HLB's Digital Health Blog

Insights 07.10.26

TEFCA OVERSIGHT AND EXPANSION

The U.S. Department of Health and Human Services (HHS), through the Office of the National Coordinator for Health Information Technology (ONC), announced new oversight measures for the Trusted Exchange Framework and Common Agreement (TEFCA), the national interoperability network designed to facilitate secure electronic exchange of health information. ONC has awarded a contract to enhance audit, review, and compliance functions and is conducting additional reviews of Qualified Health Information Networks (QHINs) and participating organizations to ensure adherence to TEFCA requirements. HHS also reported that TEFCA has grown from approximately 10 million exchanged health records to more than 1 billion records in less than one year.

FDA AUTHORIZES FIRST SOFTWARE AS A MEDICAL DEVICE INCORPORATING A PATIENT-FACING LLM

Digital health company UpDoc announced that it received Food and Drug Administration approval for what the company describes as the first Software as a Medical Device ("SaMD") incorporating patient-facing large language models for medication management purposes. The UpDoc platform, designed on previously approved tools to assist in management of type 2 diabetes medication, integrates with electronic health records and existing clinical workflows and allows patients to submit information to produce treatment plans generated in accordance with clinician-defined protocols.

While this clearance indicates the FDA's willingness to authorize certain AI-enabled clinical tools, it does not establish a required approval pathway for all LLM-based healthcare products. Federal and state regulators continue to pursue multiple oversight approaches to regulating AI in health care, including an increasing number of states expressing interest in facilitating patient access to AI-enabled care through regulatory sandbox programs. Entities developing clinical and patient-facing AI technologies should consider governance and legal strategies calibrated to the specific intended use of the product at issue, as well as the implementation of protocols sufficient to demonstrate the safety, effectiveness, and reliability of the underlying AI technology.

ILLINOIS' AI SAFETY MEASURES ACT REFLECTS THE GROWING PATCHWORK OF STATE-LEVEL AI REGULATIONS

Illinois Governor J.B. Pritzker signed the Artificial Intelligence Safety Measures Act into law on July 6, 2026. The legislation requires developers of frontier AI models to develop and publish a transparency framework describing how they apply recognized industry standards, evaluate model capabilities, and assess and mitigate risks of catastrophic harm to individuals and the public.

PROFESSIONAL

ERIC M. FISH
Partner
Washington, D.C.

CLAIRE ERNST
Director, Government Relations & Public Policy
Washington, D.C.

MONICA MASSARO
Principal, Government Relations & Public Policy
Washington, D.C.

The Illinois measure builds on transparency and accountability requirements included in California's the Transparency in Frontier Artificial Intelligence Act and New York's the Responsible AI Safety and Education (RAISE) Act, both enacted in late 2025. Like those laws, the Illinois framework imposes a range of obligations on developers of frontier models, including the publication of transparency reports and AI safety frameworks, incident reporting requirements, implementation of cybersecurity safeguards, and processes for identifying and responding to critical safety incidents.

The new law also includes, for the first time, a requirement that large frontier model developers undergo annual independent third-party audits evaluating model risks, safety controls, and mitigation measures. These audits must be conducted in accordance with accepted auditing standards and recognized industry best practices, signaling a shift from voluntary commitments toward more formal oversight and accountability mechanisms.

As transparency and accountability continue to emerge as central pillars of AI governance, particularly in healthcare, these disclosure and audit requirements may provide healthcare organizations with valuable information to support the assessment, procurement, monitoring, and governance of AI-enabled tools that incorporate frontier models. More broadly, the enactment of this law underscores the increasingly complex compliance landscape facing AI developers and deployers as states continue to advance AI-specific regulatory frameworks while federal lawmakers debate the appropriate scope and structure of national AI regulation. The result is a growing patchwork of state requirements that may create additional compliance, governance, and operational challenges for organizations deploying AI systems.

CALIFORNIA EXPANDS SALES TAX TO SAAS AND DIGITAL PRODUCTS

On June 29, 2026, California Governor Gavin Newsom signed SB122 into law, expanding the state sales tax base to include SaaS, electronically delivered software, and certain digital products beginning in 2027. The legislation generally treats many digital products as taxable tangible personal property and adopts a customer-based sourcing methodology. For remotely accessed or electronically delivered products, sales are sourced to the purchaser's "known address" in California.

The new tax classifications will require both software providers and customers to reassess their sales and use tax compliance obligations. These changes also may increase costs for healthcare providers and other end users as software vendors seek to pass through newly imposed sales and use tax liabilities. Users may also see increased compliance costs associated with implementing the new regime and amending existing contractual arrangements.

HOUSE PASSES KIDS ACT, SENDING ONLINE CHILD SAFETY DEBATE TO THE SENATE

On July 7, the House of Representatives passed the KIDS Act (H.R. 7757) in a vote of 267-117, advancing a package of online child safety measures aimed at establishing baseline federal protections for minors while allowing states to enact stronger safeguards. The legislation reflects years of congressional efforts to strengthen protections for children online and follows a bipartisan agreement reached in the House Energy and Commerce Committee.

The package includes provisions requiring AI chatbots to disclose that they are not human, restricting minors' access to disappearing messages, and requiring age-verification technologies for certain content. The bill also establishes federal standards for children's online safety while preserving states' ability to adopt more stringent protections and does not preempt state artificial intelligence laws.

While House passage marks a significant milestone, substantial challenges remain before the legislation can become law. The House and Senate continue to differ on key elements of child online safety policy, including age-verification requirements, First Amendment concerns, and whether online platforms should be subject to a "duty of care" obligation requiring them to design products with children's safety in mind. While this legislation may not see final passage this Congress, this has been an ongoing bipartisan area of interest as Congress looks to find agreement on how to regulate artificial intelligence and work will likely continue into the next Congressional session.

Digital Health Blog – Hooper, Lundy & Bookman

RELATED CAPABILITIES

HOOPER LUNDY BOOKMAN

Digital Health

Government Relations and Public Policy