Jennifer Archie
Direct Dial: 202-637-2205
jennifer.archie@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

LATHAM & WATKINS LLP

August 25, 2023

VIA MAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

Re: **Notice of Data Security Incident**

Dear Attorney General:

I am writing on behalf of HCA Healthcare (the "Company") to provide courtesy notice of ongoing Health Insurance Portability and Accountability Act of 1996 ("HIPAA") mailings to residents of Iowa, relative to a previously announced data incident. This incident involved limited fields of personal information, such as name, city, state (but not address), email address, date of birth, service location and date, but not medical records or sensitive data such as passwords, financial data, or identifiers such as social security number or driver's license.

The Company first announced this incident by press release on the morning of July 10, 2023, shortly after learning that the relevant list of information was being made available on an online forum. All persons on the list in question were immediately notified by email, and again by the ongoing hard copy letters, which provide access to identity protection and credit monitoring services, notwithstanding the limited nature of the exposed data.

In addition to the press release, which received wide national and local media coverage, the Company has engaged in a sustained campaign to inform impacted patients about this incident, including:

- Messages to email addresses on the list, starting on July 14, 2023, a copy of which is enclosed as Appendix A.
- Providing legal notice to the US Department of Health and Human Services on July 31, 2023 due to size of breach exceeding 500 individuals.
- On a rolling basis, including to Iowa this week, mailing letters under HIPAA, in the form of Appendix B.

- Publishing substitute notice on its website[1] and media notice via PR Newswire[2] on August 14, 2023.

Further information is available at https://hcahealthcare.com/about/privacy-update.dot.

If your office requires any further information regarding this matter, please contact me at (202) 637-2205 or jennifer.archie@lw.com.

Respectfully submitted,

Jennifer C. Archie
Of LATHAM & WATKINS LLP

Enclosures

[1] *See* HCA Healthcare, HCA Healthcare Provides Substitute Notice to Certain Patients about a Previously Disclosed Data Security Incident (Aug. 14, 2023), https://hcahealthcare.com/about/privacy-update.dot

[2] *See* PR Newswire, HCA Healthcare Provides Substitute Notice to Certain Patients about a Previously Disclosed Data Security Incident (Aug. 14, 2023), https://www.prnewswire.com/news-releases/hca-healthcare-provides-substitute-notice-to-certain-patients-about-a-previously-disclosed-data-security-incident-301899374.html

Appendix A

On Monday, July 10, 2023, we announced that a list of certain information with respect to some of our patients was made available by an unknown and unauthorized party on an online forum. The list includes:

- *patient name, city, state, and zip code;*
- *patient email, telephone number, date of birth, gender; and*
- *patient service date, location and next appointment date.*

*Importantly, the list **does not include:***

- *clinical information, such as treatment, diagnosis, or condition;*
- *payment information, such as credit card or account numbers;*
- *sensitive information, such as passwords, driver's license or social security numbers.*

Additional information about the data security incident can be found at hcahealthcare.com/privacyupdate.

We remain committed to protecting the personal information that is entrusted to us. Because patient contact information was involved in this incident, we encourage you to remain vigilant about any suspicious or unexpected communications from an unfamiliar source or from anyone claiming to be affiliated with HCA Healthcare. ***You can call us at 888-993-0010 beginning Monday July 17, 2023.*** *Representatives will be available to provide assistance Monday through Friday 8 am – 8 pm Central Time. Specifically, if you receive any communication regarding an invoice, outstanding balance, or payment reminder that you were not expecting or believe to be fraudulent, please contact us so that we can confirm the legitimacy of the message.*

We are working as quickly as possible to identify and contact employees and patients whose data was impacted by this data security incident. Those individuals can expect to receive a mailed notification letter in the coming weeks and will be offered complimentary credit monitoring and identity protection services.

Again, we cannot express how instrumental your dedication and understanding have been and we appreciate your patience as we continue to work through the complexities of the event.

Sincerely,
Kathi Whalen
SVP, Ethics and Compliance
HCA Healthcare

Appendix B

HCA Healthcare

PO Box 480149
Niles, IL 60714

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We are writing to provide you, or your parent, guardian or guarantor, with information about a recent cybersecurity incident involving your personal information. We wanted to share some details and offer you some resources that you may find helpful. Please note the section titled "What You Can Do" below.

Who is HCA Healthcare? HCA Healthcare is one of the country's leading providers of healthcare services and through its affiliates operates 180 hospitals and 2,300+ sites across 20 states and the United Kingdom. Our records indicate that you received care at one or more HCA Healthcare-affiliated facilities or physician offices. For a list of facilities and physician offices that are or were previously affiliated with HCA Healthcare and may have been affected by this incident, please visit https://hcahealthcare.com/about/privacy-update.dot. For more information, you may also call the toll-free number below.

What Happened? On or around July 5, 2023, HCA Healthcare discovered that a list of certain information with respect to some of its patients was made available on an online platform by an unauthorized party. Preliminary investigation suggests the information was obtained by the unauthorized party in late June in what appears to be a theft from an external storage location exclusively used to automate the formatting of email messages, such as reminders that patients may wish to schedule an appointment and education on healthcare programs and services. This incident has caused no disruption to the care and services HCA Healthcare affiliates provide to patients and communities.

What Information is Involved? Our review determined that the exposed files contained some of your personal information, including your name, city, state, zip code, email, telephone number, date of birth, gender, service date, location and, in some instances, the date of next appointment. Importantly, the exposed personal information does ***not*** include clinical information, such as treatment, diagnosis, or condition; or payment information, such as credit card or account numbers; or other sensitive information, such as passwords, government-issued ID numbers, or social security numbers.

What Are We Doing? Upon discovery, we disabled user access to the aforementioned storage location as an immediate containment measure. HCA Healthcare also reported this event to law enforcement and retained third-party forensic and threat intelligence advisors to investigate the incident. Additionally, HCA Healthcare has various security strategies, systems, and protocols already in place, which are being reviewed to identify any enhancement opportunities.

What You Can Do. It is always good practice to be vigilant against identity theft and fraud by reviewing your account statements and monitoring any available credit reports for unauthorized or suspicious activity, and by taking care in response to any email, telephone or other contacts that ask for personal or sensitive information (e.g., phishing). HCA Healthcare will never request sensitive information by phone or email. We encourage you to remain vigilant in identifying calls, emails or SMS texts which appear to be spam or fraudulent. Additionally, you should never open links or attachments sent from untrusted sources. You may also review the attached *Steps You Can Take to Help Protect Your Information* as a helpful resource.

We are also providing complimentary credit monitoring and identity protection services for 2 years via IDX. These services include credit monitoring, a $1,000,000 insurance reimbursement policy and full managed identity restoration in the event that you fall victim to identity theft, and dark web monitoring to monitor if your data appears in illicit online forums. To activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Your Information.*

For More Information. For further information, please call 1-888-993-0010, Monday to Friday from 8 am – 8 pm Central Time.

Sincerely,

Ethics and Compliance Department
HCA Healthcare

Steps You Can Take to Help Protect Your Information

Enroll in IDX Credit Monitoring and Identity Protection Services

Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is <<Date>>.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file with the credit reporting bureau. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

If you discover any suspicious items on your credit reports or from the fraud alert and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, free of charge, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency filed by you concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 888-743-0023.

For North Carolina residents, the North Carolina Attorney General can be contacted at Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, www.ag.iowa.gov, 515-281-5926 or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, www.dog.state.or.us, 503-378-6002.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfurt, KY 40601, www.ag.ky.gov, 502-696-5300.

For Massachusetts residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance .gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.