

MICHAEL B. ENZI, WYOMING  
RICHARD BURR, NORTH CAROLINA  
JOHNNY ISAKSON, GEORGIA  
RAND PAUL, KENTUCKY  
SUSAN M. COLLINS, MAINE  
LISA MURKOWSKI, ALASKA  
MARK KIRK, ILLINOIS  
TIM SCOTT, SOUTH CAROLINA  
ORRIN HATCH, UTAH  
PAT ROBERTS, KANSAS  
BILL CASSIDY, M.D., LOUISIANA

PATTY MURRAY, WASHINGTON  
BARBARA A. MIKULSKI, MARYLAND  
BERNARD SANDERS (I), VERMONT  
ROBERT P. CASEY, JR., PENNSYLVANIA  
AL FRANKEN, MINNESOTA  
MICHAEL F. BENNET, COLORADO  
SHELDON WHITEHOUSE, RHODE ISLAND  
TAMMY BALDWIN, WISCONSIN  
CHRISTOPHER S. MURPHY, CONNECTICUT  
ELIZABETH WARREN, MASSACHUSETTS

DAVID P. CLEARY, STAFF DIRECTOR  
EVAN SCHATZ, DEMOCRATIC STAFF DIRECTOR

<http://help.senate.gov>

## United States Senate

COMMITTEE ON HEALTH, EDUCATION,  
LABOR, AND PENSIONS

WASHINGTON, DC 20510-6300

April 27, 2015

The Honorable Gene Dodaro  
Comptroller General of the United States  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Dodaro:

We are writing to request that the Government Accountability Office (GAO) conduct a study to identify cybersecurity risks to electronic health information and health information technology (IT) systems.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed in 2009, was intended to promote the adoption and meaningful use of electronic health records systems. The increased use and interconnectivity of electronic health records offers many benefits, but also requires increased preparedness by health care organizations to protect personal health information and other personally identifiable information from cyber hacks and other threats. Insurance companies also store large amounts of personally identifiable information, including health information that can be vulnerable to cyber hacks.

HITECH updated federal requirements and standards to guard against these threats. Federal regulations require that organizations meet standards for security testing and conduct regular security risk analyses. The federal government also published a Cybersecurity Framework of voluntary best practices to help organizations defend against attacks.

Despite the safeguards in current law, cyber-attacks have put millions of Americans' personal information at risk. Already this year, major insurance companies Anthem and Premera have announced that they were the targets of highly sophisticated cyberattacks which compromised the personally identifiable information of nearly 90 million Americans. In the case of Premera, health information was also exposed.

To help us evaluate the efficacy of current security measures, we request that GAO conduct a study of the current health information cybersecurity infrastructure. Specifically, we request that GAO:

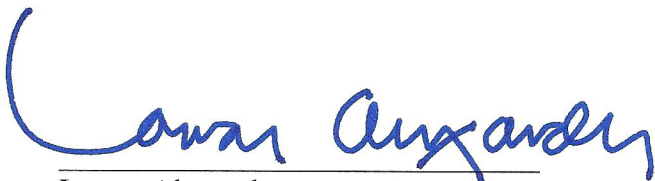
1. Identify the types of cyber threats to health IT systems and the potential consequences of such threats.

The Honorable Gene Dodaro  
Comptroller General of the United States  
April 27, 2015

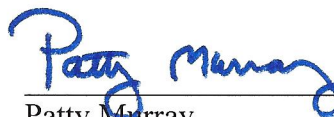
2. Determine whether any gaps or ambiguities exist in the scope and coverage of HHS' Security and Privacy Rules, HITECH Act security requirements, and the rules and guidelines established by ONC.
3. Examine the extent to which HHS and ONC oversee and monitor the implementation of – and enforce compliance with – the information security and privacy requirements. As part of this examination, GAO should assess how HHS ensures that eligible providers and hospitals, as well as other covered entities like insurance companies, have sufficiently and effectively implemented required security safeguards and privacy protections.
4. Examine issues related to industry adoption of National Institute for Standards and Technology (NIST) standards for cybersecurity. How widespread is the adoption of NIST standards in the health sector? Are standards adopted in full or in part? How frequently do organizations including eligible providers and hospitals, as well as other covered entities like insurance companies, get audited to NIST standards?
5. Conduct case studies at selected healthcare-related organizations to assess the effectiveness of their information security controls for health IT systems and privacy practices for electronic health information.

Thank you for your attention to this request. If you have any questions, please have your staff contact Virginia Heppner or Madeleine Pannell at (202) 224-5375.

Sincerely,



Lamar Alexander  
Chairman



Patty Murray  
Ranking Member