\_\_\_\_\_\_, 2022

**Address**

To Whom It May Concern:

We represent South Shore Hospital Corporation (“SSH”) with respect to a data security incident involving potential exposure of certain personally identifiable information (“PII”) and Protected Health Information (“PHI”) described in more detail below. SSH is a not-for-profit community hospital in Chicago, Illinois. SSH is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

**1. Nature of security incident.**

On December 10th, 2021, SSH detected a security incident impacting access to its systems. SSH immediately disconnected all system from external access, implemented its incident response protocols, and notified law enforcement. SSH also engaged external cybersecurity experts to conduct a forensic investigation to determine how the incident occurred and what information may have been impacted.

The investigation is now complete and SSH has determined that past and current employee information and patient information may have been compromised as part of this incident. The investigation determined that the files impacted may have contained first and last names, addresses, dates of birth, Social Security numbers, financial information, health insurance information, medical information, diagnoses, driver’s license information, health insurance policy numbers, and Medicare/Medicaid information for some employees and some patients.

**2. Number of residents affected.**

[Number (#)] of [state] residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on [date] (a copy of the form notification letter is enclosed as Exhibit A).

**3. Steps taken in response to the incident.**

SSH took steps to address this incident and to prevent similar incidents in the future, including implementing additional security controls to protect its network. These steps include enforcing stronger password requirements, enabling multifactor authentication, and additional data privacy and security awareness trainings for SSH’s workforce. SSH has also deployed supplementary anti-malware and email phishing tools and will continue to evaluate its security protocols for opportunities to further bolster its network security.

On February 7th, 2022, SSH provided substitute notice on its website and media notice to two major Chicago news outlets. As part of this initial notice, affected individuals were offered [12/24 months] of credit monitoring and identity protection services through IDX. Subsequently, once SSH identified specific individuals that were impacted as part of this incident, SSH followed up with individual notices to the affected individuals on [insert date]. Notice was also provided to the Department of Health and Human Services Office of Civil Rights on February 7th, 2022.

**4. Contact information.**

SSH takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at [jschwent@clarkhill.com](mailto:jschwent@clarkhill.com).

Sincerely,

Clark Hill

Jason Schwent

Senior Counsel

cc: Daisy Dai [ddai@clarkhill.com](mailto:ddai@clarkhill.com)