Congress of the United States
Washington, DC 20515

September 18th, 2014

The Honorable Sylvia Mathews Burwell
Secretary of Health and Human Services
United States Department of Health and Human Services
200 Independence Aveenue, S.W.
Washington, D.C. 20201

Dear Secretary Burwell,

Today there is an unprecedented boom of innovation in America. Mobile apps have grown into a $68 billion industry in just six years. The mobile health sector is growing even faster. Many medical professionals are putting these technologies to use in their practice, and the American public is increasingly adopting mobile apps to monitor their own health. Unfortunately, in some cases, the federal regulatory environment has not kept pace with this progress.

We support the privacy protections provided by the Health Insurance Portability and Accountability Act ("HIPAA"), and we recognize that oversight of highly sensitive personal medical information is an important role for HHS. In order to make sure that mobile health apps and other companies can in good faith comply with these important protections, we ask that HHS provide clear, easily accessible and up to date regulatory guidance for HIPAA compliance with regard to new technologies.

Documentation on the Health and Human Services ("HHS") website outlining technical compliance with HIPAA has not been updated since 2006, years before an app store existed, much less the modern mobile device. Many companies creating mobile health apps have told us that they want to fully comply with HIPAA regulations, but have difficulty confirming that they have done so because current regulatory guidance does not cover technologies that they are using. In some cases small technology companies have reported having to hire large legal teams just to determine, with some level of certainty that their product is in compliance with HIPAA. In order to ensure that innovative health companies do not inadvertently run afoul of the law, regulatory guidance should be routinely updated to reflect modern technologies being used in the health field.

We believe there are several steps HHS should take to ensure that mobile app developers and other new health technologies can easily determine if they are compliant with HIPAA:

1.) **Updates**: We ask that HHS provide up to date, clear information about what is expected of companies to be in compliance with HIPAA. This should include new technologies such as mobile apps. Updated guidance should also address new types of information

storage. Routine updates to regulatory guidance should continue in order to keep pace with advances in technology.

1.) **Implementation Standards**: The Office of Civil Rights (OCR) housed at HHS should clearly identify implementation standards that can help companies conform to regulation and avoid enforcement action.

2.) **Cloud Clarity**: A growing number of mobile health companies store encrypted health data in remote storage centers. These storage providers do not have an encryption key and cannot access the data. Yet, questions remain about their HIPAA obligations for information they technologically cannot access. HHS should provide clarity about the HIPAA obligations for companies and services that store data on the cloud.

3.) **Compliance Assistance**: HHS should also strive to make it as easy and clear as possible for companies and individuals operating in good faith to comply with its regulations. We would like HHS to assign employees with technological expertise to regularly engage with companies in the emergent healthcare technology space. These employees should be prepared to work with app developers and others to make sure that products incorporate HIPAA protections beginning at the early stages of product development. HHS should also consider, if feasible, providing a voluntary badge program for companies seeking to prove compliance with HHS rules and regulations. This would allow American healthcare companies to be more competitive in foreign and domestic markets and would provide an economic incentive to follow important safeguards for the benefit of patients.

We thank you for your attention to these issues and look forward to continuing the dialogue about how we can best ensure that new technologies are able to easily comply with privacy laws.

Sincerely,

TOM MARINO
Member of Congress

PETER DEFAZIO
Member of Congress