

October 8, 2020

ATTORNEY GENERAL RAOUL ANNOUNCES \$5 MILLION SETTLEMENT WITH COMMUNITY HEALTH SYSTEMS FOR DATA BREACH

Data Breach Compromised More Than 339,000 Illinois Patients' Personal Information

Chicago — Attorney General Kwame Raoul today announced a \$5 million settlement with Community Health Systems Inc. (CHS) resulting from a 2014 data breach that impacted approximately 6.1 million patients nationwide. Attorney General Raoul, along with Tennessee Attorney General Herbert Slatery III and Texas Attorney General Ken Paxton, led a bipartisan coalition of 28 states that reached the settlement with CHS and its subsidiary, CHSPSC LLC.

In 2014, CHS confirmed that its computer network was the target of an external cyber attack that allowed hackers to gain access to patient names, birthdates, Social Security numbers, phone numbers and addresses. More than 339,000 impacted patients were Illinois residents. Raoul [filed a lawsuit](#) and [a settlement today](#) requiring CHS to pay states \$5 million, more than \$611,000 of which will go to Illinois. CHS has also agreed to implement and maintain a comprehensive information security program to safeguard personal information and implement policies to quickly identify and address future breaches.

"When patients provide sensitive personal information such as Social Security numbers and birthdates, they are trusting that it will be kept safe and confidential," Raoul said. "This settlement requires CHS to enact procedures to better protect patients' information, and to develop plans to react quickly if another breach occurs. I will continue working to hold companies responsible for not doing enough to protect consumers' personal information from data breaches."

The settlement requires CHS to take a number of steps to prevent future breaches, such as developing an incident plan so that the company will know what to do if a breach occurs. The settlement also requires CHS to employ additional policies to protect sensitive patient information, such as:

- Developing and implementing a written information security program.
- Developing a plan to ensure that any needed software patches are detected and applied in a timely manner to avoid allowing security gaps.
- Maintaining strict control over access to CHS' accounts and network, and implementing measures such as multi-factor authentication to limit access only to authorized individuals.
- Providing regular security and privacy training for all employees who handle or come into contact with sensitive patient data.
- Developing and maintaining policies and procedures to encrypt sensitive data when appropriate.
- Conducting an annual risk assessment of the CHS network, and developing a plan for addressing those risks and protecting data.
- Requiring any third-party companies that provide services to CHS involving the handling or storage of sensitive patient data to agree to take certain precautions to protect the data.
- Implementing and maintaining policies to track and protect all company computers, phones and other devices that have access to or transmit sensitive patient data.
- Engaging a third-party assessor to evaluate CHS' compliance with the terms of the judgment and the handling of sensitive patient data.

Privacy Unit Chief Matt Van Hise, Consumer Fraud Bureau Chief Beth Blackston, and Assistant Attorneys General Carolyn Friedman and Ronak Shah handled the settlement for Raoul's Consumer Fraud Bureau.

Joining Attorneys General Raoul, Slatery and Paxton in today's settlement are the attorneys general of Alaska, Arkansas, Connecticut, Florida, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Michigan, Mississippi, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Utah, Vermont, Washington and West Virginia.