Statement of Senator Daniel K. Akaka
"Private Health Records: Privacy Implications of the
Federal Government's Health Information Technology Initiative"
Subcommittee on Oversight of Government Management,
the Federal Workforce, and the District of Columbia
February 1, 2007

Today's hearing, "Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative," will examine what actions the federal government is taking to ensure that privacy is an integral part of the national strategy to promote health information technology.

Studies show that the use of health IT can save money, reduce medical errors, and improve the delivery of health services. For example, in 2004, the Center for Information Technology Leadership estimated that in ambulatory care settings, the use of electronic health records (EHRs) would save $112 billion per year, or 7.5 percent of health care spending. In addition, EHRs are shown to help avoid duplicate tests and excess medication.

In 2004, President Bush called for the widespread adoption of interoperable electronic health records within 10 years and issued an executive order that established the position of the National Coordinator for Health Information Technology. The National Coordinator is charged with developing and implementing a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors.

Two months later, HHS released a framework for strategic action to promote health IT, which calls on all levels of government to work with the private sector to stimulate change in the health care industry. For example, the Departments of Veterans Affairs (VA) and Defense (DoD), the major federal health care delivery organizations, are leaders in the use of health IT.

VA, one of the country's largest health care providers, has had an automated information system in its medical facilities since 1985. DoD has provided IT support to its hospitals and clinics since 1968. As Chairman of the Veterans' Affairs Committee, we are looking at how to move DoD and VA forward in developing joint EHRs.

This Subcommittee is particularly interested in the strategy, which calls for the Office of Personnel Management (OPM) to use its leverage as the administrator of the Federal Employees Health Benefit Program (FEHBP), which covers approximately 8 million federal employees, retirees, and their dependents, to expand the use of health IT. OPM, through its annual Call Letter to carriers, has been encouraging carriers to increase the use of EHRs, electronic prescribing, and other health IT-related provisions.

Although I support efforts to increase the use of health IT, I am deeply concerned about the level of privacy protections in the health IT network. In 2005, a Harris Interactive survey showed that 70 percent of Americans were concerned that an electronic medical records system would lead to sensitive medical records being exposed due to weak electronic security. This fear is understandable.

Over the past few years, we have seen various data mining programs in the federal government that lacked key privacy protections. We also recall the loss of a VA laptop computer and the news of many other federal data breaches that put the personal information of millions of Americans at risk. These incidents reinforce the need to build into any system containing personal information privacy and security protections. Our personal health information must not be subject to these same failings. Privacy and security are critical elements in health IT and should never be an afterthought.

That's why I wrote to OPM in May 2005 seeking information on how federal employee's health information would be protected under the efforts of OPM and the health insurance carriers. OPM responded that the Health Insurance Portability and Accountability Act (HIPAA) would address these privacy concerns. But while HIPAA is a foundation, HIPAA by itself is not enough. Privacy protections must be built in conjunction with the development of the health IT infrastructure.

To ensure that this was happening, Senator Kennedy and I asked the Government Accountability Office (GAO) to review the efforts of HHS and the National Coordinator to protect personal health information. GAO's report, which was released this morning, found that while HHS and the National Coordinator have taken steps to study the protection of personal health information, an over-all strategy is needed to:

- identify milestones for integrating privacy into the health IT framework,
- ensure privacy is fully addressed, and
- address key challenges associated with the nationwide exchange of information.

Given the overwhelming evidence of the benefits associated with the expanded use of health IT, as well as the fact that 70 percent of Americans are concerned about the privacy of their health information, I am surprised to learn that HHS objects to this recommendation.

It is clear that the health care industry faces challenges in protecting electronic health information given the varying state laws and policies, the entities not covered by HIPAA, and the need to implement adequate security measures. But while more and more companies, providers, and carriers move forward with health IT, I fear that privacy suffers while HHS takes time to decide how to implement privacy protection. HHS must address these issues in a more timely fashion in order to give the private sector guidance on how to move forward with health IT and protect the private health information of all Americans.

I want to thank our witnesses for being here today to discuss this critical issue.