ASSURANCE OF VOLUNTARY COMPLIANCE[1]

This Assurance of Voluntary Compliance ("Assurance") is entered into by the Attorneys General[2] of Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut,[3] Delaware, the District of Columbia, Florida, Georgia, Hawaii,[4] Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland,[5] Massachusetts, Michigan, Minnesota, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah,[6] Vermont, Virginia, Washington, West Virginia, and Wisconsin (collectively, the "Attorneys General"), and Laboratory Corporation of America Holdings (the "Company" or "Labcorp") to resolve the Attorneys General's investigation into the data breach publicly announced in June 2019 involving one of Labcorp's debt collection vendors at that time, Retrieval-Masters Creditors Bureau doing business as American Medical Collection Agency ("AMCA"). The Attorneys General and Labcorp are referred to collectively as the "Parties."

---

[1] This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

[2] For ease of reference, each state is listed as "Attorney General." However, individual states may have more precise designations or references.

[3] Reference to the Connecticut Attorney General shall refer to the Attorney General, both acting on his own behalf and as authorized by the Commissioner of Consumer Protection.

[4] Hawaii is represented both by its Attorney General and by its Office of Consumer Protection, an agency which is not part of the state Attorney General's Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii.

[5] Reference to the Maryland Attorney General shall refer to the Consumer Protection Division of the Office of the Attorney General of Maryland, which has authority to enter into this Assurance pursuant to Md. Code Ann., Com. Law § 13-402.

[6] Utah also includes the Attorney General acting on behalf of the Division of Consumer Protection, if executed to that effect.

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

I. INTRODUCTION AND THE PARTIES

1. This Assurance constitutes a good faith settlement and release between Labcorp and the Attorneys General of claims, including those under Consumer Protection Acts, the Personal Information Protection Acts, the Security Breach Notification Acts and the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and its implementing regulations, 45 C.F.R. §§ 160, 162, and 164 ("HIPAA"), as set forth below in Section VI, related to the data breach publicly announced by Labcorp on June 4, 2019, as defined below in Paragraph 3.g).

2. Labcorp, with its principal place of business located at 358 South Main Street, Burlington, NC 27215, is a global life sciences and healthcare company that offers clinical laboratory and diagnostic services and first executed a contract with AMCA in 1996.

II. DEFINITIONS

3. For the purposes of this Assurance, the following definitions shall apply:

a) "Business Associate" is defined in accordance with 45 C.F.R. § 160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to Protected Health Information.

b) "Business Associate Agreement" refers to the contract between a Covered Entity and its Business Associate required by 45 C.F.R. § 164.308(b) and further

prescribed by 45 C.F.R. § 164.314(a) that requires the Business Associate to appropriately safeguard Protected Health Information.

c) "Company" or "Labcorp" means Laboratory Corporation of America Holdings and its affiliates, subsidiaries, divisions, successors, and assigns doing business in the United States that provide clinical laboratory and diagnostic services as a Covered Entity.

d) "Consumer" means any individual whose Personal Information or Protected Health Information Labcorp collects, uses, or maintains in the course of providing goods or services to that individual.

e) "Consumer Protection Acts" means the State citations listed in Appendix A.

f) "Covered Entity" is defined in accordance with 45 C.F.R. § 160.103 as a health plan, health care clearinghouse, or health care provider that transmits Protected Health Information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted standards.

g) "Data Breach" means the security incident publicly reported in June 2019, which resulted in AMCA and Labcorp notifying approximately 10.2 million Labcorp patients that an unauthorized person or persons potentially gained access to certain AMCA systems.

h) "Debt Collector" is defined in accordance with 15 U.S.C. § 1692a(6).

i) "Effective Date" is October 1, 2026.

j) "Fair Debt Collection Practices Act," or "FDCPA," means Public Law 95-109, codified as 15 U.S.C. § 1692 *et seq*.

k) "Minimum Necessary Standard" means the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).

l) "Personal Information" or "PI" means the data elements in the definitions set forth in the Personal Information Protection Acts and Security Breach Notification Acts.

m) "Personal Information Protection Acts" means the State citations listed in Appendix A.

n) "Privacy Rule" refers to the HIPAA Regulations that establish national standards for safeguarding individuals' medical records and other Protected Health Information, including electronic PHI, that is created, received, used, or maintained by a Covered Entity or a Business Associate, specifically 45 C.F.R. Part 160 and 45 CFR Part 164, Subparts A and E.

o) "Protected Health Information" or "PHI" is defined in accordance with 45 C.F.R. § 160.103, including electronic PHI.

p) "Security Breach Notification Acts" means the State citations listed in Appendix A.

q) "Security Rule" refers to the HIPAA Regulations that establish national standards to safeguard individuals' electronic PHI that is created, received, used, or maintained by a Covered Entity or Business Associate, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.

r) "Vendor" means any third-party that accesses, collects, or maintains Consumer Personal Information or Protected Health Information on behalf of Labcorp pursuant to a contract with Labcorp, including but not limited to Labcorp's Business Associates. For purposes of this Assurance, "Vendor" shall not include any third-party that only accesses, collects, uses, or stores *de minimis* amounts of Consumer Personal Information or Protected Health Information on behalf of Labcorp.

s) "Vendor Security Event" means any compromise experienced by a Vendor that results in the unauthorized access or acquisition of the electronic PI or PHI of at least 500 Labcorp Consumers in the United States whose PI or PHI was provided by Labcorp to the Vendor or collected by the Vendor for the benefit of Labcorp.

III. INJUNCTIVE RELIEF

GENERAL COMPLIANCE

4. The Company shall not misrepresent the extent to which it maintains and protects the privacy, security, or confidentiality of PI or PHI collected from or about Consumers.

INFORMATION SECURITY PROGRAM

5. The Company shall, within one hundred and twenty (120) days after the Effective Date of this Assurance, and annually thereafter, review, revise, and update the existing information security program ("Information Security Program") as necessary to comply with this Assurance.

6. The Company shall employ an executive or officer with appropriate credentials, background, and expertise in information security who shall be responsible for overseeing the implementation and maintenance of the Information Security Program (hereinafter for purposes of this Assurance referred to as Chief Information Security Officer or "CISO"). The CISO's responsibilities will include advising the Company's Chief Executive Officer and the Board of Directors regarding the Company's security posture, security risks, and the security implications of the Company's decisions.

7. The Company shall provide security awareness and privacy training to all personnel whose job involves access to or responsibility for Consumer Personal Information and Protected Health Information. Within one hundred eighty (180) days of the Effective Date, the Company shall either provide such training or confirm that such training has been provided within the past twelve months, and thereafter, shall provide it to all such personnel on at least an annual basis and to new personnel within thirty (30) days of hire. The Company shall also provide notice of this

Assurance to employees directly responsible for overseeing implementation, maintenance, or monitoring of Labcorp's Vendor Risk Management processes.

SPECIFIC SAFEGUARDS

8. **Incident Response Plan:** The Company's Information Security Program shall include an incident response plan, which among other things, shall cover the appropriate handling, investigation, and reporting of Vendor Security Events.

9. **Security Events – Internal Reporting of Vendor Security Events:** The Company shall maintain a process for timely reporting of Vendor Security Events to senior management and/or the Board of Directors or a Board of Directors Committee, as appropriate, based on relevant factors, such as the type of vendor and categories and volume of Consumer Personal Information and Protected Health Information involved. The requirements of this Paragraph shall not alleviate or satisfy any reporting obligations of the Company to provide notice pursuant to the Security Breach Notification Acts.

10. **Data Collection, Sharing, and Retention:** As part of its Information Security Program, the Company shall develop, implement, maintain, revise, and comply with policies and procedures governing its collection, use, disclosure, and retention of Consumer Personal Information and Protected Health Information. In particular, the Company shall limit its use and disclosure of Protected Health Information to Vendors to the minimum necessary to accomplish the intended purpose for such use or disclosure, consistent with the Minimum Necessary Standard.

11. **Data Collection, Sharing, and Retention – Debt Collectors**: As part of its Information Security Program, the Company shall develop, implement, maintain, revise, and comply with policies and procedures specific to the sharing of Consumer Personal Information or

Protected Health Information with Debt Collectors. In particular, the Company shall create and maintain:

a) A process to furnish additional information to a Debt Collector when a Consumer responds to a collection attempt with a request for debt verification, as provided by 12 C.F.R. § 1006.34, and the Debt Collector is not already in possession of sufficient information to comply with the Consumer's request. The Company shall provide no more additional information than is necessary to enable the Debt Collector to comply with the request; and

b) A process whereby Debt Collectors, on at least an annual basis, confirm in writing that they have deleted, destroyed, or otherwise made unreadable Consumer Personal Information or Protected Health Information upon satisfaction of the debt or rescission of the referral for collection of the debt, subject to requirements of any applicable law, including the Fair Debt Collection Practices Act and 45 C.F.R. § 164.504(e)(2)(J).

VENDOR RISK MANAGEMENT PROGRAM

12. **Vendor Risk Management Program:** The Company shall develop, implement, maintain, revise, and comply with written policies and procedures to document its Vendors' implementation and maintenance of reasonable security measures to safeguard Consumer Personal Information and Protected Health Information ("Vendor Risk Management Program"). The Company shall review the Vendor Risk Management Program not less than annually and make any updates necessary to reasonably protect the security, integrity, and confidentiality of Consumer Personal Information and Protected Health Information that Vendors access, collect, or

maintain on behalf of the Company. The Company shall provide the resources necessary to allow the Vendor Risk Management Program to function as required by this Assurance.

13. **Vendor Risk Management Team:** The Company shall maintain a Vendor Risk Management Team ("Team") responsible for implementing and maintaining the Vendor Risk Management Program. The Team shall have appropriate background or experience in information security, risk management, and/or auditing to effectuate the Vendor Risk Management Program. The Team shall meet regularly and report to the CISO at least quarterly on the effectiveness of the Vendor Risk Management Program, including describing any identified or potential Vendor security risks and mitigation plans developed in response to such risks.

14. **Vendor Assessment and Monitoring Mechanisms:** The Company shall utilize security assessment and monitoring tools to evaluate whether Vendors are taking reasonable security measures to safeguard Consumer Personal Information and Protected Health Information, such as questionnaires and attestations, third-party audits, formal certifications, and on-site visits. The frequency, type, and robustness of such measures shall be based primarily on each Vendor's associated risk rating, which shall take into account the nature of the Vendor and the services provided. The risk rating assigned to Debt Collectors shall also include factors documented by the Company, such as type and volume of Consumer Personal Information and Protected Health Information provided to the Debt Collector.

15. **Vendor Questionnaires:** Where the Company requires Vendors to provide responses to questionnaires, the Company shall seek corroboration as appropriate based on the circumstances, which may include supporting documentation as well as follow up with the Vendors. The Company shall implement and maintain a process to track Vendor questionnaires.

16. **Debt Collector Contract Inventory:** The Company shall maintain and regularly update an inventory of its contracts with Debt Collectors. The inventory shall include a description of the nature and type of Consumer Personal Information or Protected Health Information that each Debt Collector possesses, processes, transmits, uses, maintains, stores or accesses; the risk rating assigned to each Debt Collector; as well as the date(s) of each Debt Collector's last questionnaire and, if applicable, completed risk assessments, penetration tests, and any third-party security audit(s) performed relating to that contract.

17. **Debt Collector Contracts—Specific Security Requirements**: The Company shall require all Debt Collectors, through a Business Associate Agreement or other written contract, to implement industry-recognized standards and/or frameworks that include cybersecurity or data security-related requirements for protecting data and information systems, such as the National Institute of Standards and Technology's Cybersecurity Framework. The Company shall contractually require Debt Collectors to comply with the following data security requirements:

a) In a multi-tenant environment, data stores holding Consumer Personal Information or Protected Health Information provided by the Company or collected by the Debt Collector for the benefit of the Company must be segmented from other Consumer Personal Information or Protected Health Information, or if segmentation is not feasible, alternative reasonable measures must be used to protect such information.

b) Consumer Personal Information and Protected Health Information must be collected, accessed, disclosed, and retained only to the minimal extent necessary and consistent with the Minimum Necessary Standard, where applicable.

c) Data disposal of Consumer Personal Information and Protected Health Information must be performed in accordance with applicable National Institute of Standards and Technology (or any successor body) standards.[7]

d) Cryptographic keys must never be stored in equipment, documents or systems that are not provisioned to meet secure key management requirements (*e.g.*, log files, ticket tracking systems, knowledge management systems, or training documentation).

e) Passwords used to protect cryptographic keys must be as strong as the keys they protect.

f) Maintain a process to remediate critical vulnerabilities reported by the United States Computer Emergency Readiness Team or equivalent governmental agency ("US CERT") that impact PI or PHI within the timeframe set by policy.

18. **Debt Collector Risk Assessments**: The Company shall contractually require all Debt Collectors to conduct annual risk assessments that cover Consumer Personal Information and Protected Health Information accessed, collected, or maintained on the Company's behalf. The Company shall also require Debt Collectors to provide an attestation that such an annual risk assessment was performed and that deficiencies identified by such assessment as critical or high risk have been addressed or will be addressed.

19. **Debt Collector Penetration Tests:** The Company shall contractually require that Debt Collectors have penetration tests that cover the portions of their network used to store, process, or transmit Consumer Personal Information and Protected Health Information on at least

[7] As of the Effective Date, such standards include Special Publication 800-88 as revised.

an annual basis and provide an annual attestation to the Company that such tests were performed and that deficiencies identified by such testing as critical or high risk have been addressed or will be addressed.

20. **Debt Collector Audits**: The Company shall contractually require Debt Collectors to conduct annual SOC 2 Type 2 Audits consistent with the criteria developed by the American Institute of CPAs, or bi-annual HITRUST CSF Validated Assessments consistent with the criteria developed by the Health Information Trust Alliance, or a reasonably equivalent external audit, and provide an annual attestation to the Company that such an external audit was conducted and that deficiencies identified by such audit as critical or high risk have been addressed or will be addressed.

21. **Debt Collector Roles and Responsibilities**: The Company shall include in its Debt Collector contracts the roles and responsibilities to be undertaken by the Company and the Debt Collector in the event of a Vendor Security Event, including the provision of Consumer notice by the appropriate party or parties.

22. **Debt Collector Non-Compliance**: The Company shall retain contractual rights to take appropriate action against any Debt Collector that the Company determines is not complying with the applicable requirements set forth in this Assurance, up to and including termination of its contract with that Debt Collector.

23. **Debt Collector Contract Requirements – Implementation:** The Company shall amend existing contracts with Debt Collectors to include the requirements contained in Paragraphs 17 - 22 to the extent such requirements are not included, within twelve (12) months of the Effective Date.

IV. ASSESSMENT

24. Within eighteen (18) months after the Effective Date of this Assurance, the Company shall obtain an assessment from an independent third-party professional ("Third-Party Assessor") to assess the Company's compliance with the terms of this Assurance, using procedures and standards generally accepted in the profession ("Third-Party Assessments"). The Third-Party Assessor shall: (a) be certified as a Certified Information Systems Security Professional ("CISSP") or equivalent certification; and (b) have at least five (5) years of experience evaluating the effectiveness of information system security and, in particular, vendor risk management practices.

25. The Third-Party Assessor shall prepare a formal report of its Assessment ("Third-Party Assessor's Report") and shall provide a copy of the Third-Party Assessor's Report to the Connecticut Attorney General within sixty (60) days of its completion. The Connecticut Attorney General's Office shall, to the extent permitted by the laws of the State of Connecticut, treat the Third-Party Assessor's Report as exempt from disclosure under the relevant public records laws, or as necessary by employing other means to ensure confidentiality.

26. **Signatory State Access to Report:** The Connecticut Attorney General's Office may provide a copy of the Third-Party Assessor's Report to any other participating Attorneys General upon request, and each requesting Attorney General shall, in accordance with and to the extent permitted by the laws of the Attorney General's State, treat such Third-Party Assessor's Report as exempt from disclosure under the relevant public records laws.

V. PAYMENT TO THE STATES

27. The Company shall pay or cause to be paid the total sum of $2,287,455.00 (two million, two hundred eighty-seven thousand, four hundred fifty-five dollars) to the Attorneys General.

28. Of the total amount, $89,178.00 (eighty-nine thousand, one hundred and seventy-eight dollars) shall be paid to the State of New York. Any payment shall reference AOD No. 26-053. This payment shall be made within thirty (30) days of the Effective Date of this Assurance; provided, however, that if state law requires judicial or other approval of the Assurance, and such approval has not been obtained by the Effective Date, the payment shall be made no later than thirty (30) days after notice from the Attorney General that such final approval for the Assurance has been secured.

VI. RELEASE AND EXPIRATION

29. **Release:** Following the Effective Date and full payment of the amounts due pursuant to this Assurance, the Attorney General hereby releases and discharges the Company from all civil claims that the Attorney General could have brought under HIPAA, the Consumer Protection Acts, the Personal Information Protection Acts, the Security Breach Notification Acts, and/or any common law claims concerning unfair, deceptive, or fraudulent trade practices based on the Company's conduct related to the Data Breach prior to the Effective Date. Nothing in this Paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that the Company has under this Assurance. Further, nothing in this Assurance shall be construed to waive or limit any private rights of action. This release shall not include any of the following forms of liability:

a) Any criminal liability that any person or entity, including the Company, has or may have to the States; and

b) Any civil or administrative liability that any person or entity, including the Company, has or may have to the States under any statute, regulation or rule giving rise to, any and all of the following claims:

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

30. **Expiration:** The obligations and other provisions in this Assurance set forth in Paragraphs 9 – 22 shall expire five (5) years after the Effective Date of this Assurance.

VII. GENERAL PROVISIONS

31. **Meet and Confer**: If the Attorney General has a reasonable belief that Labcorp has failed to comply with any of the terms of this Assurance, and, if in the Attorney General's sole discretion, the failure to comply does not threaten the health or safety of the Attorney General's State or its residents and/or does not create an emergency requiring immediate action, the Attorney General may notify Labcorp in writing of such failure to comply and Labcorp shall have thirty (30) days from receipt of such written notice to provide a good faith response to the Attorney General's determination. The response shall include: (A) a statement explaining why Labcorp believes it is in full compliance with this Assurance; or (B) a detailed explanation of how the alleged violation(s) occurred, and either (i) a statement regarding whether the alleged violation(s) has been addressed and how, or (ii) a statement regarding whether the alleged violation cannot be reasonably addressed within thirty (30) days receipt of the notice, but, if (B)(ii), then also a statement (a) indicating whether Labcorp has begun to take corrective action(s) to address the alleged violation(s), (b) stating what corrective action(s) Labcorp is pursuing, and (c) providing the Attorney General with a reasonable timetable for addressing the alleged violation(s). Nothing herein shall prevent the Attorney General from agreeing in writing to provide Labcorp with additional time beyond the thirty (30) day period to respond to the notice referenced in this Paragraph. Notwithstanding the requirements above, nothing contained in any response provided

by Labcorp pursuant to this Paragraph shall prevent the Attorney General from taking any action to enforce the requirements of this Assurance.

32. Nothing in this Assurance shall be construed to limit the authority or ability of the Attorney General to protect the interests of New York or the people of New York. This Assurance shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against the Company for conduct subsequent to or otherwise not covered by the Release. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that the Company has under this Assurance.

33. Nothing in this Assurance shall be construed as excusing or exempting Labcorp from complying with applicable state or federal laws, rules, or regulations, nor shall any of the provisions of this Assurance be deemed to authorize or require Labcorp to engage in any acts or practices prohibited by such laws, rules, or regulations.

34. The Parties understand and agree that this Assurance shall not be construed as an approval or sanction by the Attorney General of the Company's business practices, nor shall the Company represent that this Assurance constitutes an approval or sanction of their business practices. The Parties further understand and agree that any failure by the Attorney General to take any action in response to information submitted pursuant to this Assurance shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.

35. Nothing contained in this Assurance is intended to be and shall not in any event be construed or deemed to be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of the Company or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without

any finding of liability of any kind. The Company enters into this Assurance for settlement purposes only.

36. The settlement negotiations resulting in this Assurance have been undertaken in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Assurance shall be offered or received in evidence in any action or proceeding for any purpose.

37. The Company shall deliver a copy of this Assurance to, or otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, CISO, the General Counsel or Senior Legal Officer, and the Chairperson of the Audit Committee of the Board of Directors within ninety (90) days of the Effective Date.

38. In the event that the Company acquires or merges with a subsidiary or affiliate after the Effective Date and that subsidiary or affiliate is wholly owned by the Company, the Company shall have one hundred and twenty (120) days from the date the Company completes the transaction to develop and implement an integration timetable regarding compliance with the applicable terms of this Assurance. For purposes of this Paragraph, implementation means that the Company or its wholly owned subsidiary or affiliate (i) has taken relevant measures where technologically feasible and otherwise reasonable or have taken alternative measures that alone or in the aggregate provide for substantially equivalent security and/or risk management, or (ii) has developed a reasonable and appropriate plan to evaluate the technological and operational feasibility of the provisions of this Assurance. When applicable, the CISO will report to the CEO on a semiannual basis regarding the implementation timetable progress, as well as document any significant delays or revisions to the timetable.

39. To the extent that there are any, the Company agrees to pay all court costs associated with the filing (if legally required) of this Assurance. No court costs, if any, shall be taxed against the Attorneys General.

40. The Company agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and the Company further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

41. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

42. This Assurance shall not be construed to waive any claims of sovereign immunity the States may have in any action or proceeding.

43. In states where this Assurance must be filed with and/or approved by a court, the Company consents to the filing of this Assurance and its approval by the court and authorizes the Attorney General in such states to represent the Company does not object to court approval of the Assurance. The Company further consents to the jurisdiction of each such court for the sole and exclusive purpose of having such courts approve or enforce this Assurance.

VIII. SEVERABILITY

44. If any clause, provision, or section of this Assurance shall, for any reason, be held to be illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Assurance, which shall be construed and

enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

IX. NOTICE / DELIVERY OF DOCUMENTS

45. Whenever the Company shall provide notice to the Attorney General under this Assurance, that requirement shall be satisfied by sending notice to:

Bureau Chief
Bureau of Internet and Technology
New York State Office of the Attorney General
Liberty Street, New York, NY 10005
ifraud@ag.ny.gov

46. Any notices or other documents sent to the Company pursuant to this Assurance shall be sent to the following addresses:

Laboratory Corporation of America Holdings
Attn: Scott Bayzle
531 South Spring Street
Burlington, NC 27215

with a copy to

Allison Holt Ryan
Adam Cooke
Hogan Lovells Cadwalader US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Email: allison.holt-ryan@hlc.com
adam.a.cooke@hlc.com

47. All notices or other documents to be provided under this Assurance shall be sent by U.S. mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document and shall have been deemed to be sent upon mailing. Additionally, any notices or documents to be provided under this Assurance shall also be sent by electronic mail if an email

address has been provided for Notice. Any party may update its address by sending written notice to the other party.

FOR LABORATORY CORPORATION OF AMERICA HOLDINGS:

By: _____ Date: 09/18/2026

Name: Matthew Mall

Title: Senior Vice President and General Counsel

Office: 10 Moore Drive, Durham, NC 27713

LETITIA JAMES

ATTORNEY GENERAL OF THE STATE OF NEW YORK

By: */s Clark Russell*

Clark Russell

Bureau of Internet and Technology

New York State Attorney General

28 Liberty St. New York, NY 10005

Date: September 10, 2026

LABCORP MULTISTATE
APPENDIX A

STATE	CONSUMER PROTECTION LAWS	DATA BREACH NOTIFICATION & PERSONAL INFORMATION PROTECTION LAWS
AK - ALASKA	Unfair Trade Practices Act, Alaska Stat. 45.50.471, *et seq*.	Alaska Stat. 45.48.010, *et seq*.
AL - ALABAMA	Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-1, *et seq*.	Data Breach Notification Act of 2018, Ala. Code §§ 8-38-1, *et seq*.
AR - ARKANSAS	Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-101, *et seq*.	Arkansas Personal Information Protection Act, Ark. Code Ann. §§ 4-110-101, *et seq*.
AZ - ARIZONA	Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, *et seq*.	Ariz. Rev. Stat. §§ 18-551 and 18-552
CO - COLORADO	Colorado Consumer Protection Act, C.R.S. §§ 6-1-101, *et seq*.	C.R.S. § 6-1-716 and C.R.S. § 6-1-713.5
CT- CONNECTICUT	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b, *et seq*.	Breach of Security, Conn. Gen. Stat. § 36a-701b; Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
DC - DISTRICT OF COLUMBIA	Consumer Protection Procedures Act, D.C. Code §§ 28-3901, *et seq*.	District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, *et seq*.
DE - DELAWARE	Consumer Fraud Act, 6 Del. C. § 2511, *et seq*.	Delaware Data Breach Notification Law, 6 Del. C. § 12B-100, *et seq*.
FL - FLORIDA	Florida Deceptive and Unfair Trade Practices Act, Chapter 501, Part II, §§ 501.201, *et seq*., Florida Statutes	Florida Information Protection Act, § 501.171, Florida Statutes
GA - GEORGIA	Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-390 through -408	Georgia Personal Identity Protection Act, O.C.G.A §§ 10-1-910 through -915
HI - HAWAII	Uniform Deceptive Trade Practice Act, Haw. Rev. Stat. ch. 481A and Haw. Rev. Stat. § 480-2	Haw. Rev. Stat. ch. 487J and Haw. Rev. Stat. ch. 487N
IA - IOWA	Iowa Consumer Fraud Act, Iowa Code § 714.16	Personal Information Security Breach Protection Act, Iowa Code Ch. 715C
ID - IDAHO	Idaho Consumer Protection Act, Idaho Code §§ 48-601, *et seq*.	Idaho Data Breach Notification Law, Idaho Code, Title 28, Chapter 51, §§ 28-51-104, *et seq*.
IL - ILLINOIS	Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.	Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.
IN - INDIANA	Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5, *et seq*.	Disclosure of Security Breach Act, Ind. Code §§ 24-4.9, *et seq*.
KS - KANSAS	Kansas Consumer Protection Act, K.S.A §§ 50-623, *et seq*.	Security Breach Notification Act, K.S.A. §§ 507a01, *et seq*.; The Wayne Owen Act, K.S.A. § 50-6,139b

LABCORP MULTISTATE
APPENDIX A

KY - KENTUCKY	Kentucky Consumer Protection Act, KRS §§ 367.110-367.300, 367.990	KRS 365.732
MA - MASSACHUSETTS	Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A	Mass. Gen. Laws ch. 93H; 201 Code Mass. Regs. 17.00, *et seq.*
MD - MARYLAND	Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101, *et seq.*	Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501, *et seq.*
ME - MAINE	Maine Unfair Trade Practices Act, 5 M.R.S.A. §§ 205-A, *et seq.*	Maine Notice of Risk to Personal Data Act, 10 M.R.S.A. §§ 1346, *et seq.*
MI - MICHIGAN	Michigan Consumer Protection Act, MCL 445.901 *et seq.*	Identity Theft Protection Act, MCL 445.61, *et seq.*
MN - MINNESOTA	Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43- .48; Consumer Fraud Act, Minn. Stat. §§ 325F.68-.694	Minnesota Data Breach Notification Statute, Minn. Stat. § 325E.61; Minnesota Health Records Act, Minn. Stat. §§ 144.291-144.29834
MO - MISSOURI	Mo. Rev. Stat. §§ 407.010, *et seq.*	Mo. Rev. Stat. § 407.1500
NC - NORTH CAROLINA	North Carolina Unfair and Deceptive Trade Practices Act, N.C.G.S. §§ 75-1.1, *et seq.*	Identity Theft Protection Act, N.C.G.S. §§ 75-60, *et seq.*
NE - NEBRASKA	Nebraska Consumer Protection Act, Neb. Rev. Stat. §§ 59-1601, *et seq.*	Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. §§ 87-801, *et seq.*
NH - NEW HAMPSHIRE	New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann §§ 358-A:1, *et seq.*	N.H. Rev. Stat. Ann §§ 359-C: 19-21
NJ - NEW JERSEY	New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1, *et seq.*	New Jersey Identity Theft Prevention Act, N.J.S.A. 56:8-161 to -166
NM - NEW MEXICO	New Mexico Unfair Practices Act, NMSA 1978, §§ 57-12-1, *et seq.*	Data Breach Notifications Act, NMSA 1978, §§ 57-12C-1, *et seq.*
NV - NEVADA	Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903, *et seq.*	Nev. Rev. Stat. §§ 603A.010-603A.290
NY - NEW YORK	N.Y. Executive Law § 63(12); N.Y. Gen. Bus. LawGeneral §§ Business Law 349/350	General Business Law, N.Y. Gen. Bus. Law §§ 899-aa and 899-bb
OH - OHIO	Ohio Consumer Sales Practices Act, R.C. §§ 1345.01, *et seq.*	R.C. §§ 1349.19 to 1349.192
OK - OKLAHOMA	Oklahoma Consumer Protection Act, 15 O.S. Section 751, *et seq.*	Oklahoma Security Breach Notification Act, 24 O.S. Section 161, *et seq.*

LABCORP MULTISTATE
APPENDIX A

OR - OREGON	Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq*.	Oregon Consumer Information Protection Act, ORS 646A.600, *et seq*.
PA - PENNSYLVANIA	Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq*.	Breach of Personal Information Notification Act, 73 P.S. §§ 2301, *et seq*.
RI - RHODE ISLAND	Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1, *et seq*.	Rhode Island Identity Theft Protection Act R.I. Gen. Laws §§ 11-49.3-1, *et seq*.
SC - SOUTH CAROLINA	South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-10, *et seq*.	South Carolina Data Breach Notification Law, S.C. Code Ann. § 39-1-90
TN - TENNESSEE	Tennessee Consumer Protection Act of 1977, Tenn. Code Ann. §§ 47-18-101, *et seq*.	Tennessee Identify Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to -2111
TX - TEXAS	Texas Deceptive Trade Practices Consumer Protection Act, Tex. Bus. & Com. Code Ann. §§ 17.41 - 17.63	Identity Theft Enforcement and Protection Act, Tex. Bus. & Com. Code Ann. §§ 521.001 - 521.152
UT - UTAH	Utah Consumer Sales Practices Act Utah Code §§ 13-11-1, et. seq.	Utah Protection of Personal Information Act, Utah Code §§ 13-44-101, *et seq*.
VA - VIRGINIA	Virginia Consumer Protection Act, Virginia Code §§ 59.1-196 through 59.1-207	Virginia Breach of Personal Information Notification Law, Virginia Code § 18.2-186.6
VT - VERMONT	Vermont Consumer Protection Act, 9 V.S.A. §§ 2451, *et seq*.	9 V.S.A §§ 2430, 2431, and 2435
WA - WASHINGTON	Washington Consumer Protection Act, RCW 19.86.010, *et seq*.	Washington Data Breach Notification Law, RCW 19.255.005, *et seq*.
WI - WISCONSIN	Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§ 100.18, *et seq*.	Wisconsin Data Breach Notification Law, Wis. Stat. § 134.98
WV - WEST VIRGINIA	West Virginia Consumer Credit and Protection Act, W. Va. Code §§ 46A-1-	West Virginia Consumer Credit and Protection Act, W. Va. Code §§ 46A-2A-101, *et seq*.