1600 Amphitheatre Parkway
Mountain View, CA 94043

Tel: 650.253.0000
Fax: 650.253.0001

December 6, 2019

VIA EMAIL

Richard Blumenthal
United States Senator
706 Hart Senate Office Bldg.
Washington, DC, 20510

Elizabeth Warren
United States Senator
309 Hart Senate Office Building
Washington, DC 20510

Bill Cassidy, M.D.
United States Senator
520 Hart Senate Office Building
Washington, D.C. 20510

Re: Google's Response to Nov. 19th Letter

Dear Senators Blumenthal, Warren, and Cassidy,

Thank you for the letter sent by your offices on November 19, 2019.

We are proud to provide more details on Google's work supporting Ascension, one of the nation's leading non-profit health systems, with technology that helps them deliver better care to patients across the United States. Progress in healthcare over the past few decades has come with challenges of information overload that have taken doctors' and nurses' attention away from the patients they are called to serve. We believe technology has a major role to play in reversing this trend, while also improving how care is delivered in ways that can save lives.

There has been a good deal of speculation about our partnership, and we want to ensure that you have the facts. Google and Ascension entered into agreements beginning in August 2018, in which Google was engaged to provide services and support to Ascension in three key areas, all of which are covered by the business associate agreement ("BAA") between Ascension and Google. First, Google was engaged to help modernize Ascension's data infrastructure, which involves migrating data to a private and secure Google Cloud environment. Second, Ascension was provided with G Suite productivity tools, including Gmail, Google Drive, Google Docs, and other applications that enable employees to communicate and collaborate securely and in real time, across Ascension sites of care. These services are provided to many organizations, including other health systems. Customers are responsible for identifying when these services

1600 Amphitheatre Parkway
Mountain View, CA 94043

Google

Tel: 650.253.0000
Fax: 650.253.0001

will involve protected health information ("PHI"). When they do, Google and the customer enter into a BAA as required by HIPAA.

Finally, Ascension and Google initiated a service offering that would involve the provision of tools that Ascension could use to support improvements in clinical quality and patient safety. This included the initial pilot for "EHR search" that would pull patient electronic health records ("EHRs") into a single, easy-to-use interface and provide Ascension doctors and other medical professionals with tools to make the records more useful, in part by improving the search function. We understand that the primary concerns have been about the EHR search pilot. Therefore, unless otherwise specified, the responses below focus on the Ascension EHR search pilot program.

We hope this overview, together with our attached responses to your specific questions, will address your concerns. However, if you would like to discuss further, please let us know.

Very truly yours,

David Feinberg, MD
Head of Google Health
Google LLC

1. **Please list all health systems, providers, insurers, or any other entity for which Google provides services related to electronic medical records**

   Google works with dozens of other healthcare providers. These organizations use our technology to help them organize their healthcare data and make this crucial information useful and secure. Our CLOUD healthcare customers site includes more details and a list of healthcare customers using Google Cloud services.

   Ascension is the initial health system involved in the EHR search pilot program. EHR search will enable doctors to access a unified view of patient data that is typically spread across multiple EHR systems. The EHR search tool being used in the pilot program allows doctors and nurses to more quickly and effectively query a medical record using words and abbreviations commonly used by health care providers and to receive results in a useful format from records stored in different types of EHR systems.

   a. Does Google have any agreements with these entities under which personal health information is provided to Google? If so, please list and describe all such agreements.

   For the EHR search pilot, patient information from electronic medical records are migrated to Ascension's secure Google cloud storage under a BAA, and access to PHI is provided to designated Google employees for purposes of providing EHR search-related services to Ascension.

2. **Are Ascension patients provided notice of Google's retention and use of electronic medical records?**

   As Ascension's business associate, Google retains and uses EHR data as permitted by Ascension in order to provide services, and in accordance with its BAA and the HIPAA regulations. We understand that providing notice to patients of uses and retention of PHI by a covered entity and its business associates is the responsibility of the covered entity.

3. **Will Ascension patients be provided the ability to opt out of the use of their health information for what is medically or operationally necessary to provide patient care? Has Google affirmatively sought permission from patients for any use of this data?**

   HIPAA permits health care providers to disclose patient information to their service providers as long as the protections of a BAA are in place and only the minimum necessary information is disclosed to the service provider. Patients do not opt in or out of having their doctor share their information with a billing service or store their information in an electronic health record hosted by a trusted third party. Allowing patients to opt in or opt out of the electronic health record, or to opt out of having their records stored in a secure cloud, would put doctors and nurses in the difficult position of navigating different channels and systems to locate a patient's record in ways that could negatively impact patient care and endanger patient safety. Although patients typically cannot opt out of permitted disclosures made by their health care providers to business associate service providers, HIPAA privacy and security obligations follow the patient records to business associates. Among other protections, business associates like Google are bound by

the HIPAA security rule and can receive only the minimum necessary information needed to provide services to the health system.

4. **Did Google's agreement with Ascension allow Google to perform research or analysis of patient data outside the direct scope of what was medically or operationally necessary to provide patient care? Would genetic information be included? Please list all planned or considered research or analysis.**

   Google is required by its BAA with Ascension to use Ascension's PHI only to provide services to Ascension and for purposes permitted or required by the BAA. This does not include research or analysis outside services provided for Ascension.

5. **Is Google using or intending to use this data for targeting individuals with advertisements? Is Google using or intending to use this data to identify services that would be targeted at specific individuals?**

   No.

6. **What procedures are in place that govern Google's use of health information from Ascension for research or analysis? Who is responsible for approving such research?**

   Google is required by its BAA with Ascension to use Ascension's PHI only to provide services to Ascension and for purposes permitted or required by the BAA. This does not include research or analysis outside services provided for Ascension.

7. **Is Google permitted to use information (aside from patient records) derived from Project Nightingale, such as machine learning models built from patient data, for contracts with other health providers and for other business purposes?**

   Google develops, builds, and validates the health-related algorithms and machine learning models used in products such as EHR Search using synthetic data, de-identified data, or data obtained for research uses in accordance with Institutional Review Board approved protocols and waivers. Google developed and validated the EHR Search tool prior to the pilot with Ascension and independent of Ascension data. Ascension PHI is used to provide services offered under the agreement, and patient data is not combined with any Google consumer data. PHI is not incorporated into the underlying algorithms and machine-learning models in the EHR Search tool and future use of the tool with other customers would not include underlying Ascension PHI.

8. **Are all products and services, including the versions used in Project Nightingale, compliant with HIPAA?**

   Google's work with Ascension is designed to adhere to industry-wide regulations, including HIPAA. We support HIPAA compliance for certain Google products and services offered under a BAA. Google has entered into a BAA with Ascension, and the services provided to Ascension subject to the BAA are also intended to support Ascension's HIPAA compliance efforts.

9. **Do Google employees have direct access to the electronic medical records from Ascension? How many Google employees and which divisions of Google have access to**

patient data? Under what conditions can Google employees access Ascension data? Could a Google employee theoretically see the patient data of an acquaintance?

Google employees who have been specifically approved by Ascension can access PHI as part of the EHR search pilot program. The complexity and lack of standardization of medical data within EHR systems is one of the significant barriers Ascension is trying to overcome in order to make data useful and available to clinicians. Google employees access PHI as part of configuring and tuning the processing systems to ensure that data is being sorted and displayed in an accurate, safe and useful way for clinicians.

Before Google employees can access Ascension medical record data as part of the EHR search pilot program, they must be individually approved by Ascension.

10. **When did Google begin obtaining personal health information from Ascension?**

    We signed a BAA with Ascension in August 2018. Covered entities like Ascension are not permitted to utilize Google's services in connection with their PHI unless they enter into such a BAA. Ascension will have insight into when it began utilizing Google's services in connection with its PHI.

11. **What are the terms and conditions of the contract between Google and Ascension? Specifically**

    a. **Is Google paying Ascension for this data or any services related to this data, and if so, how much?**

       All services are provided as part of proprietary, commercial contracts with Ascension. Google is not paying Ascension for this data and Google can only use the data as necessary for the provision of services to Ascension and for purposes permitted or required by the BAA.

    b. **What specific uses of the data by Google are allowed under the contract?**

       For the EHR search pilot program, Ascension is working with Google to pilot tools to enable Ascension's doctors and nurses to more quickly and easily access relevant patient information, in a view that consolidates medical records about a patient stored in different locations and systems within Ascension. In accordance with HIPAA and the BAA, patient data cannot be used by Google for any purposes other than to provide services to Ascension and for purposes permitted or required by the BAA.

    c. **Could Google combine Ascension data with individual search and location data to create and leverage bolstered individual profiles?**

       No. Google is not permitted under its BAA with Ascension to combine Ascension PHI with individual search or location data.

    d. **Does the contract prevent or restrict Ascension from disclosing the data sharing agreement, or providing patients with information indicating that their health information will be shared?**

Google understands that Ascension has disclosed the existence of the services agreement and provided a Notice of Privacy Practices describing how its patients' information will be shared.

12. **What is the full and complete list of patient-level information that Google is receiving from Ascension?**

    Ascension will have insight into the details of the individual health records provided to Google.

13. **How many individuals' health records has Google received under "Project Nightingale?"**

    Ascension will have insight into the number of individual health records provided to Google.

14. **How is Google protecting the information it is receiving from Ascension? Is the information encrypted? Is the data stripped of any information that could be used to identify patients, either independently or with any additional information that Google may have already collected through its other services?**

    Google approaches its Cloud Platform products with numerous administrative, technical, and physical safeguards.

    - Google implements restrictions to data access. For example, Google logically isolates each customer's data from that of other customers and users. Only a limited group of Google employees has access to customer data. Further, Google employees' access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities.
    - From an operational standpoint, Google (1) administers a vulnerability management process that actively scans for security threats; (2) has a security monitoring program focused on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities; (3) uses a variety of methods to prevent, detect, and eradicate malware in order to prevent malware attacks; and (4) maintains a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data.
    - Google has also custom-designed its servers, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," Google has created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

    With respect to Ascension data, Google utilizes those same administrative, technical, and physical safeguards to protect the information maintained on behalf of Ascension:

    - To keep data private and secure, Google logically isolates Ascension's data from that of other customers and users.
    - Approvals for roles granting access to Ascension data are managed by workflow tools that maintain audit records of changes. These tools control both the modification of

authorization settings and the approval process to ensure consistent application of the approval policies.

- Further, the Google systems and infrastructure that support the cloud-based services being provided to Ascension are subject to periodic security testing and audits against industry-standard security frameworks such as ISO 27001.

In addition, patient data in the EHR search pilot is accessible only in a strictly controlled environment with audit trails:

1. Data is isolated in a virtual private space and encrypted.
2. Access to patient data is stored, monitored and auditable.
3. Access is restricted to specific individuals approved by Ascension.
4. Binaries are cryptographically verified to contain only code that was checked into Google's code repository and explicitly reviewed by other engineers – no engineer may unilaterally modify code. There is thus a trail of the exact code of any software than ran against this data.

15. Has there been any breach or attempted breach that would present a risk of any outside party obtaining access to personal health information?

To our knowledge, there has not been a breach or attempted breach that would present a risk of any outside party obtaining access to PHI.

16. Has Google shared any personal or aggregated health information obtained via the Ascension agreement with any other third party? If so, please list and describe all such instances of sharing data.

Google has not shared such Ascension information with any third party beyond its workforce. If Google engages a third party beyond its workforce to provide services to Ascension and the third party requires access to PHI from Ascension, then Google enters into a subcontractor BAA with the party requiring them to safeguard the information in accordance with applicable HIPAA regulations.

17. Has Google informed any federal or state regulators of its agreement with Ascension and any potential uses for the health information that it is collecting?

We are happy to cooperate with any questions about the EHR search pilot program.