The Honorable Roy Blunt
Chairman
Subcommittee on Labor, Health and Human Services, Education, and Related Agencies
U.S. Senate Committee on Appropriations
Dirksen Senate Office Building, Room 131
Washington, District of Columbia 20510

The Honorable Patty Murray
Ranking Member
Subcommittee on Labor, Health and Human Services, Education, and Related Agencies
U.S. Senate Committee on Appropriations
Dirksen Senate Office Building, Room 156
Washington, District of Columbia 20510

Dear Chairman Blunt and Ranking Member Murray,

As you and your colleagues begin work on the Fiscal Year (FY) 2020 Labor, Health and Human Services, Education and Related Agencies appropriations bill, we respectfully request that you provide the Centers for Disease Control and Prevention (CDC) $100 million in FY 2020 for a new, cross-cutting initiative that will transform public health and save lives. Specifically, this funding would allow CDC, state, local, tribal, and territorial health departments to move from sluggish, manual, paper-based data collection to seamless, automated, and secure IT systems, and to recruit and retain skilled data scientists to use them. More, better, faster data yielded by secure, privacy-defending, interoperable, integrated systems will allow public health professionals and policymakers to make better decisions and get ahead of chronic, emerging, and urgent threats.

Public health agencies at the federal, state, local, tribal, and territorial levels are actively working with health care providers and the public at-large to detect, report, respond to, and prevent illness and death. Every day—often unbeknownst to most Americans—public health is saving lives by detecting and facilitating the response to health threats including \textit{E. coli} contaminated lettuce, measles, antibiotic resistance, lead poisoning, diabetes, heart disease, influenza, health care associated infections, opioid overdoses, Zika, and many more.

Unfortunately, the nation’s public health data systems are antiquated, rely on obsolete information sharing methods, and are in dire need of security upgrades. Sluggish, manual processes from the 19th and 20th centuries—paper records, phone calls, spreadsheets, and faxes requiring manual data entry—are still in widespread use. Lack of interoperability, reporting consistency, and data standards leads to errors in quality, completeness, timeliness, and communication. In addition, public health professionals are faced with rapid advances in data science and evolving cybersecurity threats, and many do not yet have the necessary 21st century skills to understand and securely integrate health data.

Health care providers are \textit{required} to report diseases and conditions to public health departments, and they have these data in electronic health records. These health records contain sensitive personal information that demands significant care in handling in order to protect the privacy and safety of patients, particularly since such systems are frequently the target of
hackers, including attacks from foreign government hackers. However, the nation’s public health infrastructure is so fragmented and antiquated that health care providers have nowhere to rapidly send these health data because public health departments cannot receive them electronically. This leads to inefficiency and frustration on the part of both care providers and public health professionals when electronic data must be manually converted back to paper and faxed, emailed, or mailed. It also leads to lost opportunities, lost time, and lost lives. For in an epidemic like opioids or an outbreak like measles, time is of the essence.

The broad scale implementation of next-generation data systems provides public health authorities the opportunity to improve coordination while defending the privacy and security of patients. Such systems would better equip under-resourced departments to address and mitigate the significant cyber security threats commonly posed to public health infrastructure. The system would require the use of encryption, multi-factor authentication, access controls, and privacy-enhancing technologies in the exchange of patient records and other information. The National Institute of Standards and Technology’s Cybersecurity Framework and its planned Privacy Framework will be used as a guide to implement industry best practices in the design and administration of the infrastructure.

The development of 21st century data systems and the public health workforce needed to operate and maintain them have been woefully underfunded. The strong, long-standing partnership with the CDC and state, local, tribal, and territorial public health departments has gone a long way in protecting the public’s health. However, just as health threats continue to evolve, so too must public health’s modes and methods. An investment of $100 million starting in FY 2020, with a goal of $1 billion over the next ten years, would provide the down payment CDC needs to move public health into the 21st century and harness the power of electronic data and technology in the same way such federal investments in health information technology have transformed health care delivery. Indeed, it is the connection of the health care and public health systems—seamlessly sharing health information—that will offer returns on these investments, and ultimately improve Americans’ health.

Thank you for your consideration of this request.

Sincerely,

Richard Blumenthal
United States Senate