NEWS RELEASE

Attorney General Mike Hilgers

FOR IMMEDIATE RELEASE
December 16, 2024

Attorney General Mike Hilgers Files Lawsuit Against Change Healthcare for Critical Failures to Protect Consumer Data and Prevent Against Harm from a Widespread Cyberattack

Lincoln—Today, Attorney General Mike Hilgers filed a major lawsuit in Lancaster County District Court against Change Healthcare alleging violations of Nebraska's Consumer Protection and Data Security Laws.

The complaint stems from a catastrophic data breach and subsequent operational shutdown that exposed the personal and electronic protected health information of what the Attorney General's Office believes to be at least hundreds of thousands of Nebraskans, if not over a million. The data stolen includes some of the most sensitive information about a person, including information reflecting medical diagnoses. The shutdown also disrupted critical healthcare services across the state. The lawsuit claims that the defendants' failure to implement proper security measures exacerbated the data breach, leaving healthcare providers unable to deliver timely care and placing Nebraskans' most sensitive information at risk.

"This data breach is historic. Not only because it compromised the most sensitive privacy and financial data of Nebraskans, but also because it shut down the payment and claim processing systems that form a significant part of the backbone of the medical payment processing industry," said Attorney General Hilgers. "Healthcare providers, including critical access hospitals in rural areas, have unfairly been forced to absorb financial pain, forcing major cash flow issues and, in some cases, delayed services. And to make matters worse, Change has woefully disregarded the duty to provide notice to Nebraskans, depriving them of a fighting chance to be prepared for possible scams and fraud. We're filing this suit to hold Change accountable."

The Attorney General's lawsuit highlights systematic failures by including:

- **Outdated and poorly segmented IT systems** that failed to meet basic enterprise security standards.
- **Inadequate response to the breach,** including the failure to detect unauthorized access for over a week, allowing hackers to establish themselves unnoticed inside Change's systems. This allowed hackers to access personal data and protected health information.

- **Delays in notifying consumers of the breach**, with affected Nebraskans only beginning to receive notifications nearly five months after the breach was discovered.
- **Widespread operational disruptions** that halted prior authorizations for medical care and prescriptions, leaving patients without necessary medications and treatments.
- **Financial and operational burdens** placed on healthcare providers, such as Nebraska hospitals, pharmacies, and doctors' offices.
- **Significant harm to Nebraska patients**, including the potential for identity theft, financial fraud, and exploitation of personal health information.

The Change Healthcare data breach began on February 11, 2024, when the username and password of a low-level customer support employee were posted in a Telegram group chat notorious for selling stolen credentials. Using these credentials, a hacker accessed Change's systems through a remote access service called Citrix. For over nine days, the hacker navigated Change's systems undetected, creating privileged administrator accounts, installing malware, and exfiltrating terabytes of sensitive data.

The stolen data included Social Security numbers, driver's license numbers, health insurance information, medical records, billing details, and more. Defendants failed to detect this activity until February 21, 2024, when the hacker deployed ransomware, crippling Change's systems. In response, Change took its systems offline, effectively shutting down its operations and exacerbating the harm.

The breach caused widespread disruption to Nebraska's healthcare system, particularly affecting rural hospitals and critical access facilities operating on already thin margins. Providers were forced to deliver care without receiving payment for insurance claims, while others incurred significant costs switching to new transaction clearinghouses. Patients faced delays in receiving medications and treatments, while their sensitive information remained vulnerable on the dark web.

The Attorney General was involved shortly after receiving notice of the breach, and its work culminated in this lawsuit. The complaint seeks to hold Change accountable for their failures to implement basic security protections, which exacerbated the extent of the cyberattack. The Attorney General's Office asks the Court to order the companies to implement stronger data security measures and to pay damages and penalties for the harm caused to Nebraska residents and healthcare providers.

The Attorney General's Office is also calling on Nebraska healthcare providers who may have been affected by this cyberattack to come forward. Providers can submit their contact to the Nebraska Attorney General's Office at ProtectTheGoodLife.Nebraska.gov.

"A functioning medical marketplace needs to have a trustworthy medical payments backbone. It requires companies who do what they say they will do, and do everything possible to protect Nebraska's health information and who provide proper notice to Nebraskans when their data is breached. This suit is intended to

help restore trust in our system and remedy the harm suffered by Nebraskans and their medical providers." said Attorney General Hilgers.

###

Court Filing Attached

Suzanne Gage
Director of Communications
Nebraska Attorney General's Office
Office: 402-471-2656
Mobile: 402-560-3518
Suzanne.gage@nebraska.gov