BERG Corporate Privacy and Security Policy

The Policy applies to the BERG website and any data provided by the User/ Provider pursuant to a user agreement with BERG for services.

Identification of User Personal Information

User information and identification will only be collected in a manner in which BERG may conduct business, communicate and contact the User. As necessary, the User agrees to voluntarily provide BERG such information as to inquire about services, attain information, register to subscribe, receive a quote for services provided and engage in transactions.

User information that may be collected include, but is not limited to, name, email address, mailing address and phone number.

Users may visit the BERG website anonymously by not providing or entering personal information. While visiting the BERG website, a User may gather information on services and/ or access provided links for information.

Security Identification of User Information

Information that may be collected by BERG while a User is accessing the BERG website and solely for the purpose of ensuring the access request is genuine may consist of the following details:

- Page Information: URL – the URL of the page the user is viewing, Title –the title of the page the user is viewing.
- Browser Information: Browser name- the browser the user is using, Viewport or Viewing pane – the size of the browser window, Screen resolution – the resolution of the user's screen, Java enabled – whether the user has Java enabled.
- User Information: Location – this is derived from the IP address where the hit originated, Language – derived from the language settings of the browser.

Browser Cookies

As per General Data Protection Regulation, EU 2016/679 (GDPR), when accessing the BERG website, a User will be asked to accept "cookies", which are used by BERG only to improve USER participation while accessing BERG's website.

A User may refuse to accept cookies, however experience within certain parts of the BERG website might be reduced.

Sharing User Information

BERG will not forward, sell, share and/or identify any User personal information to third parties, unless agreed to in writing with User and explicitly detailed in an agreement with BERG.

De-Identification of Data must abide by the Requirements

The BERG Corporate Privacy and Security Policy adheres to and upholds the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Protected Health Information (PHI) and General Data Protection Regulation, EU 2016/679 (GDPR) for electronic, paper, and orally protected information handled by BERG employees, business associates and data providers.

Outlined within this Policy are BERG's corporate mandated standards for privacy and security governing the manner in which de-identified Protected Health Information (PHI) data provided to BERG is to be processed, viewed, transmitted, received, managed and reported for the purpose of, including but not limited to, data processing, feature engineering, AI, machine learning, statistical analyses and hypothesis generation.

Protected Health Information (PHI) data may include, but is not limited to, medical and billing records about individuals maintained by or for a covered health care provider, enrollment, payment, claims adjudication, case or medical management record systems maintained by or for a health plan and other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals, including and whether the records have been used to make decisions about individuals requesting access.

The term "record" means any item, collection, or grouping of information that includes Protected Health Information (PHI) and is maintained, collected, used, or disseminated; the past, present, or future physical health or condition of an individual; healthcare services rendered to an individual; the past, present, or future payment for the healthcare services rendered to an individual, along with any of the identifiers as information that appears in medical records, as well as conversations between healthcare staff such as Doctors and Nurses regarding patient treatment. PHI also includes billing information and any information that could be used to identify an individual in a health insurance company's record. Generally, PHI can be found in a wide variety of documents, forms, and communications, such as prescriptions, doctor or clinic appointments, MRI or X-Ray results, blood tests, billing information, or records of communication with doctors or healthcare treatment personnel.

De-Identification of Personal Health Information

BERG will only accept de-identified PHI. As per HIPAA 164.514(b), this Policy, and any BERG contract and/ or agreement the data Provider must remove or omit specified individual identifiers in order to render PHI de-identified (not individually identifiable) prior to transferring data to BERG for the purposes of including but not limited to, dissemination of information, data processing, feature engineering, AI and machine learning, statistical analyses, and hypothesis generation.

Data Providers may include, but are not limited to, Data Purveyor, Provider, Covered Entity, Sponsor, Corporations, Insurance Agencies, Biotechnology Companies, Hospitals, Research facilities, Health Plans, Health Care Clearinghouses, and Health Care Providers.

Provider may use the "Expert Determination" or the "Safe Harbor" methods to render Protected Health Information (PHI) de-identified to BERG.

A data Provider may use the "Expert Determination" method, is by which a formal determination by a qualified expert assess risk, results and provides justification to render information not individually identifiable (de-identifiable) through accepted statistical and scientific principles.

Alternatively, a data Provider may use the "Safe Harbor" method, which requires absence of actual knowledge. Data identifiers listed below must be removed or omitted to ensure provided data cannot be used alone or in combination with other information to identify the individual.

> Name, Address, City, Country, Zip code (including equivalent geocodes), Names of relatives and employers, Birth date, Date of death, Admission and discharge dates, Telephone and fax numbers, E-mail addresses, social security number, medical record number, Health plan beneficiary number, Account number (organization and health plan account numbers), Certificate/license number, Vehicle or other device/ license, serial number, Web URL, Internet Protocol (IP) address, Finger or voice prints, Photographic images, Any other unique identifying number, characteristic, or code

Age and some geographic location information may be included in the de-identified information. All dates directly related to the subject must be removed or limited to the year. Zip codes must be removed or aggregated (in the form of most 3-digit zip codes) to include at least 20,000 people.

Ages of 90 and over must be aggregated to a category of 90+ to avoid the risk of re-identification.

Note: Not included in Data identifiers that must be removed are demographic information, such as gender, race, ethnicity, and marital status.

Sanctions for PHI in Breach of this Policy

In the case that PHI previously de-identified and provided to BERG is found to be identifiable, BERG will immediately conduct an assessment to ascertain the extent of the PHI breach and will immediately take steps to remediate such breach and cease the violation.

BERG will document all breaches and/ or violations. Documentation of a breach will entail, and will not be limited to, de-identified data provider business name, location, type of business, type of information provided, type of information to be gathered, type of breach and/ or violation, extent of breach, assessment, remediation, and steps forward.

A Provider of the de-identified data will be notified by BERG and will be provided with documentation of breach or violation to ensure remediation of breach or violation ceases.

A Provider must acknowledge the BERG notification of breach and/ or violation within 48 hours and propose steps to remediate and ensure breach and/ or violation is ceased and not repeated. A Provider may be asked to participate and meet with the BERG HIPAA, Security and Privacy Office to further discuss a breach or violation and plan an acceptable path forward.

The Provider remediation plan will be assessed by BERG to ascertain if steps provided for remediation are acceptable. A breach and/ or violation finding will be documented as closed if Provider remediation is acceptable.

If BERG finds the remediation to be unacceptable, and/ or a breach and violation continues, BERG has the right to discontinue and terminate the agreement with a Provider.

BERG will inform a Provider that the assessment has been rendered unacceptable and will inform the US Department of Health and Human Services, as well as Business Associates and Government entities, of a Protected Data Breach and /or violations of state and/ or federal law to external agencies to further investigate under HIPAA and GDPR.

Changes to this Policy

BERG, at its own discretion, or upon updates to HIPAA and GDPR may update this Policy. If a User is under agreement with BERG, the User will be notified of upcoming updates to this Policy.

If you have any concerns and/ or questions regarding the BERG Corporate Privacy and Security Policy, please contact us at:

privacy.policy@berghealth.com