Questions for the Record – Responses from Paul Misener, Vice President, Global Public Policy, Amazon

The Honorable Joe Pitts:

Q 1. You mentioned the CDC's use of cloud for providing awareness for health-related threats and to support responses to these threats – how has the cloud strengthened our emergency response system to maximize our emergency operations health care delivery system?

More details about Amazon's work with the CDC are available here: http://aws.amazon.com/solutions/case-studies/us-centers-for-disease-control-and-prevention/

With the organization's BioSense 2.0 program, the CDC is tasked with providing awareness for all health-related threats and to support responses to these threats at the national, state, and local level. Needing to avoid purchasing expensive hardware and software, the organization turned to AWS for its low cost, pay-per-use model of cloud computing services, which has helped to enable this system with high availability and security, and improved agility.

Q2. Are there other nations that have utilized the cloud for their research? What could this mean for working with other nations and global clinical trials?

There are over 800 government agencies and 3,000 educational institutions worldwide that currently leverage cloud computing services from AWS. One example is how the Centre for Software Practice (CSP) at the University of Western Australia is leveraging cloud services to enable research into the impact of technology on online communities, open source development, and health informatics, at a much lower cost. More information is available on this case study here: http://aws.amazon.com/solutions/case-studies/university-of-western-australia/

Q3. Are there any laws or regulations that have impacted the development of cloud?

As suggested in my July 17 testimony, Congress could work with the Department of Health and Human Services (HHS) to modernize implementation of the Health Insurance Portability and Accountability Act (HIPAA) so that healthcare providers can readily employ the benefits of cloud computing without any compromise of the strong privacy protections HIPAA now affords health information.

Q4. Amazon worked with the FDA to turn 900,000 hand written reports of adverse drug effects each year into machine-readable information with 99.7 percent accuracy, reducing costs from 29 dollars per page to 25 cents per page. This cures initiative is in part focused on using technology to relieve administrative burdens for agencies such as the FDA so they can use those resources to invest in more researchers or new development methods such as biomarkers.

Do you have suggestions for other ways we can increase the efficiency at the FDA and other agencies?

One area where CIOs should be given more authority and flexibility is with respect to spending models, specifically capital expenditures (CAPEX) versus operating expenditures (OPEX). Given that much IT hardware and software has only a three-year lifecycle, agencies should be allowed to place capital funds into "Working Capital Funds" that preserve the funding for the agency to pay in multiple

years for cloud computing services based on what they actually use. The current "use or lose" approach is a disincentive to saving money. Agencies should shift to paying only for what they use in OPEX, versus spending in CAPEX to stockpile servers, software, etc., because their budgets expire at the end of a fiscal year.

Also, to help accelerate the discovery and development of new biomedical treatments and cures, Congress could enact H.R. 967, the Advancing America's Networking and Information Technology Research and Development Act (one section of the bill would require an assessment of how federal science agencies can facilitate the use of cloud computing for federally-funded science and engineering research).

How can we modernize HIPAA to ensure that patient information is protected but we can utilize data?

Amazon fully supports the need for strong protection of the privacy and security of health information. However, there are areas where the HIPAA statute and regulations are a poor fit for cloud computing services. For example, the HHS Office for Civil Rights indicated that a cloud provider is subject to HIPAA as a "business associate," even where the information is encrypted and the cloud services provider does not have the decryption key. This impedes health care entities from leveraging the cloud, causing the parties to negotiate a "business associate agreement" in which virtually all of the terms are inapplicable because the cloud services provider does not have access to the information. Additionally, the HITECH Act provides that an entity is subject to substantial HIPAA penalties even if it did not and reasonably could not know of a HIPAA violation. HHS has broadly interpreted that an entity becomes subject to HIPAA when they maintain protected health information on behalf of a HIPAA covered entity, regardless of whether they agreed to do so in a business associate agreement or otherwise.

Congress can play a critical role in facilitating health care's greater use of cloud computing services by addressing some of these regulatory challenges, including excepting from HIPAA entities that: (1) maintain encrypted information but do not have the technical ability to access the information; or (2) have received no notice that they have received HIPAA-covered health information. By narrowing the application of HIPAA to situations where the cloud provider has access to the information and knowledge of the information, parties can avoid wasting money on contracts that are mostly inapplicable and cloud service providers can more reasonably comply with HIPAA by focusing on areas where they have been informed that health information resides.

Q5. How should we encourage academic researchers to utilize the cloud? What are the reasons researchers wouldn't want to utilize the cloud?

Congress could work with the National Institutes of Health (NIH) to establish and operate cloud-based data management platforms, which federally funded researchers could use to share their data. If federal funding agencies, such as NIH, established and operated cloud-based data management platforms, federally-funded researchers would simply upload their research data along with any relevant software resources required to reproduce their analysis of the data. Other researchers in the field could then access the data and software in order to reproduce results, re-analyze previously collected data in novel ways, or even automate the analysis of new data using the same approach as the original

experiment. This would result in the elimination of costly and unnecessary duplicative research and thereby accelerate the pace of biomedical discovery.

More and more researchers are using AWS and our pay-per-use model of cloud computing services and are significantly lowering costs and enabling greater innovations in the process. However, one challenge that federally funded research organizations and researchers still face is that the federal funding process still enables more capital expenditures (CAPEX) then operational expenses and significant amounts of research dollars are allocated for hardware and software expenditures or related overhead costs. If there is more emphasis by federal researching funding agencies on the use of cloud computing services via operating expenditures (OPEX), recipient organizations can spend less on capital expenditures to buy equipment and can invest more on the actual research.

The importance of the utility-based model of cloud computing on Page 41 of the President's FY2015 Budget Request:

Expanding Federal Cloud Computing.

The Budget includes investments to transform the Government IT portfolio through cloud computing, giving agencies the ability to purchase IT services in a utility-based model, paying for only the services consumed. As a result of the Administration's Cloud First policy, Federal agencies adopting cloud-based IT systems are increasing operational efficiencies, resource utilization, and innovation across the Government.

The Honorable Joe Barton

Q2. Please provide us with examples of how we can "modernize" the implementation of HIPAA? Are you suggesting weakening the law or creating some sort of loophole as it relates to privacy? Please provide examples of when cloud-computing services would not have access to, or knowledge of, the information stored on their services and would therefore have no responsibility as relates to any sort of breach of data or security vulnerability?

Amazon fully supports the need for strong protection of the privacy and security of health information. However, there are areas where the HIPAA statute and regulations are a poor fit for cloud computing services. For example, the HHS Office for Civil Rights indicated that a cloud provider is subject to HIPAA as a "business associate," even where the information is encrypted and the cloud services provider does not have the decryption key. This impedes health care entities from leveraging the cloud, causing the parties to negotiate a "business associate agreement" in which virtually all of the terms are inapplicable because the cloud services provider does not have access to the information. Additionally, the HITECH Act provides that an entity is subject to substantial HIPAA penalties even if it did not and reasonably could not know of a HIPAA violation. HHS has broadly interpreted that an entity becomes subject to HIPAA when they maintain protected health information on behalf of a HIPAA covered entity, regardless of whether they agreed to do so in a business associate agreement or otherwise.

Congress can play a critical role in facilitating health care's greater use of cloud computing services by addressing some of these regulatory challenges, including excepting from HIPAA entities that: (1) maintain encrypted information but do not have the technical ability to access the information; or (2) have received no notice that they have received HIPAA-covered health information. By narrowing the application of HIPAA to situations where the cloud provider has access to the information and knowledge of the information, parties can avoid wasting money on contracts that are mostly inapplicable and cloud service providers can more reasonably comply with HIPAA by focusing on areas where they have been informed that health information resides.