, discharge date, death date
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate
13. Device identifiers and serial numbers
14. Web addresses (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger prints and voice prints
17. Full face photographs and comparable images
18. Any other unique identifying number, characteristic or code

Definitions:

"Personal information" is defined as an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Personal Data" is defined as any information relating to an identified or identifiable natural person recorded in any form.

"Protected Health Information" is individually identifiable health information, recorded in any medium, which is related to an individual's past, present or future physical or mental health or condition, or the provision or past, present or future payment for the provision of health care.