Statement of
J. Leonard Lichtenfeld, MD, MACP
Deputy Chief Medical Officer
American Cancer Society

Before the U.S. House Energy and Commerce
Subcommittee on Health
Hearing on
"Examining Federal Regulation of Mobile Medical Apps and Other Health Software"
November 19, 2013

Chairman Pitts, Ranking Member Pallone and Members of the Subcommittee, I am Dr. Leonard Lichtenfeld, deputy chief medical officer for the American Cancer Society. On behalf of the Society, I want to thank you for the opportunity to testify at today's hearing. The Society is a nationwide, community-based voluntary health organization dedicated to eliminating cancer as a major health problem by preventing cancer, saving lives, and diminishing suffering from cancer through research, education, advocacy, and service. The Society, operating through its national office and 12 geographic divisions throughout the United States, is the largest voluntary health organization in the United States.

Health information technology (HIT), software programs and mobile applications (apps) play an increasingly integral role in the care of patients, so I applaud this Committee's bipartisan attention to the question of providing the proper level of oversight. In addition to my role at the Society, I am involved with the eHealth Initiative and the Bipartisan Policy Center, where we are exploring the promise of technology for improving patient health and are working together to develop the policies needed to ensure continued progress in this direction. I am pleased to share with you my perspectives gleaned from these ongoing conversations as well as the unique cancer lens on these issues.

Cancer is the second leading cause of death in the United States, taking the lives of more than 575,000 Americans every year. Advances in cancer prevention, detection and treatment over the past 40 years have led to improved outcomes and even curative treatments for many types of cancers. That progress has been significantly aided through the use of computing and software applications. New applications will undoubtedly play an increasing role in cancer prevention, detection and treatment. While years ago it might have been enough to assess tumor size, histology and location within the body to determine the appropriate diagnosis and treatment for cancer, we are moving to an era of personalized medicine where large panels of genes are routinely assayed and processed using algorithms to determine prognosis and appropriate treatment. Imaging hardware paired with the latest software can now detect differences in MRIs or tissue samples that may not be visible to the human eye. These new imaging techniques can

also be performed in less time than through traditional human methods. The explosion of computing power has increased our ability to quickly and accurately diagnose patients, predict disease trajectory and develop the most effective treatment plans. With this promise, the development of ever more powerful HIT and software applications is an urgent priority for cancer patients and survivors.

Our optimism for the power of HIT and software applications to improve patient care, however, must be tempered by the potential dangers that come with any new medical intervention. We would consider it unethical to administer new drugs or devices as part of a patient's treatment without first understanding the safety and efficacy of these interventions in treating a specified disease. In the same manner it would be unacceptable to integrate software applications directly into patient care, whether diagnostic, prognostic, or therapeutic, without first understanding the safety and efficacy of those applications or the implications for patient privacy. A determination of safety and efficacy requires some form of appropriate oversight.

The spectrum of HIT and software applications, which ranges from the billing software used in the administration of a doctor's office to the software that is actively controlling a respirator sustaining a patient's life, merits different levels of oversight. The idea of risk-based oversight is widely embraced by multiple sectors within the medical community and shares bipartisan support. You will find nearly universal agreement that scheduling and billing software does not merit Food and Drug Administration (FDA) clearance and that diagnostic imaging software does merit FDA oversight. The real challenge lies in creating the risk-based paradigm to calibrate oversight for everything in between.

The types of applications that fall into this zone of uncertainty could include, for example, clinical decision support or mobile apps that guide patient self-therapy. For each of these examples there are instances where the application in question could pose little risk, or instances where it could pose grave risk. Clinical decision support that uses data from electronic health records to calculate BMI and suggests that a physician discuss weight loss strategies with an overweight patient is very different than decision support that incorporates several dozen variables ranging from histology reports, genetic tests and imaging reports to deliver a cancer diagnosis, prognosis and suggested treatment protocol. A self-therapy mobile app may be relatively harmless if it is suggesting exercise to improve fitness, but it may pose serious risk if it is recommending insulin dosing. In these cases, creating definitions for broad categories of apps does not necessarily provide adequate illumination of the risk posed by individual products within those categories, so someone must be the umpire for individual cases.

I was recently part of a Bipartisan Policy Center initiative that examined what a risk-based regulatory paradigm for HIT might look like that would involve three different categories of oversight. The current FDA guidance has also endorsed a risk-based paradigm with three categories of oversight for HIT, software and mobile apps, one category clearly subject to strict FDA regulation, one subject to regulatory enforcement discretion based on risk, and one category not subject to FDA oversight. Lastly, bipartisan legislation introduced by several members of this committee has similarly proposed a multi-tiered model for a risk-based oversight paradigm. These three models use different approaches including statutory changes, sub-regulatory guidance, and partnership with professional organizations. Regardless of the

approach taken, I would like to offer several considerations that must not be overlooked in the design of a new model.

Patient safety and privacy are paramount. Medicine is performed in the service of patients and it is the first duty of medical professionals, Congress, and the relevant oversight agencies to ensure that patients are not subjected to dangerous, ineffective, or misleading treatment, and that their information is secure. Wherever medical software or mobile apps are involved in diagnostic, prognostic, or therapeutic decisions, oversight is not only appropriate, but necessary.

Any oversight system should be fluid. Technology is advancing at a speed that challenges our ability to provide effective oversight. Some of the technology in use today was almost unheard of five years ago. While it is possible to create systems to address today's technologies, any oversight structure should not be so rigid that it cannot quickly adapt to new realities.

Details matter. If changes are enacted to create new categories of medical software applications with differing levels of oversight, then the definitions of those categories must be very clear and not create loopholes, ambiguities, or unintended consequences. Many software applications contain multiple functions, and each individual function in isolation could conceivably fit into a different regulatory category, so clarity about where in the regulatory scheme these multi-functional applications fit is needed. Furthermore, software is currently considered a device by the FDA, so without changing the existing paradigm by redefining devices in statute to explicitly exclude software, new categories may simply cause confusion rather than clarity. In other words, creating a new category of "Software that is not a component of a device…" could be seen as a circular definition given that software is currently seen as a type of device.

Focus the solution on the actual problem. Innovation in HIT, software, and mobile apps can be promoted through regulatory certainty and the relief of regulatory burden on sectors of HIT where it is not appropriate. (As noted above, however, this cannot take precedence over patient safety.) Targeted changes aimed at narrow sets of software and mobile apps may provide the desired regulatory certainty while lowering the chance of unintended consequences rather than creating an entirely new paradigm for the full spectrum of HIT, software and mobile apps.

Lastly, I suggest that a new model of oversight be well-informed by the health IT regulatory strategy report commissioned by the Food and Drug Administration Safety and Innovation Act (FDASIA) that is being prepared jointly by the FDA, the Office of the National Coordinator for Health Information Technology, and the Federal Communications Commission. Like you, I will be eager to read the findings when it is issued in the next few months.

Conclusion

In closing, I would like to reiterate the vital role of HIT, software programs, and mobile apps in making progress against cancer and ensuring patient safety. There is broad recognition that not all software applications pose the same risk to patients; therefore, there needs to be a risk-based paradigm for calibrating the appropriate oversight. We do not want a heavy regulatory hand to stifle innovation, but we must never allow the pursuit of innovation to displace patient safety and

privacy as our primary considerations. When software or mobile apps have the potential to affect patient health, someone must be on the watch.

Thank you again for the opportunity to share our views.