Comments to the EC Green Paper on mHealth

Submitted by the International Pharmaceutical Privacy Consortium

I. Introduction

The International Pharamaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data protection professionals from nineteen research-based global pharmaceutical companies, all of which conduct business in the European Union. The membership and mission of the IPPC is described in Attachement A. We appreciate this opportunity to provide feedback on the European Commission's "Green Paper on mobile Health ('mHealth')" COM (2014) 219.

II. IPPC Comments

The European Commission's Green Paper on mHealth provides a welcome opportunity to discuss the innovative and rapidly growing field of mobile health solutions. As the Commission noted throughout the Green Paper, mHealth represents an exciting opportunity to promote efficient, sustainable health care that empowers patients and improves patient outcomes. Mobile health solutions have a dramatic impact on the speed and efficiency of medical care and can be valuable tools to help patients adhere to prescribed treatment. Medical mHealth solutions will in the future help patients, doctors, caregivers and others to improve health and reduce costs.

The Commission's paper includes and requests feedback on a number of specific questions. The IPPC wishes to addess the following two questions, presented by the Commission on page nine of the paper.

1) "Which specific security safeguards in mHealth solutions could help to prevent the unneccessary and unauthorised process of health data in an mHealth context?"

The IPPC believes that many of the safeguards currently developed to protect consumer privacy in other contexts are equally efficacious when applied to mHealth. Data encryption, secure hashing, data collection minimisation, and other common approaches to protecting patient and consumer safety will also serve to protect consumers in the mHealth context.

When developing mHealth applications and devices, it is important that developers follow a Privacy-by-Design approach. This requires consideration of what personally identifiable information is necessary to fulfill the stated purpose(s), and then limiting data collection to just that information. It also requires consideration of what privacy and security controls can be reasonably implemented to protect the confidentiality of data collected and limit its use to legitimate, authorized purposes. Finally, PbD approaches involve providing notice to users of what data will be collected, and, where feasible, providing users with meaningful

choices as to whether to provide the data. Depending on context, these notices may be incorporated into a privacy statement that accompanies the mHealth app/device, or they may need to be provided "just-in-time" (e.g., alerts provided at the point of use of a feature).

It is important to note, in addition, that pharmaceutical companies are already subject to comprehensive regulatory and ethical requirements designed to protect patient privacy. These requirements apply regardless of whether the patient's information arrives via an mHealth solution or a more traditional route.

2) "How could app developers best implement the principles of 'data minimisation' and of 'data protection by design,' and 'data protection by default' in mHealth apps?"

The IPPC would like to call the Commission's attention to the Groupe Speciale Mobile Association's ("GSMA") *Privacy Design Guidelines for Mobile Application Development* ("Guidelines").[1] The GSMA's guidelines contain recommendations for mobile application developers on designing applications that give users control over privacy settings and data flows. The Guidelines reflect a "*Privacy by Design* approach and are intended to help ensure that mobile applications are developed in ways that respect and protect the privacy of users and their personal information." The IPPC also suggests that the Commission take note of the CTIA – The Wireless Association's *Best Practices and Guidelines for Location Based Services*,and the Mobile Marketing Association's *Mobile Application Privacy Policy Framework*.[2] Although these documents are not specifically tailored to mHealth applications, they represent compilations of best practices applicable to privacy and mobile applications generally. These best practices should serve as a baseline for further conversations about mHealth.

The IPPC also wishes to note that the use of Privacy Impact Assessments (PIAs) can be an effective tool to ensure that apps have undergone appropriate data protection vetting prior to release to the public. A PIA is an analysis of how personally identifiable information is collected, used, shared, and maintained. A PIA can be used to demonstrate that a developer has consciously incorporated privacy protections throughout the development life cycle of an mHealth app.

The IPPC is supportive of efforts to harmonize data protection requirements through the adoption of an EU Data Protection Regulation. The inconsistent application of privacy requirements among EU member states impedes innovation and risks leading to uneven playing fields. Similarly, standards for health information systems interoperability will be important to ensure compatibility.

The IPPC supports efforts to further harmonize data protection requirements applicable to mHealth applications. Commission guidelines in this area could be extremely valuable, both to harmonize requirements and to ensure that all application developers are aware of regulatory

[1] A copy of these guidelines is available here: http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf

[2] These documents are available, respectively, here: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf , and here: http://www.mmaglobal.com/education/bestpractice

expectations. Commission consideration of stakeholder input in the development of such guidelines will be critical to ensure they support rather than hinder innovation.

Finally, the IPPC wishes to offer three general observations on the Commission's paper.

First, many of the sources cited by the Commission expressed concern about apps which may make scientifically unsupported claims of benefit to consumers and patients. The IPPC shares these concerns, but wishes to remind the Commission that many of those same sources also singled out a number of mHealth applications as beneficial and useful to patients. *See, for example, New England Center of Investigative Reporting,* "Lacking Regulation, Many Medical Apps Questional at Best" (noting that there are "many outstanding health apps" which could help to "revolutionize medical care"). The world of mHealth is rapidly evolving and changing, and the IPPC hopes that the Commission will adopt an approach that allows those apps of real benefit to patients and consumers to flourish.

Second, the IPPC notes that the several of the sources the Commission cited on the prevelence or use of mHealth solutions may no longer be current. Recent research suggests that consumer use of cell phones for health purposes has rapidly increased over the last few years. *See, for example,* Pew Research Internet Project, *Mobile Health 2012* (noting that from 2010 to 2012, use of a cell phone to access health information increased from 17% to 34%). Further, some of the statistics cited by the Commission do not clearly distinguish between cell phone users generally and smartphone users. For clear reasons, smartphone users are significantly more likely to use mobile health solutions than cell phone users generally. *Id.* (noting that 52% of smartphone users have used their phone to access health information, as compared to 6% of other cell phone users). The IPPC suggests that the Commission expect rapid growth in the use of mHealth solutions, as smartphone usage continues to increase.

Third, it is important to emphasize that mHealth applications may use data in different ways. Sometimes the data will be stored on the user's mobile device alone, while in other settings, the data may be backed up to a third-party data storage solution. Other applications will only accept data inputted directly by the user on a specific device, while in other cases the application will have an interface that allows the user to input the data from another computer or device. The Commission should also note that some mHealth solutions may not even be true "apps," but are rather mobile-enabled website interfaces that can be easily used from a mobile device. The Commission should take all of these approachs to mHealth data flows into account when crafting any new policy.

The IPPC appreciates this opportunity to provide feedback on the European Commission's Green Paper on mHealth. Please feel free to contact us with any questions on this submission or our position or practices related to mHealth more generally.

APPENDIX A: INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

MEMBERS

The IPPC is an association of companies that face worldwide responsibility for the protection of personal health information and other types of personal data. Members of the IPPC include:

- AbbVie
- Amgen
- Astellas Pharma, Inc.
- AstraZeneca Pharmaceuticals
- Baxter International, Inc.
- Bristol-Myers Squibb
- Celgene
- Eli Lilly and Company
- Genentech/Roche
- GlaxoSmithKline
- Johnson & Johnson
- Merck & Co., Inc.
- Novartis
- Novo Nordisk
- Otsuka America Pharmaceutical, Inc.
- Pfizer Inc.
- Sanofi
- Shire
- Takeda Pharmaceuticals

MISSION

The IPPC works to promote responsible privacy and data protection practices by the global pharmaceutical industry. Maintaining data confidentiality and subject privacy are essential to clinical research, pharmacovigilance, and other activities of the pharmaceutical industry. The IPPC seeks to increase awareness of privacy and data protection issues and to engage government in a dialogue about the need for data to support cutting edge biomedical research and other public health activities. The IPPC pursues opportunities to collaborate with government and other stakeholders to develop data protection practices that enhance data subject privacy.

GOALS

The IPPC goals are to:

- Engage government and stakeholders in the biomedical research and healthcare communities in a constructive dialogue on significant issues of privacy and data protection.
- Serve as a resource for sound analyses of privacy and data protection requirements and compliance tools tailored to the pharmaceutical industry.
- Serve as a forum for industry dialogue and promote responsible privacy and data protection practices.
- Promote consistent privacy and data protection standards that can be achieved on a worldwide basis.

- Remain on the leading edge of privacy and data protection.

SCOPE OF ACTIVITIES

The IPPC advances understanding of existing and emerging data protection and security rules in Europe, the US, and other key countries. The Consortium engages regulators and policymakers in the following areas:

- Biomedical research
- Pharmacovigilance
- Sales and marketing
- Market research
- Human resources programs
- Other corporate programs