

Traceability becomes the new battleground in healthcare data breach litigation

By Abbye Alexander, Esq., Henry Norwood, Esq., and Emily Taing, Esq., Kaufman Dolowich LLP

OCTOBER 27, 2026

Recent caselaw suggests a shift in how courts analyze healthcare data breach claims.

For years, defendants largely prevailed by arguing that plaintiffs could not demonstrate a sufficiently concrete injury because plaintiffs' private information had not been misused following a data breach or because the alleged future harm was overly speculative (such as hackers *may* misuse their personal health information in the future).

Recent decisions suggest that disputes over standing in healthcare data breach litigation are shifting.

Despite the judicial willingness to recognize concrete injuries from cyber incidents, plaintiffs increasingly face dismissal over failure to establish causation.

While courts have become more receptive to claims involving actual misuse of compromised information, they are closely scrutinizing whether the alleged harm can be tied to the specific breach. The central question is at what point the exposure of medical information becomes a legally cognizable injury.

Recent decisions have recognized standing in healthcare data breach cases when plaintiffs plausibly link actual fraudulent activity to a healthcare data breach. However, in some of these cases, plaintiffs are still unable to establish causation by failing to adequately link the cyber theft of their health information to their alleged damages.

The result is a changing healthcare data breach landscape in which plaintiffs are more easily able to plead damages, but struggle to plead the causation element of their claims.

Pleading injury through actual misuse

Courts recognize that actual misuse of patient data constitutes a concrete injury, but plaintiffs still must plead facts plausibly connecting that misuse to the breach.

Claims involving unauthorized exposure of health information have gained traction as courts recognize that actual downstream fraud — such as unauthorized financial accounts or tax fraud — constitutes a concrete, cognizable injury.

In *Webb v. Injured Workers Pharmacy, LLC*, the First Circuit reversed the dismissal of a putative class action arising from a 2021 cyberattack on a home-delivery pharmacy that exposed patients' medical records, including Social Security numbers.

The lawsuit included one plaintiff who alleged that, shortly after the breach, a fraudster used her information to file a false tax return, requiring her to spend time resolving the issue with the IRS.

The district court found these allegations insufficient because the complaint did not adequately connect the fraudulent filing to the hack. The First Circuit disagreed, holding that the actual misuse of stolen information is itself a concrete injury and need not be accompanied by additional harm.

Notably, the court further concluded that the complaint plausibly linked the fraud to the hack. The temporal proximity between the cyberattack and the fraudulent tax filing, coupled with allegations that the plaintiff carefully safeguarded her information, supported the inference that the compromised data originated from the breach rather than another source.

The court also recognized that costs incurred responding to the identity theft may support damages claims at the pleading stage. By treating actual misuse as a cognizable injury, *Webb* illustrates the type of allegations that may suffice to establish injury at the pleading stage.

Strict causation and the traceability barrier

Despite the judicial willingness to recognize concrete injuries from cyber incidents, plaintiffs increasingly face dismissal over failure to establish causation. The First Circuit underscored that distinction in *Santos-Pagán v. Bayamón Medical Center*, a 2026 case arising from a ransomware attack on a hospital system that exposed the health information of more than 500,000 patients.

The plaintiff alleged that an unauthorized cellphone account was opened in her name, causing approximately \$800 in losses and credit damage. The court held these allegations were sufficient to establish a concrete injury, consistent with an earlier decision in *Webb v. Injured Workers Pharmacy, LLC*.

However, it nevertheless affirmed dismissal because the complaint failed to plausibly allege the fraudulent account was fairly traceable to the hospital's breach.

Unlike the plaintiff in *Webb*, the plaintiff did not allege she had taken steps to safeguard her personal information, did not provide allegations supporting temporal proximity between the hack and the fraud, and did not explain what information was required to open the cellphone account or whether the hospital possessed that information.

As a result, the complaint failed to support a reasonable inference that the fraud resulted from the hospital hack.

Santos-Pagán demonstrates the important distinction between injury and causation in healthcare data breach litigation because plaintiffs must allege their injuries are traceable to the defendant's breach. Actual identity theft, fraudulent accounts, and related mitigation expenses may satisfy the injury requirement, but plaintiffs must still plead specific facts linking the misuse to the breach.

Disentangling injury from traceability

Recent healthcare data breach decisions highlight a recurring issue: the difference between alleging a concrete injury and alleging facts that connect the injury to the defendant's breach.

Courts are generally willing to recognize actual misuse of personal information, such as identity theft or financial fraud, as a concrete injury. The more difficult hurdle is establishing that the misuse is fairly traceable to the defendant's breach rather than another source.

The contrast between *Webb* and *Santos-Pagán* illustrates this divide. In *Webb*, the plaintiff plausibly connected a fraudulent tax return to the breach through allegations of temporal proximity and careful handling of her personal information.

In *Santos-Pagán*, by contrast, the plaintiff alleged actual fraud but failed to plead facts linking the unauthorized cellphone account to the hospital's ransomware attack. The court emphasized that Article III traceability requires more than speculation; plaintiffs must allege specific facts supporting a causal connection between the exposed data and the subsequent misuse.

After *Santos-Pagán*, the court's analysis suggests that allegations concerning temporal proximity, protection of personal

information, and the relationship between the compromised data and the subsequent fraud are relevant to traceability.

Actual identity theft, fraudulent accounts, and related mitigation expenses may satisfy the injury requirement, but plaintiffs must still plead specific facts linking the misuse to the breach.

These considerations may be especially significant in healthcare cases, where breaches often expose a mix of financial identifiers and medical information. Plaintiffs must therefore plead not only that data was exposed, but why the particular breach was the likely source of the misuse.

Whether exposure alone, without subsequent misuse, constitutes a cognizable injury remains unsettled. *Webb* expressly left open whether unauthorized access to personal information may itself qualify as an intangible harm.

Outside the healthcare context, however, the Second Circuit in *Bohnak v. Marsh & McLennan Companies* concluded that the exposure of a plaintiff's name and Social Security number in a targeted cyberattack was sufficient to establish standing.

If courts ultimately adopt a similar theory for medical information, plaintiffs may focus less on proving downstream misuse and more on the unauthorized access itself. The viability of those theories remains unsettled in cases involving medical information.

Conclusion

Taken together, *Webb* and *Santos-Pagán* suggest that healthcare data breach plaintiffs face a two-step standing inquiry.

Actual misuse of compromised information may satisfy the injury requirement, but plaintiffs must still allege facts plausibly connecting that misuse to the breach being litigated.

As breaches increasingly involve information that may have been exposed through multiple incidents over time, traceability may become the central battleground in future standing disputes.

About the authors



Abbye E. Alexander (L) is co-managing partner of **Kaufman Dolowich LLP**'s Orlando, Fla. office and chair of the firm's health care and managed care practice group. She focuses her practice on issues affecting national and local businesses to include health care professionals, organizations and facilities, including long-term care facilities, assisted living facilities, rehabilitation centers and doctors. She may be reached at aalexander@kaufmandolowich.com. **Henry E. Norwood** (C)

is of counsel at the firm and practices through its San Francisco, Calif. and Orlando, Fla. offices. He concentrates his practice in health care and managed care litigation and compliance, ERISA litigation and compliance, general liability, and commercial litigation. He may be reached at henry.norwood@kaufmandolowich.com. **Emily C. Taing** (R) is an associate at the firm. She focuses her practice in commercial litigation, data privacy, employment law, healthcare and managed care law, and professional liability. She represents clients in a range of business disputes involving breach of fiduciary duty, contract claims, negligence, and regulatory compliance. She is based in San Francisco and may be reached at emily.taing@kaufmandolowich.com.

This article was first published on Reuters Legal News and Westlaw Today on October 27, 2026.