United States Securities and Exchange Commission
Washington, D.C. 20549

NOTICE OF EXEMPT SOLICITATION
Pursuant to Rule 14a-103

Name of the Registrant: Laboratory Corporation Holdings of America
Name of persons relying on exemption: Tara Health Foundation
Address of persons relying on exemption: 47 Kearny Street, San Francisco, CA 94108

Written materials are submitted pursuant to Rule 14a-6(g) (1) promulgated under the Securities Exchange Act of 1934. Submission is not required of this filer under the terms of the Rule, but is made voluntarily in the interest of public disclosure and consideration of these important issues.

PROXY MEMORANDUM

TO:	Shareholders of Laboratory Corporation Holdings of America
RE:	Proposal No. 7 (Reproductive Rights and Data Privacy Report)
DATE:	April 4, 2023
CONTACT:	Shelley Alpern, Rhia Ventures at Corporate.Enagement@rhiaventures.org

---

This is not a solicitation of authority to vote your proxy. Please DO NOT send us your proxy card; Tara Health Foundation is not able to vote your proxies, nor does this communication contemplate such an event. Tara Health Foundation urges shareholders to vote for Proposal No. 7 following the instructions provided on management's proxy mailing.

Tara Health Foundation urges shareholders to **vote YES** on Proposal No. 7 on the 2023 proxy ballot of Laboratory Corporation Holdings of America ("Labcorp" or the "Company"). The Resolved clause states:

> Shareholders request that our Board issue a public report detailing any known and potential risks and costs to the Company of fulfilling information requests relating to LabCorp customers for the enforcement of state laws criminalizing abortion access, and setting forth any strategies beyond legal compliance that the Company may deploy to minimize or mitigate these risks. The report should be produced at reasonable expense, exclude proprietary or legally privileged information, and be published within one year of the annual meeting.

About Tara Health Foundation

Tara Health Foundation aims to improve the health and well-being of women and girls through the creative use of philanthropic capital. Our main areas of focus are reproductive and maternal health in the United States, equitable workplaces, and gender lens impact investing.

Tara Health Foundation is a long-term shareholder in Labcorp. We support this shareholder proposal because the Company amasses massive amounts of women's personal health data but lacks transparency as to how such data is or may imperil access to reproductive healthcare. In a time when abortion access is criminalized or severely restricted by half of the states, greater understanding about the Company's data handling practices is warranted.

Background on the Proposal

Following the unprecedented revocation of the constitutional right to abortion in June 2022, at least a dozen states have criminalized the procedure, and about half of the states are expected to enact laws making abortion broadly illegal. Law enforcement in these abortion-restrictive states are expected to rely on consumer data to investigate and prosecute individuals who provide, aid, or receive the procedure, even if conducted in states where abortion remains legal.

A digital reproductive health footprint could be easily accessed by law enforcement and lead to criminal charges. Meta recently received significant negative press after complying with a data request from a Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy (for additional examples, see Addendum A).[1]

Labcorp has been largely silent on the issue, even though it is a nationwide provider of reproductive healthcare services and is heavily investing in women's healthcare.[2] Indeed, the Company "conducts about 250 million tests yearly on women" ranging from infertility to pregnancy and general women's health.[3] In 2021, the Company acquired Ovia Health, a digital health app used by over 15 million women seeking information and support with family planning, pregnancy, and parenting.[4]

---

[1] https://tinyurl.com/2etavr8t

[2] https://ir.labcorp.com/static-files/129475f0-f71c-45de-985d-1c74cfb5cabc.

[3] https://womenshealth.labcorp.com/about

[4] https://www.labcorp.com/newsroom/labcorp-extends-leadership-womens-health-acquisition-ovia-health

Given the nature of the Company's sensitive data, Labcorp will be especially vulnerable to law enforcement data requests related to abortion, particularly with respect to interstate conflicts regarding exercise of reproductive rights in states where abortion remains legal. Shareholders have reason to be concerned about whether the enforcement of criminal abortion laws will impact the reputation and financial wellbeing of the Company. The Proposal therefore calls upon management to examine the risks associated with the Company's current data handling practices, including its response to government information requests, in the face of new restrictive abortion laws.

Rationale in Support of the Proposal

1. Labcorp's data handling policies are unclear, inconsistent, and incomplete.
2. The Company does not offer transparency reporting regarding data privacy.
3. Regulatory and legal compliance is insufficient to minimize privacy risks related to reproductive healthcare.
4. Production of the requested report would be feasible and cost-effective.

Labcorp's data handling policies are unclear, inconsistent, and incomplete

Women and other birthing people interact with Labcorp in a number of ways governed by different Labcorp privacy policies that are unclear, incomplete, and sometimes inconsistent.

1. Sensitive personal data collected from Labcorp's website could be shared without consumer consent with third parties like law enforcement and advertisers

Consumers may access the Labcorp website to research information, make inquiries, or pay for Company products and services related to reproductive healthcare.

According to Labcorp's *Website Privacy Policy*, the Company may collect personal information from website visitors such as an individual's "usage details, IP addresses, [and] location data."[5] Notwithstanding the sensitive nature of this data, Labcorp may share it with third parties without the individual's consent. For example, Labcorp may provide personal consumer information to "contractors and partners" for services like data and payment processing, thereby expanding the net of companies that may be subject to government data requests from states criminalizing abortion access. While Labcorp's *Website Privacy Policy* sets parameters on how these third parties may use the personal data, it does not disclose what privacy guidelines, if any, third parties must follow in order to minimize their vulnerability to leaks or government data requests.

[5] https://www.labcorp.com/about/web-privacy-policy

Labcorp may also provide personal information collected from its website "in response to duly authorized information requests of any law enforcement agency." However, Labcorp has failed to clarify if such data requests must be accompanied by a court order or if the Company could voluntarily share the data. For instance, could the Company disclose information about searches related to pregnancy testing in response to a police department seeking evidence in connection with an illegal abortion, but without a judge having ever reviewed or approved the request?

2. Personal health data is vulnerable to law enforcement information requests

General personal information collected via the Labcorp website, as described above, is generally not protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), but personal health information ("PHI") collected by entities such as Labcorp in the course of provision of health-related services is protected under HIPAA in certain instances. For example, PHI that the Company collects from consumers related to pregnancy, fertility, or women's general health is covered by HIPAA.

While HIPAA would normally prohibit Labcorp from sharing PHI with third parties without the individual's consent, HIPAA provides an exception for law enforcement purposes. This exception is somewhat reflected in Labcorp's *HIPAA Information* notice, which states that the Company may disclose PHI "in response to a court order, warrant, subpoena or summons, or similar process authorized by law."[6]

Guidance from the U.S. Department of Health and Human Services ("HHS"), which enforces HIPAA, following the revocation of abortion rights in 2022 provides stricter HIPAA protections, which the Company has failed to expressly adopt in its privacy policies.[7] According to HHS, entities regulated by HIPAA may disclose only the PHI expressly requested by a court order, but no more. In addition, HHS provides that HIPAA generally "permits but *does not require*" a covered entity to disclose PHI to law enforcement without consumer consent if the entity believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Some have argued that this exception applies to reproductive healthcare, and even to protection of a fetus, which position HHS disavows.

---

[6] https://www.labcorp.com/about/hipaa-information

[7] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

To date, the Company has failed to clarify whether and how it applies the foregoing HHS guidance on HIPAA privacy safeguards with regard to reproductive healthcare information, even though it is a recommended service provider by reproductive healthcare organizations like Planned Parenthood.[8] For instance, unlike other publicly traded companies and its own subsidiary Ovia Health,[9] Labcorp provides no assurances that it will only deliver the narrowest possible set of data to the extent it is legally required by a court, or notify the affected consumer of the data request.

3. Personal information collected by the reproductive health and family planning platform Ovia Health may not be protected against law enforcement data requests

Ovia Health's data collection practices, on the other hand, are governed by separate privacy policies. Although Ovia Health collects incredibly sensitive and detailed information from consumers, most of its data is not protected by HIPAA given that the privacy law is generally inapplicable to health apps.[10]

Ovia Health collects sensitive information from app users that may be relevant to abortion-related criminal investigations. Such data includes "date of last period, due date, and other fertility, pregnancy, health, sex life and life" information, in addition to data about the user's habits, purchases, geolocation, and "photos or videos" uploaded to the app.[11] Ovia Health further collects information from non-app users that visit its website, similar to the type of data collected from Labcorp website visitors.[12]

According to Ovia Health, HIPAA privacy safeguards only apply to data of "premium" users,[13] since premium features are obtained through a health insurer or a health plan – both of which are covered entities under HIPAA. As a result, many app users are exposed to lax privacy protections. For example, Ovia Health sells much of this data with third parties such as advertisers. The *Ovia Health Apps Privacy Policy* is unclear if these third parties must comply with any privacy safeguards, including reselling the data to other parties such as data brokers who may then make the data available to police or even to those seeking to take advantage of "vigilante abortion laws," which incentivize citizens with a cash bounty if they succeed in suing individuals who have helped a person get an illegal abortion.

Overall, Labcorp publishes vague, confusing, incomplete, and sometimes inconsistent privacy policies that leave both consumers and investors puzzled as to whether the Company may be unnecessarily exposing consumers to risk of criminal punishment for accessing reproductive healthcare by virtue of the data the Company collects and retains. Implementation of this Proposal would clarify whether any such risks indeed exist, in addition to those identified herein.

---

[8] https://tinyurl.com/2tnehyz2

[9] https://www.oviahealth.com/how-does-ovia-respond-to-data-requests/

[10] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html

[11] https://www.oviahealth.com/privacy-policy/

[12] https://www.oviahealth.com/non-app-privacy-policy/

[13] https://www.oviahealth.com/guide/255768/why-do-we-ask-for-this/#you-say-under-hippa

Labcorp does not offer transparency reporting regarding data privacy, exposing the Company to financial and reputational risks

A recent empirical study in the *Journal of Marketing* showed that vulnerabilities concerning the misuse of commercial data can generate negative outcomes for businesses, including negative abnormal stock returns and damaging customer behaviors such as negative word of mouth and switching to a close business rival.[14] These findings could apply to data vulnerabilities from actual and potential disclosures of abortion-related data to law enforcement, thereby amplifying consumer worries about data misuse. Consequently, corporations collecting large troves of consumer data, such as Labcorp, are likely exposing themselves to higher financial and reputational risks. Apropos to the current Proposal, the study found that data transparency, among other things, can alleviate these detrimental effects.

Labcorp does not publish transparency reporting regarding data privacy. Conversely, many publicly traded companies offer transparency reporting specifically on the issue of government data requests. Meta, Amazon and Google offer such reporting semiannually, which includes details on the types of requests, compliance rates and jurisdictional information. This information would be extremely helpful for investors to make determinations about the Company's risk exposure as well as serve as an accountability tool. In turn, consumers would gain more assurances that Labcorp respects the privacy of their data.

Why a YES Vote is Warranted: A Response to Labcorp's Opposition Statement

In opposing the Proposal, the Company states it has systems and processes that are designed to comply with applicable privacy laws and regulations. The Company further provides that preparation and publication of the requested report would create an undue burden and incur an unnecessary cost to the Company and shareholders. However, as this solicitation shows, existing privacy regulations may not be sufficient to minimize the privacy risks contemplated by the Proposal, and the requested report could be prepared at minimal cost.

[14] *See* Kelly D. Martin et al., *Data Privacy: Effects on Customer and Firm Performance*, 81.1 Journal of Marketing at 36-58 (2017), https://doi.org/10.1509/jm.15.0497.

Regulatory and legal compliance is insufficient to minimize privacy risks related to reproductive healthcare

Data privacy laws in the United States are considered by many experts to be lacking in scope and woefully outdated. In fact, there is no single, comprehensive federal law regulating how companies collect, store, or share customer data.

As the *New York Times* reports, "[t]he data collected by the vast majority of products people use every day isn't regulated."[15] In most states, companies can use, share, or sell most data they collect about consumers without notifying them that the company is doing so. There is no federal law standardizing when (or if) a company must notify consumers if their data is breached or exposed to unauthorized parties. If a company shares consumer data – including sensitive information such as an individual's health or location – with third parties (e.g., data brokers), those third parties can often sell the data or share it without notifying the affected consumers. HIPAA – one of the few federal privacy laws but which only protects PHI – has loopholes that could allow Labcorp to disclose information to law enforcement seeking to prosecute abortion-related crimes.

As a result of this lax regulatory environment, many businesses have implemented firmer privacy practices that more fully protect consumers from nefarious data uses and increase brand trust. One such practice is abiding by the principle of "data minimization," in which companies only collect personal data that is strictly necessary for delivering the service a user is expecting to receive, and use it for only that purpose.[16] Data minimization is already a legal requirement for certain companies doing business in the European Union.[17] As a result of data minimization, companies amass less information that may be subject to law enforcement information requests or shared with third parties seeking to participate in the enforcement of abortion-restrictive laws. Notably, data minimization would also reduce the Company's liability, reputational risk exposure, and storage costs.[18] Labcorp has nonetheless failed to disclose in its various privacy policies whether it abides by this principle.

Privacy experts further recommend that in order to protect consumers from being targets of abortion-related prosecutions, companies should employ data security measures such as data encryption, de-identification, and anonymization.[19] Encryption is the process of converting information or data into a code, especially to prevent unauthorized access. De-identification entails segregating personally identifiable data like names and addresses from PHI and other sensitive data that the company stores. Anonymization protects private or sensitive information by erasing identifiers that connect an individual to stored data.

---

[15] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[16] https://pirg.org/articles/do-you-know-where-your-data-is-because-facebook-doesnt/

[17] https://www.business.com/articles/how-to-apply-data-minimization/

[18] https://tinyurl.com/2p92fr8t

[19] https://www.securitymagazine.com/articles/98414-privacy-and-data-protection-in-the-wake-of-dobbs

While Labcorp applies some of these security measures to transactional data and before sharing HIPAA-covered PHI, it is unclear whether these measures could be applied to other consumer information contemplated in the Proposal such as data collected in its website. In fact, Ovia Health declined to answer questions on this issue as part of a popular news report on period-tracking apps after the revocation of abortion rights, to significant negative press.[20] Yet, sharing consumer data without proper security measures could expose the Company to significant risks, including the threat of burdensome litigation. In 2021, for example, the most popular fertility and period tracking app developer, Flo Health, faced legal action upon claims that the platform shared sensitive health information with third parties, including Google and Facebook, without the users' consent.[21]

Finally, most companies doing business in California, Virginia and the European Union are also required to provide consumers with "deletion rights," as contemplated by the Proposal.[22] Deletion rights generally grant consumers the ability to have personal information erased in instances where the business is not required to maintain the data. Implementing a sustainable data deletion program can help Labcorp reinforce its standards and governance for data deletion, meet regulatory requirements, reduce the risk of data breaches, and improve data hygiene overall.[23]

Since Labcorp already complies with data deletion requirements under California and Virginia law, applying deletion rights or other related data deletion mechanisms nationwide could be a feasible and cost-effective mitigation measure to the problems raised identified in the Proposal. Synalab Group, one of Labcorp's international competitors, automatically deletes or anonymizes a website visitor's IP address from the company data logs, while other remaining website-visitor data "is stored for a limited period of time" with the explicit purpose of improving the "operation of [Synalab's] website."[24] DaVita, a leading healthcare provider, gives consumers the opportunity to "amend or delete" information collected from them through the company's online platforms.[25] The requested report would advise investors whether such measures indeed provide such benefits to the Company.

---

[20] https://www.inverse.com/input/culture/period-tracking-apps-abortion-privacy-roe-v-wade

[21] https://tinyurl.com/2sduk56f

[22] https://oag.ca.gov/privacy/ccpa (California); https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ (Virginia); https://gdpr-info.eu/art-17-gdpr/ (European Union)

[23] https://www.grantthornton.com/insights/articles/advisory/2020/how-data-deletion-empowers-data-protection

[24] https://www.synlab.com/privacy-policy

[25] https://www.davita.com/privacy-policy

Production of the report would be feasible and cost-effective

While ignoring the substance of the Proposal, Labcorp focuses a substantial part of its opposition statement on the supposed undue burden and unnecessary costs associated with the preparation of the requested report.

The scope of research involved in the production of the requested report is narrow and limited to the risks associated with the Company's fulfillment of information requests relating to LabCorp customers for the enforcement of state laws criminalizing abortion access. The Proposal and a number of reports and studies have already identified many of the potential risks, thereby providing useful guidance that the Company may follow in preparing the requested report. Notably, the Proposal recommends the Company consult with reproductive rights and civil liberties organizations in preparing the report, which could reduce the burden of identifying relevant data privacy risks associated with criminal abortion laws.

Contrary to the Company's position, producing the requested report would *not* require the development and implementation of new processes and policies. Indeed, one of the purposes of the report is to study the feasibility and potential impact of any new processes and policies before they are implemented. Such an analysis would provide useful information to the Company and investors as to whether new or improved data handling practices could reduce material risks, in addition to potentially expanding the Company's customer base by positioning itself as a market leader in protecting consumer data. Despite massive investments in women's healthcare, the Company cannot expect to grow its business in that area without first ensuring that consumers will trust the Company's handling of their sensitive personal data in the face of restrictive criminal abortion laws.

Lastly, production of the requested report would be cost-effective and feasible. A similar shareholder proposal submitted to Interpublic Group Companies was withdrawn after that company conducted an assessment of their policies and practices regarding reproductive health data, ultimately finding there was no significant risk to customers in the face of newly-enacted state laws criminalizing abortion.[26] Conversely, the Company's explanation in its opposition statement as to why it would be difficult to examine the nature of the crime investigated as part of a government data request demonstrates that the Company could appropriately explore in the report the feasibility of mitigation measures that would minimize retention of data vulnerable to data requests and abortion-related prosecutions. We believe existing Labcorp counsel and technical experts, in consultation with outside experts and groups, could satisfy the request report analyzing, among other things, such mitigation measures without incurring substantial cost.

[26] https://tinyurl.com/mvrmfj2x

In sum, we believe that implementing the requested report will help ensure that Labcorp does more to monitor its data handling practices so that they do not expose consumers to serious risks stemming from abortion-related criminal prosecutions, thereby eroding shareholder value by diminishing the Company's reputation, consumer loyalty, brand, and values.

Vote "Yes" on Shareholder Proposal No. 7.

For questions, please contact Corporate.Engagement@rhiaventures.org.

The foregoing information should not be construed as investment advice.

ADDENDUM A:

Examples of harms from companies' sharing of reproductive health-related data with third parties without consumer consent

https://nebraskaexaminer.com/2022/08/10/facebook-data-used-to-prosecute-nebraska-mother-daughter-after-alleged-abortion/
In 2022, Meta complied with a data request from a local Nebraska police department for private Facebook messages between a mother and daughter, who were both subsequently charged with felony crimes related to the alleged illegal termination of the daughter's pregnancy.

https://scholarworks.law.ubalt.edu/cgi/viewcontent.cgi?article=2078&context=ublr
In 2017, a woman in Mississippi experienced an at-home pregnancy loss. A grand jury later indicted her for second-degree murder, based in part on her online search history, which recorded that she had looked up how to induce a miscarriage.

https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/
A 2019 report in *The Washington Post* revealed that pregnancy app Ovia Health sold user health data to their employers, without user consent.

https://www.leagle.com/decision/ininco20160722184
In 2013, a woman was sentenced to twenty years in prison for "neglect of a dependent and feticide" after taking abortion pills she purchased online. Evidence presented against her at trial included online research she conducted, the email confirmation she received from internationaldrugmart.com, and unencrypted text messages to a friend about her relationship, becoming pregnant, and the pills she purchased.

https://gizmodo.com/data-brokers-selling-pregnancy-roe-v-wade-abortion-1849148426
In 2022, *Gizmodo* identified 32 brokers selling data on 2.9 billion profiles of U.S. residents pegged as "actively pregnant" or "shopping for maternity products."

https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google
A 2023 investigation by *ProPublica* found online pharmacies that sell abortion medication such as mifepristone and misoprostol are sharing sensitive data (including users' web addresses, relative location, and search data) with Google and other third-party sites — which allows the data to be recoverable through law-enforcement requests.

https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

In 2022, the Federal Trade Commission sued Kochava – a data analysis platform primarily used by companies for marketing purposes – for selling data that tracks people at reproductive health clinics, places of worship, and other sensitive locations.

THE FOREGOING INFORMATION MAY BE DISSEMINATED TO SHAREHOLDERS VIA TELEPHONE, U.S. MAIL, E-MAIL, CERTAIN WEBSITES AND CERTAIN SOCIAL MEDIA VENUES, AND SHOULD NOT BE CONSTRUED AS INVESTMENT ADVICE OR AS A SOLICITATION OF AUTHORITY TO VOTE YOUR PROXY. THE COST OF DISSEMINATING THE FOREGOING INFORMATION TO SHAREHOLDERS IS BEING BORNE ENTIRELY BY THE FILER OF THIS SOLICITATION. PROXY CARDS WILL NOT BE ACCEPTED. PLEASE DO NOT SEND YOUR PROXY TO TARA HEALTH FOUNDATION. TO VOTE YOUR PROXY, PLEASE FOLLOW THE INSTRUCTIONS ON YOUR PROXY CARD.