Eye on Telehealth: Opening Doors and Surfacing New Data Privacy Questions as the Pandemic Ebbs

Across the country, there's increasing optimism that the worst of the pandemic is behind us, and that we can begin to contemplate what our 'new normal' looks like. We know, of course, that nothing will be quite the same – and in this moment of unprecedented transition, healthcare is morphing to match the new realities on the ground. In this context, the evolution of telehealth offers a useful case study – both for healthcare operations and for healthcare data privacy.

The Transformation of Telehealth

It's fair to say that telehealth exploded onto the national stage during the pandemic, with growth in many respects attributable to emergency-driven regulatory relaxations. As the U.S. Department of Health & Human Services (HHS) has noted, in relation to Centers funded by the Health Resources and Services Administration (HRSA) there has been "significant growth in the number of virtual visits from 478,333 in 2019 to 28,550,608 in 2020, a remarkable 6,000 percent increase." Another sector transformed by telehealth is behavioral health, where there has been a monumental increase in usage patterns. Telehealth also has revealed promise in its power to extend healthcare resources into underserved communities (a topic that came up as a thread throughout presentations during a mid-February University of Pennsylvania conference, "A Fair Shot at Health," which this writer attended), and in its support of healthcare delivery in emergency response. Seeing such positive developments, the federal government is increasing funding to expand telehealth's reach.

Healthcare Data Privacy Implications

Of course, telehealth comes with data security questions – particularly because some of it involves care delivery taking place on apps and via other technologies presently outside of HIPAA's reach. These types of gaps weren't contemplated when HIPAA standards came online, but now are patent as more care described as "telehealth" moves outside traditional boundaries. Indeed, there is proposed legislation on Congress aiming to remedy this discrepancy.

What Is Likely to Stick – And Potential Barriers

Notwithstanding the legitimate concerns around data privacy and robust protections around telehealth's use, the notable uptick in telehealth volume from pre-pandemic levels seems here to stay across the country. It's likely, however, we will see greater prevalence in some corners of health delivery as opposed to others. For instance, according to trade research, "Many patients with chronic illness plan to continue seeing their doctors for some or all of their visits via telemedicine, even after the pandemic." All this will be affected by whether pre-pandemic regulations limiting reimbursement parity and other drivers of its growth (including interstate care compacts) come off the books when public health emergency relaxations ultimately end. Congress is just one governmental entity that has begun looking at this, including through legislation introduced late last year.

The Surrounding Context – 2022 Stands to Be a Watershed Year in Healthcare Data Exchange

All this comes in an environment where information sharing already was on a roadmap to growth this year in the healthcare space, as Micky Tripathi commented in Health Affairs. This stems from scheduled implementation of elements of the 21st Century Cures Act, including those involving 'information blocking,' application programming interface (API) standardizations, and the 'Trusted Exchange Framework' and 'Common Agreement.' As Bond attorneys signaled earlier this year, the changes are part of a shifting post-pandemic regulatory landscape at the governmental level, and they come at a time when more data are being shared through electronic health records than ever before, and with that, attendant risks to healthcare data may be on the rise. (These are the types of topics front-of-mind with the 405d task group, of which this writer is a member.)

What's Next

Where this all goes will be the focus of Bond attorneys – both in the healthcare and cybersecurity and data privacy practices – as we move deeper into the 2022 calendar. If you have questions about the information presented in this piece, please contact Gabriel S. Oberfield, any attorney in our Health Care practice, the Cybersecurity and Data Privacy practice or the attorney at the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Bond has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, www.bsk.com. Attorney Advertising. © 2022 Bond, Schoeneck & King PLLC.

Bond, Schoeneck & King, PLLC BondLawFirm Bond, Schoeneck & King bondlawfirm