User Scope

1. PHR providers will often push new capabilities or updates that affect the privacy and security of consumers' data. While the difference between an update and a new capability is sometimes unclear and the definition of an update versus a new capability may vary in the industry, it may be beneficial to describe in the Privacy Notice the consumer notification actions the company will take when either of these events occur.

Information Type

1. The list of data elements considered to be "PHR Data" appears to be too broad. Credit card numbers and GPS data should not be within scope although they may be necessary to facilitate the initial collection of data. PHR Data should be restricted to data elements that "uniquely" identifies an individual or when used in aggregate with other data elements uniquely identifies a specific person; this does not appear to be the case for "cookie" preferences or with IP addresses:

    a. The IP address used by a particular individual may be shared by others, such as the use of a computer in a public library; which may affect the integrity of the data.
    b. The IP address used by a particular individual may be shared by a family member with the same name (ex. Jr. Sr., etc.).
    c. In today's Internet of Things (IoT) world, there may be several IP addresses associated to one individual or multiple individuals simultaneously.

Information Practices/Access to Other Device Information

2. It would be useful for consumers to know whether the PHR company will aggregate data from other sources not specifically connected to the PHR device in its attempt to derive insight into or make decisions about or on behalf of the consumer (a type of big data analytics).

Sharing and Storage

3. The current system lacks clarity regarding the use and disclosure of data once the company that owns the PHR is sold or acquired or has some other significant change in ownership status. A customer's meaningful choice selections or data use and disclosure selections should not change based on changes in ownership; customers should be given the right to re-establish their meaningful choice selections once changes in ownership occur, if the new owners will use or disclose data differently.
4. The DHA Privacy and Civil Liberties Office affirms the criticality of notifying customers where data is being stored and specifically whether data is being stored on the cloud or using servers outside the United States. DoD currently has restrictions in place to limit the use of servers outside the US and also has rules regarding using the cloud to store data. Companies that provide PHRs are likely to obtain data from multiple family members, including active duty military personnel. Health purchase decisions are often made by spouses who may not be aware of specific military requirements.

Security and Encryption

5. The strength of user authentication to access the device or application should be addressed (for example, password strength). This is the first line of defense to safeguard customer's information.

6. As addressed by ONC, bit encryption does not provide most consumers with sufficient information to make an informed decision since they are generally unaware of the relative difference in protection between 128 and 256 bit encryption. Perhaps, the number could be associated with a qualifier such as “highest” or “lowest” level of encryption commercially available, or the encryption bit strength should be “pegged” to a Federal standard such as the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), a U.S. government computer security standard used to accredit cryptographic modules.
7. It is difficult for the average consumer to deduce an overall risk level by reviewing individual responses on the Model Notice. The security that a consumer is expecting should be linked to risk levels. Using the example that is often cited, with the Model Notice being likened to the FDA nutrition facts label, then there needs to be a consistent standard or objective reference model if you will, similar to the “% Daily Value.” This type of objective reference provides the uninformed consumer at a glance, the ability to identify the risk(s) associated with the PHR.