ALM | LAW.COM

New York Law Journal

Technology Today

E-DISCOVERY

Court Allocates Costs for Data Security in Discovery

By H. Christopher Boehning and Daniel J. Toal
October 1, 2024

In an era where data breaches and cyber-attacks are increasingly prevalent, data security is often top of mind. During discovery, which can involve vast sets of confidential or protected information, it thus is hardly surprising that producing parties may expect recipients to implement data security protections to guard against data breaches. But such protections can be expensive, and parties may disagree on both the level and type of protections required and the allocation of related costs.

The recent decision in *United States v. Anthem, Inc.*, 2024 WL 2982908 (S.D.N.Y. June 12, 2024), marks a significant development in this area. Addressing the novel question of how to allocate data security costs, the court in *Anthem* highlights the importance of data security in discovery and establishes a new test to determine when and whether cost-shifting may be appropriate.

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *deputy chair and counsel, e-discovery, and* LIDIA M. KEKIS, *e-discovery attorney, assisted in the preparation of this article.*

H. Christopher Boehning

Daniel J. Toal

'United States v. Anthem'

In *Anthem*, the United States alleged that health insurance company Anthem submitted inaccurate information regarding Medicare-covered service costs and that this resulted in the government overpaying Anthem millions of dollars. As a key part of discovery in the matter, the government received protected health information – the medical records of Anthem's members. While the parties agreed that this electronically stored information ("ESI") should receive special security attention, they disputed "the level of security needed to protect the health data…and who should pay for the costs of that security." *Id.* at *1.

The government "proposed a robust set of protections" for the health information and was

already incurring a cost of "about $5,000/month" for such measures. *Id.* Anthem, though, sought additional security measures, including protections in case of future data breaches, that it described as "consistent with industry standards and with applicable regulatory guidance." *Id.* Such measures would add $4,300 a month to the government›s expenses. The government sought to shift those security costs to Anthem.

Protective Orders and Protecting ESI

The court began its analysis by observing that the "issue of data security in discovery and how costs should be allocated for same is one that does not appear to have been addressed in any other court decision." *Id.* at *2. And while under the Federal Rules of Civil Procedure "there is a presumption that the responding party bears the expense of complying with and responding to discovery requests, . . . who should bear the cost of maintaining the security of data turned over in litigation is a slightly different question." *Id.* (cleaned up).

Addressing the novel question of how to allocate data security costs, the court in 'Anthem' highlights the importance of data security in discovery and establishes a new test to determine when and whether cost-shifting may be appropriate.

Protective orders, noted the court, are typical in discovery but they usually focus on confidentiality rather than "secure storage of data or who bears the costs of protecting electronically stored information produced in discovery." *Id.* The court pointed to its own model protective order, which, in relation to personal information, states, in part, "The producing party may specify the minimal level of protection expected in the storage and transfer of its information." *Id.* And while the protective order entered in this case contained the court›s model language, it was silent on "cost-shifting in the event the receiving party disputes the level of protection specified by the producing party." *Id.*

Emphasizing the increased data security risks in litigations and for law firms, the court cited a 2022 report finding that 27% of law firms experienced a data breach and a 2023 report that data breaches have an average cost of $4 million. *See id.* And, given that "one of the government›s vendors experienced a ransomware attack that compromised some of Anthem›s data,… Anthem is rightfully concerned about the protection of its data in this case." *Id.* Moreover, the court observed that the U.S. Department of Health and Human Services "has recognized that healthcare information is frequently a target of cyberattacks and care must be taken to protect health information." *Id.*

A Test for Cost-Shifting

Next, the court turned to the issue of cost-shifting and the factors to examine in determining when it would be appropriate. Under Federal Rule of Civil Procedure 26(c)(1)(B), courts have discretion to allocate discovery costs when there is a showing of "good cause." The court referenced a leading case on the topic, the e-discovery landmark *Zubulake* opinion from 2003, which "set forth various factors to aid courts in analyzing which party should bear the cost of electronic discovery." *Id.* at *3. But given that "[t]hese factors were developed over twenty years ago in the infancy of electronic discovery," prior to even the 2006 amendments to the Federal Rules that

addressed discovery of ESI, the court concluded that the factors "are informative, but are not all directly relevant to the question of whether a producing party who wishes a certain level of data security be provided for data produced in discovery can require the receiving party to bear the full cost of such data security protections for the duration of the litigation until the data is destroyed or returned." *Id.*

The court acknowledged that the receiving party typically shoulders "the costs of maintaining the security of data and the risk of a data breach, as each side will receive data and will need to protect that data pursuant to the terms of any protective order and the level of security and costs will be similar for both sides." *Id.* Moreover, the financial and reputational risks associated with data breaches incentivize parties and attorneys in safeguarding productions received during discovery. Even so, the court also recognized that "there may be some instances when it is appropriate to shift certain costs of data security" and that "there may be different levels of security needed for different types of information produced in a litigation." *Id.*

In this latest decision, Judge Parker addressed a critical aspect of managing data in discovery, and in doing so raised important considerations for parties, the bench, and the bar.

With this in mind, the court set forth a new test for cost-shifting for data security measures in discovery: "After careful consideration, the Court has identified the following, non-exclusive factors as relevant to determining whether there is good cause to shift all or a portion of costs of data security measures from the receiving party to the producing party: 1) the nature of the information to be protected and risks and costs associated with unauthorized disclosure of such information; 2) the reasonableness of the security measures requested by the producing party (which can include an evaluation of the degree of risk mitigated by the security requested relative to less costly security measures); 3) the cost of the data security requested relative to the overall costs of discovery and amount in controversy; and 4) relative ability of the parties to pay the costs of the security requested by the producing party. These factors are not necessarily entitled to the same weight in every case and should be balanced based on the particulars of each case." *Id.*

Applying these factors, the court determined that, as to factor one, since the nature of the information to be protected is "medical information and related personally identifying information" of non-parties and that such information carries a high risk of cyberattacks with costly consequences—including already having been breached in this matter, "Anthem's concern for the security of the data is reasonable and this factor weighs against shifting the costs of that security to Anthem." *Id.*

On factor two relating to the reasonableness of the measures, the court stated that only Anthem provided a technical opinion as to the importance of the additional measures and, as such, it could "not rely on the representations of lawyers for the government to conclude that their proposed safeguards are sufficient." *Id.* at *4.

Thus, the court found that this factor also weighed against shifting the costs to Anthem. The court reached the same conclusion with factor three concerning the proportionality of costs,

finding that the added annual cost to implement Anthem's requested measures was minimal relative to the millions of dollars at stake. *See id.*

And regarding factor four, the relative ability of the parties to pay the costs, the court found that after comparing the resources of the parties, this factor slightly weighed in favor of shifting the costs to Anthem. *See id.*

Having reviewed and analyzed the four factors, the court concluded "that the additional security measures requested by Anthem are proportionate to the nature of the information sought to be protected, reasonable in light of the only evidence provided on the level of security required, and proportionate to the total amount in controversy and the overall costs of litigation." *Id.* Balancing the factors, it determined that "the government has not shown good cause to shift the burden to Anthem to pay for the additional security requested" and directed the government to implement Anthem's added security measures and bear the additional costs. *Id.*

Moving the Law Forward

Magistrate Judge Katharine Parker has issued several key e-discovery decisions during her tenure, including a prior ruling in this matter (frequent readers may recall our June 4, 2024 column, "Clone Discovery Must Meet Relevance, Proportionality, Particularity Requirements"). In this latest decision, Judge Parker addressed a critical aspect of managing data in discovery, and in doing so raised important considerations for parties, the bench, and the bar.

First, *Anthem* underscores the importance of addressing data security as part of discovery practice, emphasizing the need for parties and judges to be guided by technology experts to protect sensitive data from potential breaches and other cyberattacks.

Second, the decision promotes the inclusion of data security provisions in protective orders between parties, highlighting this as a key issue alongside more traditional topics often covered in such agreements. Many practitioners and parties, particularly those who have experienced data breaches, may find this approach beneficial.

Third, by introducing a new test for cost-shifting of data security measures in discovery—grounded in the principles of reasonableness and proportionality—Judge Parker provides valuable precedent and guidance, advancing the law on this important and timely topic.