HEALTH CARE AND CYBERSECURITY AND DATA PRIVACY PRACTICE
INFORMATION MEMO
AUGUST 4, 2025

Keeping Data Secure When Government Funding Is Shrinking – the Lean But Mean Imperative for Smaller Health Care Delivery Organizations

By: Gabriel S. Oberfield, Esq., M.S.J.

When President Donald Trump signed the Federal reconciliation bill into law on July 4th, things became more challenging for smaller or rural health care delivery organizations – often working on shoestring budgets heavily reliant on Medicaid as a payor – to fund their cybersecurity and data privacy efforts. Despite the challenges, now is *not* the time to take the foot off the gas, because the risks remain significant and the Federal government continues to pursue enforcement actions when it senses that inaction has led to data compromise.

There are lots of strong sentiments nationally concerning the implications of the One Big Beautiful Bill Act ("OBBBA"), – in particular, as relating to the changes afoot for the nation's Medicaid program. Notably, Medicaid is celebrating its 60th anniversary last week – a program borne out of President Lyndon Johnson's Great Society. That program, of course, is a major source of revenue across the health care delivery system among its various 'safety net' providers, including nursing homes, hospitals and a plethora of community based providers.

OBBBA driven changes to Medicaid affect who is eligible for the program, the retroactivity of coverage and they institute new participant work requirements. These, among other shifts, will have profound effects on the flow of Medicaid funds to healthcare providers across New York State and beyond. At the annual Medicaid conference of the United Hospital Fund on July 30, keynote speaker Amir Bassiri, the State's Medicaid director, presented in stark terms the various and overlaying ways that Federal government funding to Medicaid will be diminishing in New York. Among other observations, Bassiri noted challenges that smaller and rural healthcare providers will face in the redefined environment.

Regardless of how one views OBBBA's provisions, effects on Medicaid funded providers will begin to play out – some promptly, and others, over time. Remember, many of the same providers have been working to rebound, as best possible, from the ravages of the pandemic. This is the same cohort that entered the pandemic with finances already in some turbulence due to the differences in reimbursement in the Medicaid program relative to actual costs of care (which many have roughly estimated in the nursing home space, as just one example, as thirty cents short for every dollar expended). Rural health care providers – regardless of service profile – have experienced comparable stresses, including the high costs to recruit and retain staff following the outbound exodus of health care practitioners that the pandemic spurred, and other expenses attendant to service delivery in environments where Medicaid often is the primary payor for care.

All of this financial stress ties into cybersecurity and data privacy – a reality that the Health Sector Coordinating Council[1] recognized in its May 2025 report to the Federal Department of Health and Human Services ("HHS") concerning so-called 'resource constrained' providers. In its report, HSCC defined such

[1] The author is an HSCC member – as well as a member of a Region II planning body examining healthcare delivery system resilience, a review which includes inquiry into cyber threats.

entities as, e.g., rural, critical access hospitals, federally qualified health centers, post-acute care sites and certain physician practices, among other examples. Risks the HSCC highlights for this group include the dearth of enterprise trained staff, insufficient health IT infrastructure and "the [lack of] funding or the expertise to manage ongoing and evolving cyber threats against their health systems." Moreover, the authors posit, "…while the biggest concern has traditionally been about the … personal health information exposed by these attacks, the existential threat has evolved to the disruption of actual patient care and the likelihood that a ransomware or other disruptive attack could result in patient harm or death."

The HSCC white paper calls for government investment to support the nation's cybersecurity backbone – most critically, among the under-resourced providers its report highlights. To this point, the recommendations remain under HHS's advisement and have been shared with Congress as well.

Nonetheless, Federal agencies such as HHS's Office for Civil Rights continue to pursue enforcement actions concerning data compromise with alacrity. For instance, in July, it censured an ambulatory surgical center in upstate New York for alleged data privacy infractions involving the Health Insurance Portability and Accountability Act ("HIPAA") and its security rule and attendant breach notification protocol. Notwithstanding the pressure of the moment that some constrained healthcare providers may be experiencing, vigilance concerning data privacy and cybersecurity remains of paramount importance. The threats aren't going away – just last month, Federal agencies issued a broad warning concerning a focused set of health care ransomware incidents.

At Bond, we can help you develop robust policies, procedures and strategies that meet your budget and work within your means to defend your patients' data and keep your institution on the right side of governmental compliance and audit inquiries. If you are looking for a hand, please reach out to the Bond attorney with whom you have a working relationship, including this author.