Healthcare

Healthcare Breaches & Litigation Risk At A Glance

Companies that have a breach involving protected health information ("PHI") worry not only about fines and penalties imposed by the Department of Health and Human Services ("HHS"), but about class action lawsuits. The risk that a class action lawsuit will lead to financial liability, however, is often misunderstood.

In many, if not most, class action lawsuits that involve the loss of PHI, plaintiffs have been unable to prove that they have standing to seek recovery. Specifically, unless a plaintiff has been the victim of identity theft or has suffered some other type of concrete injury, most courts have refused to let them proceed based solely on the allegation that they are subject to an increased risk of harm as a result of the breach.[1] The following summarizes the types of allegations that courts have, and have not, led to a finding of standing.

Allegations Found To Be Insufficient

- Alleged violation of HIPAA
- Data loss, but no evidence of access or misuse
- Data lost could not lead to identity theft
- Loss of value of PHI because the PHI can be sold on the cyber black market
- Patients' right to truthful information about the security of their PHI after the breach
- Plaintiffs' receipt of unsolicited phone calls from telemarketers and scam artists, without evidence that these calls result from the breach
- Costs incurred to travel to a different hospital with allegedly better security

Allegations Found By Some Courts to Be Sufficient

- Plaintiffs' lost data has been actually accessed or misused
- Plaintiffs with no prior history of identity theft become identity-theft victims shortly after breach
- Plaintiffs' personal information had not previously been the subject of another unrelated breach
- Plaintiffs receive unsolicited phone calls marketing products related to information that has been breached (e.g. the products are for a specific medical condition listed in the breached PHI), but have never received such phone calls in the past

[1] *See, e.g., Clapper v. Amnesty Int'l. USA*, 133 S. Ct. 1138 (2013) (indicating, outside the realm of PHI, that the mere risk of harm is too speculative).

Bryan Cave's Healthcare Team and Global Data Privacy and Security Team can help you devise a data security program that is compliant with HIPAA, and implement measures to mitigate the risk and damages resulting from a breach.

David A. Zetoony
Partner
david.zetoony@bryancave.com

Darryl Landahl
Partner
darryl.landahl@bryancave.com

Pou-I "Bonnie" Lee
Associate
bonnie.lee@bryancave.com

Frank Fabiani
Law Clerk
frank.fabiani@bryancave.com

BRYAN CAVE

Healthcare

What factors should you look at when considering the risk that litigation poses following a breach:

- ✓ Was the quantity of records lost lower, or greater, than the average number of records involved in recent class action lawsuits?
- ✓ Were the records lost encrypted, obscured, or de-identified?
- ✓ Could the type of information lost be used to commit identity theft?
- ✓ Did patients suffer any direct monetary harm?
- ✓ Has there been any evidence of actual identity theft?
- ✓ Could the data loss hurt the reputation of a patient or cause emotional distress?
- ✓ Did you offer credit monitoring, identity theft insurance, and/or credit repair services?
- ✓ If so, what percentage of impacted consumers availed themselves of your offer?
- ✓ If filed as a class action, is the class representative's claim of identity theft premised on unique facts?

Bryan Cave's Healthcare Team and Global Data Privacy and Security Team can help you devise a data security program that is compliant with HIPAA, and implement measures to mitigate the risk and damages resulting from a breach.

David A. Zetoony
Partner
david.zetoony@bryancave.com

Darryl Landahl
Partner
darryl.landahl@bryancave.com

Pou-I "Bonnie" Lee
Associate
bonnie.lee@bryancave.com

Frank Fabiani
Law Clerk
frank.fabiani@bryancave.com

BRYAN CAVE