BREACH AT DSH-COALINGA

FAQ

1. What happened?

ANSWER: On August 12, 2021, DSH discovered that a DSH-Coalinga (DSH-C) employee had been providing DSH-C patient rosters to the United States District Court, Eastern District of California (the District Court) at the request of the District Court so that the District Court Clerk could determine whether patients were eligible for a waiver of their filing fees when filing a lawsuit. The roster contained patient names, case numbers, birth dates, legal commitment, admission dates, unit numbers, and gender. Although the information in the roster contained more information than was needed, including information regarding patients who never filed any lawsuits, there is no evidence that the information on the roster was used for any purpose apart from the District Court clerk making an eligibility determination for a public benefit administered by the Court.

2. How was the data breach discovered?

ANSWER: The breach was discovered on August 12, 2021, when the Privacy Officer was apprised by a DSH-C employee of an email from the District Court Operations Supervisor, requesting an updated roster.

3. What kind of information was accessed?

ANSWER: The DSH-C rosters provided to the District Court contained names, case numbers, birthdates, legal commitments, admission dates, unit numbers, and genders, of individuals who were DSH-C patients on July 21, 2013, October 12, 2016, and August 27, 2019.

4. Did the data breach happen on the same day that you learned about it? If not, when did it happen?

ANSWER: The breach did not occur on the date it was discovered. Based on the investigation, the DSH-C rosters were provided to the courts on July 21, 2013, October 12, 2016, and August 28, 2019.

5. How would I know if my information was accessed?

ANSWER: If your information was accessed you would have been notified by DSH via a Notice of Data Breach letter. The next of kin or personal representatives of deceased patients were notified by first-class mail if their address is known to DSH. If you did not receive a Notice of Data Breach letter, but were a patient at DSH-C on July 21, 2013, October 12, 2016, or August 28, 2019, please call (833) 573-2641, or send an email to DSHCSHPrivacyOfficer@dsh.ca.gov.

6. If my information was accessed, what should I do?

ANSWER: Keep a copy of the Notice of Data Breach letter for your records in case there are future problems with your medical records. You may also want to request a copy of your medical records from DSH-C, to serve as a baseline by submitting the DSH 6406 form to your treatment team. If you are no longer a patient at DSH-C, you may mail the form to the Health Information Management Department, Department of State Hospitals – Coalinga, PO Box 5000, Coalinga, CA 93210.

If you have additional questions about this breach, please call (833) 573-2641, or visit the DSH homepage at www.dsh.ca.gov and click on the data breach link. DSH's website will have this notice along with a copy of Frequently Asked Questions, which is also enclosed with this Notice. You may also e-mail us with questions at DSHCSHPrivacyOfficer@dsh.ca.gov. Please do not include your social security number or medical information in an e-mail to DSH.

For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at https://oag.ca.gov/privacy.

You may also contact your Patients' Rights Advocate, Jodie Keasler, at (559) 934-3861, or the Patients' Rights Assistant, Garrett Stipe, at (559) 476-2027.

7. What was done with the accessed information?

ANSWER: The DSH-C patient roster was used by the District Court Clerk to determine whether patients were eligible for a waiver of their filing fees when they file a lawsuit in District Court. There is no evidence that the information in the patient roster has been used for any purpose apart from the District Court Clerk providing a public benefit to which DSH-C patients may be entitled to by the District Court.

8. Is it possible that more information was accessed than you know about right now? When will you know?

ANSWER: DSH continues to seek more information about the extent of the data breach. If it is determined that more information was accessed than what was provided in the Notice of Data Breach letter, another notification will be provided to the effected individuals within 15 business days of the discovery that more information was accessed.

9. Who was responsible?

ANSWER: The DSH-C roster was shared by a DSH-C employee whose job duties included working with the courts to ensure the DSH-C patients had appropriate court orders in place.

10. Is the person who did it still working at DSH?

ANSWER: The individual who shared the DSH-C roster is no longer working at DSH.

11. Was the data breach intentional?

ANSWER: The individual who shared the DSH-C roster intended to provide the District Court with information so that the Court Clerk can determine patients' eligibility for the public benefit of filing fee waivers.

12. Do you know why someone did this?

ANSWER: The individual who shared the DSH-C roster intended to help the District Court determine patients' eligibility for the public benefit of filing fee waivers and did not realize that it was not permitted.

13. Why didn't you tell us about this sooner?

ANSWER: DSH was not aware that the DSH-C employee had been providing the District Court with the DSH-C patient roster until the Court Clerk emailed requesting an updated DSH-C roster.

14. How often does DSH look for data breaches?

ANSWER: The DSH Privacy and Security Programs review, investigate, and analyze privacy incidents on a daily basis for potential data breaches pursuant to its information and systems and access rights policy and procedure and incident response plan.

15. Is the search for data breaches automated, manual or something else?

ANSWER: The search for data breaches is both an automated and manual process. DSH employs automated Data Loss Prevention techniques in an effort to eliminate data being transmitted externally from the Department. A manual process for detection is also utilized, as many DSH employees require access to confidential data as a normal part of their jobs, including copying and moving data between systems internally.

16. Is there a policy for looking for data breaches and, if so, was it followed?

ANSWER: DSH has a Privacy and Security incident response plan that was followed in this incident.

17. What are you doing to make sure that this doesn't happen again?

ANSWER: The DSH Privacy and Security Programs provide annual Privacy and Security Awareness Trainings to all of its employees, along with targeted trainings and education and awareness reminders, as needed to its employees throughout the year. The detection of this breach is evidence that these trainings are working, as the employee who received the request for an updated DSH-C roster was able to recognize that the District Court should not be provided with all the information contained in the DSH-C roster. Additionally, any procedures the staff follow

regarding patient records will be reviewed and revised to provide DSH staff with further clarity, education, and awareness regarding data protection.

18. Who has been notified about the breach?

ANSWER: In addition to the notifications provided to impacted patients and former patients, the breach is being reported to the United States Health and Human Services, Office of Civil Rights, the California Office of Information Security, the California Office of Health Information Integrity, the California Highway Patrol, the California Department of Public Health, and the California Attorney General's Office.