HIPPA Compliance and DIVERSIGEN Privacy Policy

1.0 Purpose

1.1 To state DIVERSIGEN's policy on HIPPA compliance and receiving personal health information (PHI) and to outline the process for mitigating erroneous receipt of PHI.

2.0 Scope

2.1 This procedure pertains to all personnel and effects all metadata and PHI received by DIVERSIGEN

3.0 Definitions

3.1 **Personal health information (PHI)**: also referred to as protected health information, is defined as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.

3.1.1 Examples of PHI - names, initials, address, social security number, insurance information, drivers license number, etc.

3.2 **NOT PHI**: some research studies use data that is person-identifiable because it includes personal identifiers such as name, address, but it is not considered to be PHI because the data are not associated with or derived from a healthcare service event (treatment, payment, operations, medical records) not entered into the medical records, nor will the subject/patient be informed of the results. Research health information that is kept only in the researcher's records is not subject to HIPAA but is regulated by other human subject's protection regulations.

3.3 **De-identification**: is the process used to prevent a person's identity from being connected with information. Common uses of de-identification include human subject research for the sake of privacy for research patients. A common strategy for de-identifying datasets are deleting or masking personal identifiers, such as name and social security number, and suppressing or generalizing quasi-identifiers, such as date of birth and zip code.

3.4 **HIPAA**: is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

3.5 **Unique ID**: is any identifier that could be used by the clinical investigator to associate project data with individual patients.

4.0 References

4.1 Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information.

5.0 Materials

5.1 N/A

6.0 Procedure

6.1 All DIVERSIGEN employees are required to read the current BCM policies on HIPAA as well as the Patient Information Privacy and Security Education policy.

- 6.1.1 BCM's policies on HIPAA can be found at https://intranet.bcm.edu/?tmp=/compliance-audit/hipaa/practices/
- 6.1.2 BCM's Patient Information Privacy and Security Education policy can be found at https://intranet.bcm.edu/?fuseaction=home.showpage&tmp=/compliance-audit/pdfs/201_Patient_Information_Privacy_and_Security_Education
- 6.1.3 BCM's code of conduct can found at https://intranet.bcm.edu/?fuseaction=home.showpage&tmp=/compliance-audit/docs/DraftCodeOfConduct26Feb2015
- 6.1.4 Employees should sign and date form CD-9998 to be placed in a their training file acknowledging that they have been informed of BCM's policies and expected conduct.

6.2 It is the responsibility of the sponsor or clinical investigator to de-identify all patient metadata before submitting samples to DIVERSIGEN.

6.3 De-identification occurs either by: (1) meeting the safe harbor in removing 18 identifiers (listed below) and verifying there is no actual knowledge that the residual information can identify the individual; or (2) an expert has documented its statistical or scientific analysis determining that there is a very small risk of an anticipated recipient using such health information with other reasonably available information to identify an individual who is a subject of the information.

- 6.3.1 Names
- 6.3.2 All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- 6.3.3 All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- 6.3.4 Phone numbers
- 6.3.5 Fax numbers
- 6.3.6 Electronic mail addresses
- 6.3.7 Social Security numbers
- 6.3.8 Medical record numbers
- 6.3.9 Health plan beneficiary numbers
- 6.3.10 Account numbers
- 6.3.11 Certificate/license numbers
- 6.3.12 Vehicle identifiers and serial numbers, including license plate numbers;
- 6.3.13 Device identifiers and serial numbers
- 6.3.14 Web Universal Resource Locators (URLs)
- 6.3.15 Internet Protocol (IP) address numbers
- 6.3.16 Biometric identifiers, including finger and voice prints
- 6.3.17 Full face photographic images and any comparable images; and Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

6.4 Mitigation of erroneous receipt of PHI by DIVERSIGEN: Upon receipt, the technician and project manager review all forms of the MCF for accuracy and content.

6.5 If the MCF is found to contain PHI, the reviewer should notify the project manager and remove any information that could be used to identify subject while retaining any unique IDs.

6.5.1 Electronic – Columns in the spreadsheet containing PHI should be deleted

6.5.2 Hard copy – PHI should be marked through with a black marker so that the information is no longer legible

a Note the reason for the mark through

b Initial and date

6.6 The project manager should inform the sponsor that future submissions should not contain PHI and only unique IDs will be accepted.

6.7 Storage and maintenance of all PHI is the responsibility of the sponsor or clinical investigator.

6.8 If a violation/non-compliance involving personal information occurs, the party responsible will undergo repeat training as defined in section 6.1. The effected collaborators will be notified immediately utilizing ADM.004 Deviation Reporting.

7.0 Responsibility

7.1 The administrative staff is responsible for ensuring that all employees are compliant with this SOP. All DIVERSIGEN employees are responsible for compliance with this SOP.

8.0 Revision History

Revision Number	Description of Revision
01	Establishment of SOP. June 5, 2015.

9.0 Dispute Resolution

Within the scope of this privacy notice, if a privacy complaint or dispute cannot be resolved through Diversigen, Inc.'s internal processes, Diversigen, Inc. has agreed to participate in the VeraSafe Privacy Shield Dispute Resolution Procedure. Subject to the terms of the VeraSafe Privacy Shield Dispute Resolution Procedure, VeraSafe will provide appropriate recourse free of charge to you. To file a complaint with VeraSafe under the Privacy Shield Dispute Resolution Procedure, please submit the required information to VeraSafe here: http://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/