MIS

MIS SOLUTIONS, INC.

Georgia's healthcare data breach crisis

How 106 breaches exposed 33 million patient records in five years,
and which counties are hit hardest

An original analysis of federal HHS breach data by MIS Solutions, Inc.
April 2026

Authored by Lliam Holmes, CEO of MIS Solutions
www.mis-solutions.com

Key findings

MIS Solutions analyzed every healthcare data breach reported to the U.S. Department of Health and Human Services by Georgia-based organizations from 2010 through early 2026. The analysis draws on the HHS Office for Civil Rights Breach Portal, which requires organizations to publicly disclose any breach affecting 500 or more individuals. Here is what the data reveals.

Georgia ranks #5 nationally for per-capita healthcare data breach impact over the last five years. In that period, breaches reported by Georgia organizations exposed records equivalent to nearly 3x the state's entire population.

106 breaches were reported by Georgia healthcare organizations between 2021 and 2025, affecting an estimated **32.9 million individual records**.

Hacking and IT incidents now account for 88% of all healthcare breaches in Georgia, up from 53% in 2019.

The biggest damage isn't at the doctor's office. Business associates and health plans account for just 37% of breach incidents but 87% of all individuals affected.

Rural Georgia is hit harder than metro Atlanta. Per-capita breach impact outside the metro Atlanta area (7.7x population) is more than triple the metro rate (2.3x).

The scale of the problem

Since 2010, healthcare organizations operating in Georgia have reported 219 data breaches to the HHS Office for Civil Rights, affecting a cumulative 38 million individual records. The pace of exposure has accelerated sharply in recent years, with the last five years alone accounting for 86% of the total.

Two dynamics are driving the acceleration. First, the number of breaches has risen from an average of 9 per year in 2015–2019 to an average of 21 per year in 2021–2025. Second, individual breaches have become far more damaging. The median breach in 2021–2025 affected 18,354 individuals, compared to smaller-scale incidents in earlier years. Several single incidents each exposed more than a million records.

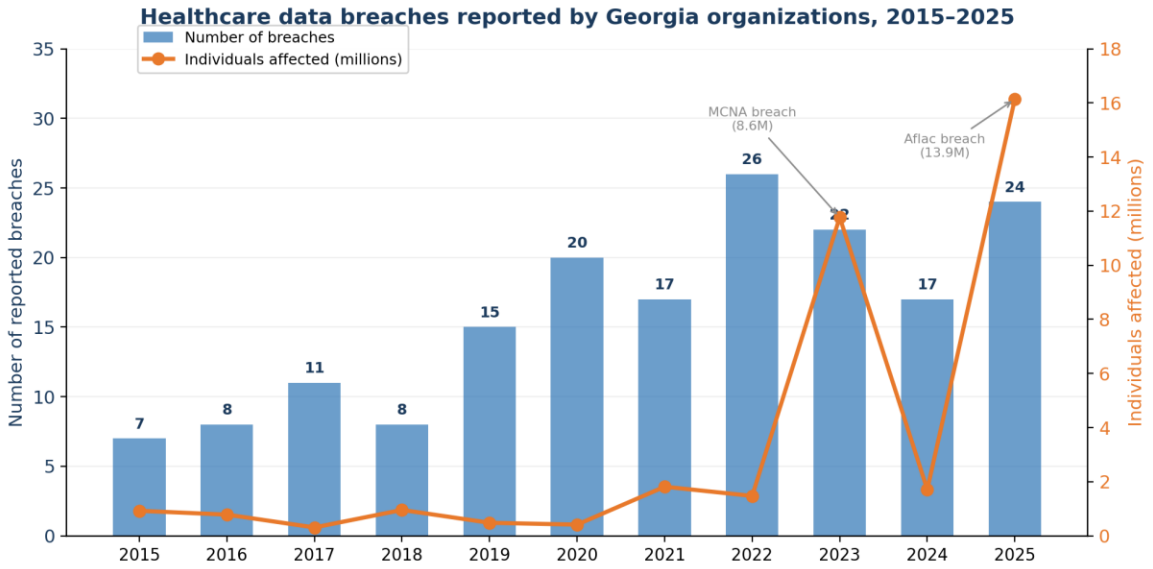

Figure 1. Georgia healthcare breaches and individuals affected, 2015–2025. Source: HHS OCR Breach Portal.

The spikes in 2023 and 2025 are largely attributable to single catastrophic incidents such as the Managed Care of North America breach (8.6 million individuals, 2023) and the Aflac breach (13.9 million individuals, 2025). Even excluding those two events, the underlying trend shows steady growth in both breach frequency and scale.

How breaches happen

The nature of healthcare data breaches in Georgia has fundamentally changed. A decade ago, breaches were often physical — stolen laptops, lost paper records, improper disposal. Today, the threat is overwhelmingly digital. Hacking and IT incidents have risen from 53% of all Georgia healthcare breaches in 2019 to 88% in both 2024 and 2025.

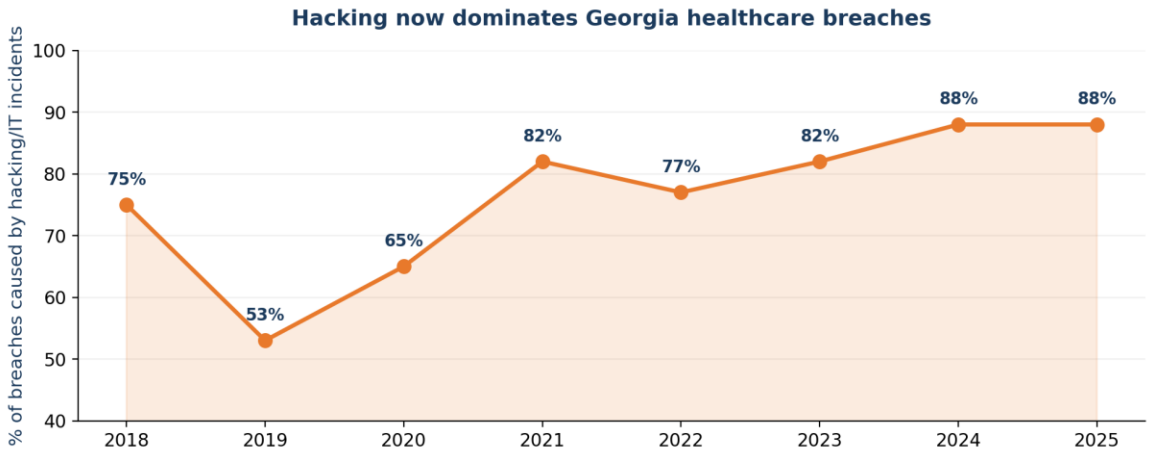

Figure 2. Hacking/IT incidents as a percentage of all Georgia healthcare breaches, 2018–2025.

Network servers are the most common location of breached information (45% of all Georgia incidents), followed by email systems (23%) and paper/film records (13%). The dominance of network server breaches reflects the reality that most healthcare data now lives on networked infrastructure — electronic medical records, cloud platforms, and third-party hosted systems.

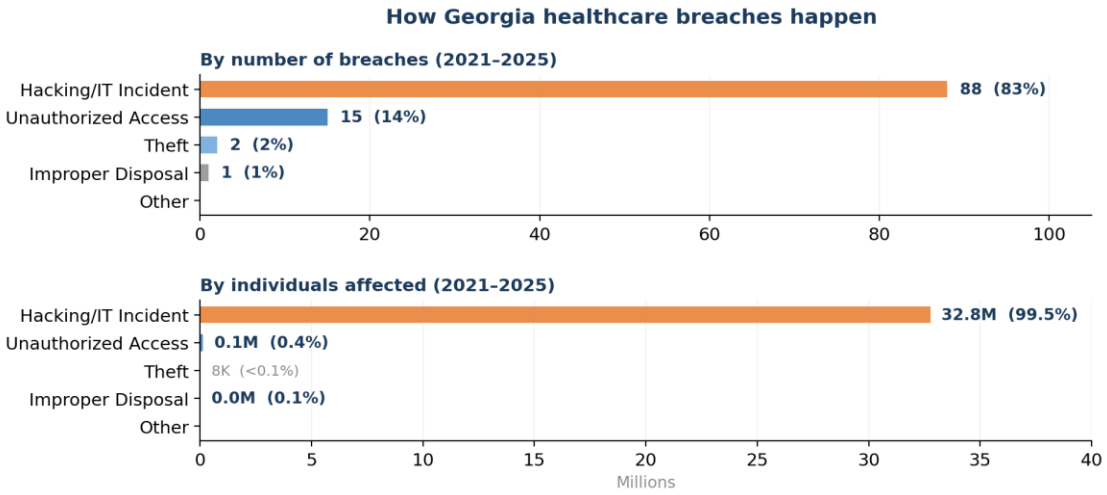

Figure 3. Georgia healthcare breach types by number of incidents and by individuals affected, 2021–2025.

> *"The shift from physical theft to network-based attacks tells us something important: the organizations that haven't modernized their cybersecurity infrastructure aren't just behind the curve — they're operating with open doors. Firewalls, endpoint protection, and network monitoring aren't optional anymore. They're the baseline."*
>
> — Lliam Holmes, CEO, MIS Solutions

The hidden weak link: business associates and health plans

One of the most striking findings in this analysis is the disconnect between who reports breaches and who exposes the most records. Healthcare providers — hospitals, clinics, physician practices — account for 62% of all breach incidents reported by Georgia organizations over the last five years. But they account for only 13% of all individuals affected.

The vast majority of exposed records (87%) come from business associates and health plans — the vendors, billing companies, insurance administrators, and technology contractors that handle healthcare data behind the scenes. A single business associate breach can expose millions of records because these entities process data for dozens or hundreds of healthcare organizations simultaneously.

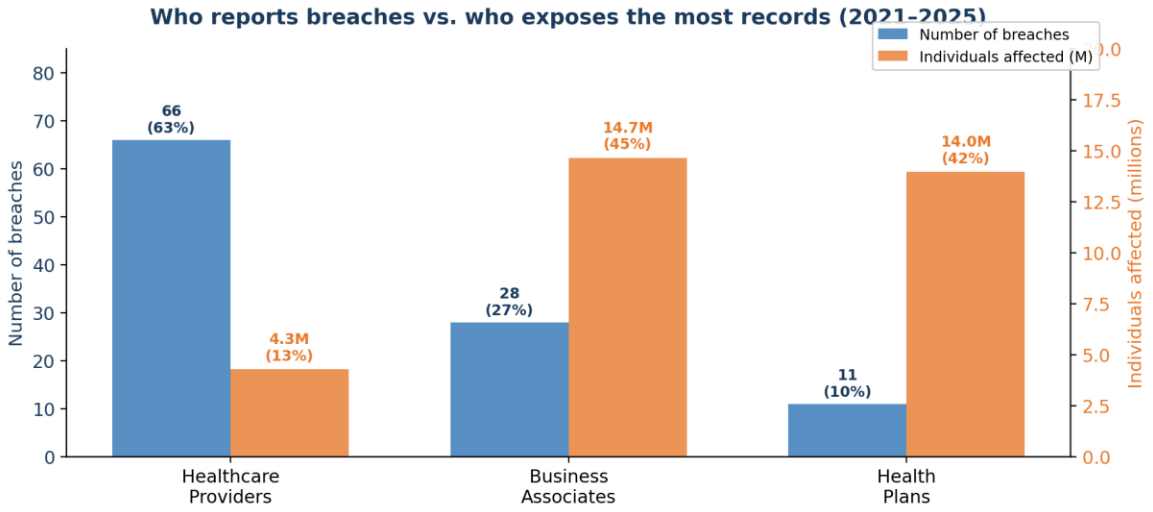

Figure 4. Healthcare providers report the most breaches, but business associates and health plans expose the most records.

The five largest Georgia healthcare breaches (2021–2025)

Organization	Individuals	Year	Type
Aflac Incorporated	13,924,906	2025	Health Plan
Managed Care of North America	8,627,242	2023	Business Associate
NASCO	1,744,655	2023	Business Associate
St. Joseph's/Candler Health System	1,400,000	2021	Healthcare Provider
Lockton Companies (Southeast)	1,124,727	2025	Business Associate

Table 1. Largest healthcare data breaches by Georgia organizations, 2021–2025. Source: HHS OCR Breach Portal.

Of the five largest breaches, only one (St. Joseph's/Candler) was a healthcare provider. The other four were business associates or health plans. This pattern has significant implications for healthcare organizations evaluating their cybersecurity posture: the greatest data-exposure risk often lies not within the organization itself but with the third-party vendors it entrusts with patient data.

> *"When a healthcare practice evaluates its cybersecurity, they typically think about their own network, their own staff, their own systems. But the data tells a different story. The biggest exposures are happening at the companies they share data with — the billing services, the claims processors, the cloud vendors. If you're not asking hard questions about your business associates' security posture, you're ignoring where 87% of the damage actually occurs."*
>
> — Lliam Holmes, CEO, MIS Solutions

Which Georgia counties are hit hardest

To understand the geographic distribution of healthcare data breaches across Georgia, MIS Solutions mapped each of the 219 breaches to the county where the reporting organization is located. This mapping covers 73% of all affected individuals; the remaining 27% are attributable to statewide government entities or national companies that filed under Georgia in the federal portal.

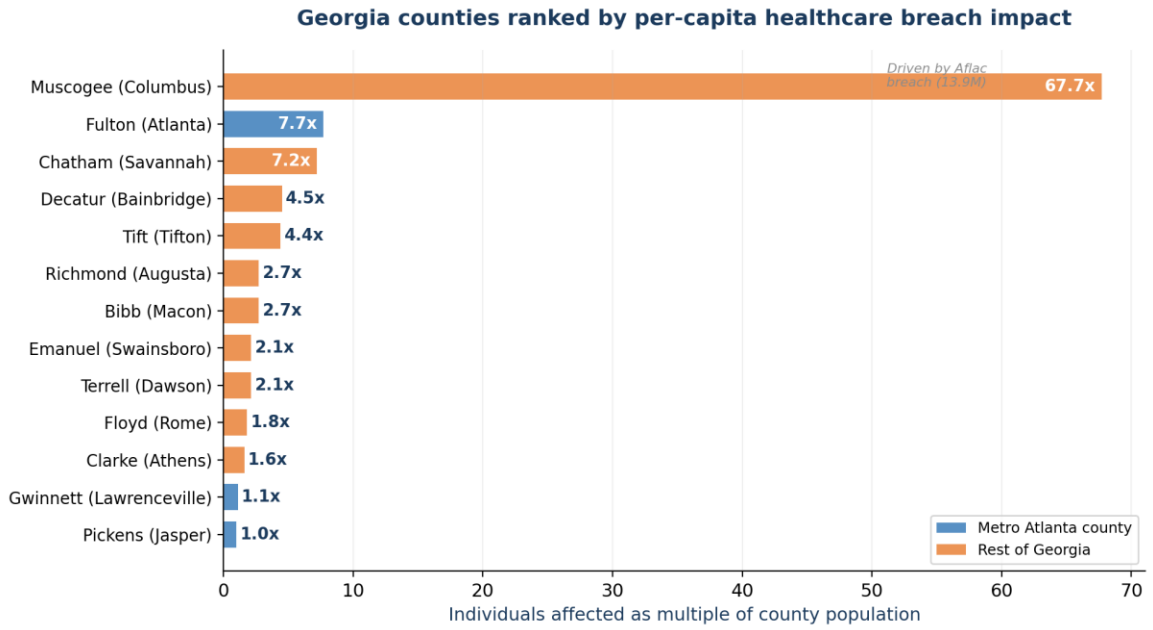

Figure 5. Georgia counties ranked by per-capita healthcare data breach impact (all years).

Fulton County (Atlanta) leads the state in total breach count with 90 reported incidents, reflecting its concentration of healthcare organizations, insurance companies, and business associates. But the per-capita picture reveals a more nuanced story. Multiple counties outside metro Atlanta — including Chatham (Savannah), Tift (Tifton), Decatur (Bainbridge), and Richmond (Augusta) — have per-capita breach rates that rival or exceed the Atlanta metro area.

Top 10 Georgia counties by per-capita healthcare breach impact

County	City	Breaches	Individuals	Per capita
Muscogee	Columbus	12	14,004,818	67.7x*
Fulton	Atlanta	90	8,213,801	7.7x
Chatham	Savannah	11	2,133,957	7.2x
Decatur	Bainbridge	1	120,085	4.5x
Tift	Tifton	2	181,187	4.4x
Richmond	Augusta	8	553,936	2.7x

Bibb	Macon	3	408,483	2.7x
Emanuel	Swainsboro	2	47,973	2.1x
Terrell	Dawson	1	18,000	2.1x
Floyd	Rome	2	177,968	1.8x

** Muscogee County's extreme ratio is driven primarily by the Aflac breach (13.9M individuals). Aflac is headquartered in Columbus but serves customers nationally.*

Table 2. Georgia counties with the highest per-capita healthcare breach impact (all years). Source: HHS OCR Breach Portal, U.S. Census Bureau.

Metro Atlanta vs. the rest of Georgia

Aggregating the data reveals a counterintuitive pattern: healthcare organizations outside metro Atlanta have a higher per-capita breach impact (7.7x population) than those within it (2.3x). This challenges the assumption that cybercrime is primarily an urban problem. Rural and smaller-city healthcare organizations in Georgia are experiencing significant data exposure — potentially because they have fewer dedicated IT and cybersecurity resources.

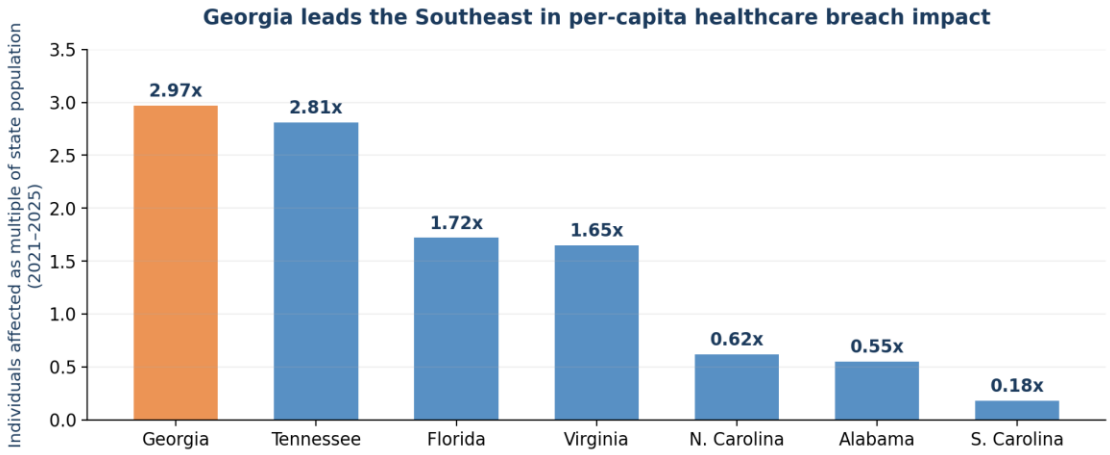

Figure 6. Georgia leads the Southeast in per-capita healthcare breach impact, 2021–2025.

Across the Southeastern United States, Georgia ranks first for per-capita healthcare breach impact at 2.97x its population, ahead of Tennessee (2.81x), Florida (1.72x), and Virginia (1.65x). Nationally, Georgia ranks 5th — behind only Minnesota, Colorado, Delaware, and Nevada — a position that few would expect from a state not typically associated with healthcare data vulnerability.

> *"There's a misconception that cybersecurity is only a big-city problem. Our analysis shows the opposite — healthcare organizations in smaller Georgia communities are being hit hard, and they often don't have the in-house IT teams to detect or respond to these incidents effectively. That's the gap that managed IT services are designed to fill."*
>
> — Lliam Holmes, CEO, MIS Solutions

Methodology

Data source

This analysis is based on data from the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) Breach Portal, accessible at ocrportal.hhs.gov. Under the HIPAA Breach Notification Rule, covered entities and business associates must report breaches of unsecured protected health information affecting 500 or more individuals to HHS. These reports are made publicly available through the portal.

Scope

The dataset includes all HIPAA breach reports filed under the state of Georgia, encompassing both cases currently under investigation and archived/resolved cases. The data spans from April 2010 through February 2026. A total of 219 breach records were analyzed.

Important limitations

- **Reporting state vs. affected population.** The HHS portal lists breaches by the state of the reporting entity, not by where affected individuals reside. Organizations like Aflac and Managed Care of North America are headquartered or filed in Georgia but serve customers nationally. The "individuals affected" figures reflect total breach scope, not Georgia-specific impact.
- **Per-capita figures are illustrative, not literal.** When we say Chatham County has a per-capita breach rate of 7.2x its population, this means that organizations in Chatham County reported breaches affecting 7.2 times the county's population in total records. It does not mean every resident was affected 7.2 times.
- **Only breaches affecting 500+ individuals are included.** Smaller breaches are reported to HHS but are not publicly listed. The true number of healthcare data security incidents in Georgia is likely higher than what this dataset captures.
- **County mapping is based on organizational location.** Each entity was mapped to its primary Georgia county based on publicly available address information. National companies that filed under Georgia are categorized separately.

Analysis

All data was downloaded from the HHS OCR Breach Portal in CSV format. Analysis was performed using standard spreadsheet and statistical methods. Population data for per-capita calculations is drawn from U.S. Census Bureau 2024 population estimates. State-level and county-level rankings were calculated by dividing total individuals affected by the relevant population.

About MIS Solutions

MIS Solutions is an Atlanta-based managed IT services provider serving businesses across Georgia. The company provides outsourced IT support, cybersecurity services, cloud solutions, backup and disaster recovery, IT consulting, AI consulting, and compliance-focused technology management. MIS Solutions works with healthcare organizations, professional services firms, and small to mid-sized businesses that require enterprise-grade IT security without the cost of a full in-house IT department.

For more information, visit mis-solutions.com or contact MIS Solutions directly.

Media inquiries

For questions about this study, requests for additional data, or to schedule an interview with Lliam Holmes, please contact MIS Solutions at 678-745-5109 or info@mis-solutions.com