United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

May 21, 2026

VIA ELECTRONIC TRANSMISSION

Andrew Dudum
Chief Executive Officer
Hims & Hers
2269 Chesnut Street #523
San Francisco, CA 94123

Dear Mr. Dudum:

Cybersecurity threats are one of the most significant risks currently affecting the health care system. In 2025, there were 628 reported health care data breaches, resulting in delayed care, patient data stolen or accessed without authorization, and a potential for increased fraud.[1] At a time when hostile actors are increasingly using sophisticated tactics leveraging artificial intelligence, it is essential for the health care sector to take meaningful steps to safeguard patient and consumer information.

The recent cybersecurity incident affecting Hims & Hers highlights the risk cybersecurity incidents pose to patients. While Hims & Hers has stated that "customer medical records were not impacted by this incident," additional transparency is needed about what information hostile actors accessed, how Hims & Hers safeguarded protected health information (PHI) prior to the incident, and steps that the company intends to take going forward.[2] To that end, I request answers to the following questions by June 8, 2026:

1. What security protocols, both cyber and physical, does Hims & Hers have in place to protect against a cyberattack?

2. How does Hims & Hers incorporate cybersecurity best practices implemented by other critical infrastructure sectors?

[1] Steve Alder, *Healthcare Data Breach Statistics*, The HIPAA Journal (Jan. 4, 2026), https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[2] *Notice of Data Event*, Hims & Hers (Apr. 2, 2026), https://oag.ca.gov/system/files/Hims%20%26%20Hers%2C%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20CA_0.pdf.

3. When did Hims & Hers first become aware of a cyber incident affecting its systems?

4. When did Hims & Hers notify federal agencies of a cyber incident, and which agencies did Hims & Hers notify?

5. Hims & Hers has stated that "personal information related to a limited set of individuals" may have been accessed without authorization.[3]
    a. What information was contained in this dataset?
    b. What steps is Hims & Hers taking to identify any additional information that may have been accessed?
    c. How is Hims & Hers proactively communicating with potentially impacted individuals and entities?

6. What remedial steps has Hims & Hers taken or intend to take to improve its security protocols?

7. What additional reporting does Hims & Hers commit to doing for individuals who have had their information disclosed, beyond the reporting requirements under the Health Insurance Portability and Accountability Act (HIPAA)?

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Chairman
U.S. Senate Committee on Health,
Education, Labor, and Pensions

[3] *Id.*