NOTICE OF PRIVACY PRACTICES

January 2019

THIS NOTICE DESCRIBES HOW MEDICAL AND PERSONAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Our Commitment to Safeguard Your Personal Data and Protected Health Information.

BioReference Laboratories, Inc. and its subsidiaries and divisions, including but not limited to, GeneDx, Inc., Florida Clinical Laboratory, Inc., and GenPath (collectively "BRLI") are committed to complying with and addressing data protection requirements under all laws that apply to our business, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and in the case of our customers in the European Union, the General Data Protection Regulation (GDPR). This notice of privacy practices **(NOPP**) explains how we handle your personal data and protected health information (PHI) in connection with the provision of clinical laboratory testing services. Please keep in mind that depending on each specific arrangement, we may be considered to be either Data Controllers or Data Processors for purposes of GDPR.

BRLI is required by law to protect the privacy of your personal data and PHI and may need to notify data protection authorities, affected individuals or those Data Controllers instructing it following a breach of unsecured protected health information. As a Data Controller, BRLI is also required to provide you with a copy of this NOPP, and to follow its terms then in effect, except that BRLI reserves the right to change its privacy practices and the corresponding policies and procedures and, where permitted by applicable law, to make these changes effective regarding PHI created or received prior to the effective date of such changes. To this effect, should we make changes to this NOPP, we will post a revised NOPP in our website and in our patient service centers. BRLI may also need to materially change its policies and procedures as necessary to comply with changes in the law and for other valid reasons, in which case it will promptly revise its policies and this NOPP and distribute the revised NOPP in the manner described below.

You have the right to obtain a paper copy of the NOPP upon request. A copy of BRLI's current NOPP will always be available in the reception area of our patient service centers. You will also be able to obtain your own copy by accessing our website at http://www.bioreference.com/privacy calling our office, or asking for one at the time of your on-site visit.

If you have any questions about this NOPP or would like additional information, please contact our Privacy Office at 800-229-5227 Ext 8222.

Please address any written request (such as requests for a copy of this NOPP, access to your record, to restrict a disclosure to a payer, etc.) to:

Data Protection Officer Privacy
Office
BioReference Laboratories, Inc. 481
Edward H. Ross Drive Elmwood Park,
NJ, 07407
Fax: (201) 663-6585

TYPES OF DATA PROCESSED

Personal data that we may process includes the following types of data: name, date of birth, address, e-mail address, telephone numbers (landline and mobile), insurance status, unique numbers that could identify you such as government or private insurance numbers, social security numbers, driver's license or national ID numbers, gender, marital status, and your PHI including but not limited to, names and addresses of your healthcare providers, dates of service, laboratory test results, diagnosis, information about your family or ethnicity (only to the extent required to enable us to provide you with accurate results or diagnostics), genetic or biometric data, and information about your credit card or other forms of payment used to pay for our services. For reference, PHI includes laboratory test orders, laboratory test results and invoices and billing data relating to the healthcare services we provide.

PURPOSE OF DATA PROCESSING, LEGAL BASIS AND DISCLOSURES

We may collect, use, process, disclose and maintain your personal data and PHI for the following purposes:

For Treatment, Benefits and Services: As a service provider we may disclose your PHI to doctors, nurses, and other health care personnel who are involved in providing your health care, and in the course of providing services, we may use your PHI to determine care management options. For example, your PHI will be shared among your doctor(s) and healthcare professionals.

We may also make your PHI available to providers by making it accessible through a Health Information Exchange (HIE), an electronic network that makes it possible to share information electronically, but no one will be permitted to access it through the HIE without your consent except in an emergency and not even then if you direct us not to. Be aware that if your physician allows us to transfer your laboratory and pathology reports to his or her electronic health record (EHR) in his or her office, once they have been transferred anyone taking care of you at that office may be able to access your laboratory and pathology results directly.

For Payment: We may use/disclose your personal data and PHI in order to bill and collect payment for your health care services and/or release portions of your PHI to a private insurer to get paid for services that we delivered to you. For example, we may share your PHI with your health insurance plan so it will pay for your services.

For Health Care Operations: We may use/disclose your PHI in the course of operating our clinical laboratory. For example, we may use your PHI for certain administrative, financial, legal and quality improvement purposes, such as to conduct quality assessments, internal audits, general administrative and business planning activities and other activities necessary to support our healthcare operations.

Business Associates. We may disclose the minimum amount of your personal data and PHI necessary to contractors, agents and other business associates who need the information to help us with billing or other business activities related to the services we provide. For example, we may share personal data and PHI with a billing company that helps us obtain payment from your insurer, an attorney or with a quality assurance consultant in order to obtain their advice regarding our operations. If we do disclose your personal data or PHI to a business associate, we will have a written contract with them that requires the business associate and any of its subcontractors to take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract. Business associates and their subcontractors are considered to be data processors and, as such, are directly bound by law and/or contract to protect your information. With that said, you must keep in mind that some of these business associates may be located outside the United States or the European Union and, consequently, in countries that may not necessarily provide the same level of data protection as in your country of residence. If you are a European resident and would like to request copies of a specific business associate agreement relating to your personal data under GDPR, please contact our Privacy Office at the number and address mentioned above in this NOPP.

PHI from Alcohol and Other Substance Abuse Records: The confidentiality of alcohol and drug abuse patient records is protected by law. We may not disclose PHI regarding alcohol or drug abuse, the fact that a patient attends an alcohol or drug abuse program, or disclose any information identifying a patient as an alcohol or drug abuser without the patient's written consent, unless the disclosure is allowed by a court order, is made to communicate with your treatment providers or medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation, or to report a threat of crime, or a committed crime, by a patient against or at our facilities or our personnel.

When Required by Law: We may collect, use, maintain, process or disclose your personal data and PHI as required by law to do so. For instance, under the United States' *Clinical Laboratory Improvement Amendments of 1988* (CLIA), we are required to obtain and maintain for designated periods of time personal data and specimens belonging to patients for whom we are providing laboratory testing services. Therefore, while you may refuse to provide BRLI with your personal data, we are unable to test any specimen of yours without the personal data elements which we are required to obtain under CLIA. Please note that the CLIA-mandated retention periods can range from two (2) years for test requisitions and authorizations to ten (10) years for pathology test reports and histopathology slides. For more information on the specific CLIA-mandated retention periods please check 42 CFR§493.1105, as amended from time to time. In addition, we maintain patient and customer information in connection with pending litigation, legal processes, legal claims, compliance, regulatory matters and investigations as necessary. If you are providing us with the data of third parties (such as contact information of next of kin or information about your healthcare provider), you must ensure that you notify the relevant third party before sharing their personal information with us by showing them this NOPP, explaining that their personal data will be processed in accordance with this NOPP, and obtaining their consent, where appropriate.

For Public Health Activities: We may disclose PHI when we are required to collect information about disease or injury, or to report vital statistics to the public health authority. We are also required to release some PHI about you to your employer if your employer hires us to perform a pre-employment test or we discover that you have a disease that your employer must know about in order to comply with employment laws.

For Research Purposes: In certain circumstances, pursuant to the approval and supervision of a privacy board, we may use your personal data and disclose PHI to our research staff and their designees in order to assist in medical research.

Victims of Abuse, Neglect or Domestic Violence: We may release your personal data or PHI to a public health authority that is authorized to receive reports of abuse, neglect or domestic violence. For example, we may report your personal data or PHI to government officials if we reasonably believe that you have been a victim of such abuse, neglect or domestic violence. We will make every effort to obtain your permission before releasing this information, but in some cases we may be required or authorized by law to act without your permission.

Judicial and Administrative Proceedings: We may disclose your personal data and PHI in response to valid court orders, court-ordered warrants, and judicial summonses and subpoenas, grand jury subpoenas and administrative requests. We may also disclose your PHI in response to a discovery requests or other legal process and legal requests, but only if efforts have been made, either by the requesting party or us, to first tell you about the request or to obtain an order protecting the information requested.

For Health Oversight Activities: We may disclose PHI to an agency responsible for monitoring the health care system for such purposes as reporting or investigation of unusual incidents and inspecting our facility. These government agencies monitor government benefit programs such as Medicare and Medicaid, as well as compliance with government regulatory programs and civil rights laws.

To Avert Threat to Health or Safety: In order to avoid a serious threat to health or safety, we may disclose personal data or PHI as necessary to law enforcement or other persons who can reasonably prevent or lessen the threat of harm.

For Specific Government Functions: We may disclose personal data and PHI of U.S. military personnel and veterans and to correctional facilities in certain situations, to government benefit programs relating to eligibility and enrollment, and for national security and intelligence activities, such as protection of the President.

For Law Enforcement: We may disclose your personal data or PHI to comply with court orders, to assist law enforcement officers with identifying or locating a suspect, fugitive, witness, or missing person; if we suspect that death resulted from criminal conduct; or if necessary to report a crime that occurred in any of our facilities;

Workers' Compensation: We may disclose your personal data and PHI for workers' compensation or similar programs that provide benefits for work-related injuries, as authorized by and to the extent necessary to comply with laws regarding workers' compensation or similar programs providing benefits for work-related injuries or illness.

Coroners, Medical Examiners and Funeral Directors: Where allowed by applicable law, we may disclose PHI relating to an individual's death to coroners, medical examiners or funeral directors, and to organ procurement organizations relating to organ, eye, or tissue donations or transplants (Note: Information belonging to patients who are deceased more than 50 years is **not** considered PHI.)

To Family, Friends or Others Involved in Your Care: If you do not expressly object we may share your PHI with your family members, friends and others if this information is directly related to their involvement in your care, or payment for your care. In some cases, we may need to share your information with a disaster relief organization that will help us notify these persons.

Completely De-identified or Partially De-identified Information: We may use and disclose your health information if we have removed any information that could identify you. Where permitted by applicable law, we may also use and disclose health information about you for research, public health and specific healthcare operations if most of your identifiers are removed and the person who will receive the information signs an agreement to protect the privacy of the information as required by federal and applicable law. In that case any direct identifiers would be removed, but your zip code, date of birth, dates of service would not be removed.

For Internal Assessments and Healthcare Operations Communications: We may use your personal data to help us understand which products, services and offers are relevant to you, to improve our products and services and generally to communicate news or matters involving quality of care that may be relevant to you. Keep in mind that this use is solely for internal purposes and that we will not sell any of your personal data to any third party. If you do not wish to receive these communications you can inform us of your decision by providing notice to the Privacy Office at the address set forth in this NOPP and we will not engage in such activity.

Other Permitted Disclosures: Regardless of any other provisions in this NOPP, we may disclose or otherwise process your personal data in the context of any sale or transaction involving all or a portion of our business, or as may be required or permitted by law or required for the purposes of any regulatory audit to which we may be subject from time to time.

We will use your personal data, including PHI, only for the purposes for which we collect it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. If we need to use your personal data for another purpose we will explain the legal basis we rely on. Our legal basis to use, process, maintain and disclose your personal data and PHI includes (i) your consent (which may subsequently be withdrawn at any time by contacting the Privacy Office at the address listed in this NOPP), (ii)

legitimate business needs, which include but are not limited to ensuring that we provide accurate results and that we have the right information on file to communicate with you at any time, obtaining payment for our services, and ensuring that we comply with our quality assurance policies, (iii) creation or performance of contractual obligations (e.g. communicating laboratory results to you or your provider) and (iv) compliance with legal requirements (e.g. complying with a court order or a legal mandate).

Requirement for Written Authorization: We will only make other uses and disclosures of your PHI that are not described in this NOPP, and not otherwise required or allowed by law, with your written authorization. For example, we will not sell your PHI or use or disclose your PHI for marketing purposes without your written authorization.

If you provide us with written authorization, you may revoke that written authorization at any time, except to the extent that we have already collected, maintained, used, processed or disclosure the same in accordance with the provisions set forth above. You must revoke your authorization in writing.

Special Protections for HIV, Alcohol and Substance Abuse, Mental Health and Genetic Information: We will comply with all special federal and state privacy protections that apply to HIV-related information, alcohol and substance abuse treatment information, mental health information, and genetic information.

RETENTION PERIOD

We will only retain your personal data and PHI for so long as reasonably necessary for the purposes set out above or as required by applicable laws.

PARTICIPANTS

The privacy practices described in this NOPP will be followed by:

- Any employee or healthcare professional who may draw or test your specimen at any BRLI location;
- Any business associates of BRLI (as described below) and their subcontractors.

These facilities and individuals may share protected health information (PHI) with each other, only as necessary to carry out the treatment, payment, and healthcare operations described in this NOPP.

Personal Representatives: If we confirm that a person has the authority under law to make decisions for you relating to your healthcare ("personal representative"), BRLI will allow your personal representative to make choices with respect to your PHI.

DATA SECURITY

We maintain reasonable security measures to safeguard personal data from loss, interference, misuse, unauthorized access, disclosure, alteration or destruction. We also maintain reasonable procedures to help ensure that such data is reliable for its intended use and is accurate, complete and current.

USE OF COOKIES

From time to time we use cookies and similar technology in our websites and e-mail communications for legitimate business purposes such as collecting statistics, helping optimize site functionality and security, to determine the effectiveness of our communications with customers and, generally, to help us better understand how we can improve our services. Cookies are small files that are placed on your computer by websites that you visit or certain emails you open. These include "preference cookies", "security cookies" or "process cookies". Cookies are widely used in electronic communications around the world. Upon accessing our website you provided us with your consent to the placement of cookies in your computer. Bear in mind that you have the ability to configure your internet browser at any time to block cookies from a specific domain or from all domains. Please take the time to familiarize yourself with your internet browser so that you may configure your privacy settings as you deem appropriate.

YOUR RIGHTS TO ACCESS AND CONTROL YOUR PERSONAL DATA AND PHI

To Request Restrictions on Uses/Disclosures: You have the right to ask that we limit how we use or disclose your personal data and PHI. We will consider your request, but are not legally bound to agree to the restriction However, if you are a EU resident for purposes of GDPR we will comply with any restriction on the use of your data that you request. To this effect, you will need to contact our Privacy Office and provide us with your written and duly authenticated (notarized and certified) instructions, which we will keep on file. To the extent that we do agree to any restrictions on our use/disclosure of your PHI, we will put the agreement in writing and abide by it to the extent permitted by law. We are required, however, to honor your written request if you direct us

not to share specific PHI with your insurance company relating to a service you pay for personally. It is your responsibility to inform other providers who may receive copies of such information that they may not share this information with your insurer.

To Choose How We Contact You: You have the right to ask that we send you information at an alternative address or by an alternative means. We must agree to your request as long as it is reasonably easy for us to do so and we may not ask the reason for the request.

To Inspect and Copy Your PHI: You have the right to inspect and obtain a copy of any of your PHI in either electronic or paper form for as long as we maintain this information in our records. We will provide the records in the specific form and format that you request if it is readily producible in such form or format. To obtain a copy of your PHI, please submit your request in writing. Depending upon where you live, we may charge a fee as permitted by law for the costs of copying, mailing or other supplies necessary to fulfill your request. For example, we do not charge a fee to any European Union residents in connection with the access and copying of such residents' data and/or records, provided that we are provided with appropriate evidence that the requestor is indeed a European Union resident. We generally require payment before or at the time we provide the copies and will let you know the amount due in advance.

Under certain very limited circumstances, we may deny your request to inspect or obtain a copy of your information. If we do, we will provide a written statement that explains the reasons for the denial and a description of your right to have that decision reviewed. In such cases where you have the right to have your denial reviewed, we will describe the review process to you in writing. In the event that your request for access to your PHI is denied for any reason, we will describe to you in writing how you can file a complaint with BRLI or with the Secretary of the United States Department of Health and Human Services' Office of Civil Rights (OCR).

To Request Amendment of Your Personal Data or PHI: If you believe that the personal data or PHI in our system is incorrect or incomplete, you may ask us to amend the information for as long as the information is kept in our records. If you wish to amend your personal data or PHI please request an amendment in writing including why you think we should make the amendment. We will respond to requests by EU residents within 30 days and all other requests within 60 days, barring exceptional circumstances. If we need additional time to respond, we will notify you in writing within 60 days to explain the reason for the delay and tell you when you can expect to have a final answer to your request. If we deny part or all of your request, we will provide you with a written notice explaining our reasons for doing so and how you can appeal the decision.

To Receive an Accounting of Disclosures: You have a right to submit a request in writing asking for information about our disclosures of your personal data or PHI, except for disclosures made:

- For treatment, payment, and operations;
- To you or your personal representative;
- At your written request;
- For national security purposes;
- To family, friends and other persons involved in your care;
- To correctional institutions or law enforcement officers;
- Incidental to permissible uses and disclosures of your PHI (for example, when information is overheard by another person passing by);
- For research or public health using limited portions of your health information that do not directly identify you; and
- That occurred prior to the compliance date of this requirement. If you are a EU resident you have the right to submit a request in writing asking for information about any disclosures of your personal data, regardless of timing. To this effect, you will need to contact our Privacy Office and provide us with your written and duly authenticated (notarized and certify) request, which we will keep on file.

We will respond to your written request for such a list within 60 days (30 days if you are a EU resident) of receiving it. Your request can relate to disclosures going as far back as six years. There may be a charge for more than one such list each year.

To Port Your Personal Data or PHI: You have the right to obtain and reuse your personal data and PHI for your own purposes across different services. Accordingly, to the extent technically feasible, you have the right to request us to move, copy or transfer your personal data and PHI to the data controller of your choice in a safe and secure way. All portability requests shall be addressed in writing to the Privacy Office at the address listed in this NOPP.

To Request the Erasure of Your Personal Data or PHI: If you are a resident of the European Union, you have the right to request that your personal data and PHI be erased from our systems. Bear in mind, however, that we are a U.S.-based diagnostic laboratory and, as such, we are required under CLIA, state laboratory laws and other laboratory accreditation requirements to maintain our patients' PHI for designated periods of time from its receipt/generation, all of which affects our ability to accommodate your request. Once that mandatory timeframe expires we will have the ability to delete your personal data or PHI from our systems if you so desire. To this

effect, please send your written request to the Privacy Office at the address listed in this NOPP.

How to Complain About Our Privacy Practices:

If you believe your privacy rights have been violated, you may file a complaint with BRLI or the federal agency that enforces HIPAA by submitting your complaint as described below:

Data Protection Officer HIPAA
Privacy Office
BioReference Laboratories, Inc.
481 Edward H. Ross Dr.
Elmwood Park, N. J. 07407
800 229-5227 Ext. 8222

Or

Office of Civil Rights
U.S. Department of Health and Human Services 200
Independence Avenue, S.W.
Washington, D.C. 20201
Telephone: (800) 368-1019
www.hhs.gov/ocr/hipaa

If you are a resident of the European Union you may lodge a complaint with a supervisory authority if you consider that our processing of your personal data infringes applicable European law.

You will not be penalized or subject to retaliation for filing a complaint.