# Frequently Asked Questions For Mobile Health Informatics 2013.1 Version Release 1

## HL7 Project Management Office
## mHealth Security Subgroup

Version: HL7 mHealth Security FAQ Statement v2013.1.1

**Point of Contact Name and Email:**
**Paul Petronelli (palm@palmcorp.com)**

**Publication Date: May , 2013**

The objective of this list is to provide a useful resource for product development groups considering security issues in the mobile health informatics product area. .

## Contents

# Introduction

## *Scope*

In addition to an active Wiki posting, the subgroup will publish an annual FAQ (Frequently Asked Questions) document which explains answers to design, implementation, test, evaluation, and compliance and verification .security questions dealing with mobile application, appliance and information systems product development.

## *Project Need*

This is a young evolving market space. As a result, security issues for mobile health informatics are changing and evolving along with the technologies involved and the information science applied. This space, that is the security space, is under constant attack from a variety of threats as well as the danger of breach of confidential information. These aspects of the market provide the motivation for this effort.

## *Success Criteria*

This effort will be considered successful when product developers consistently turn to the FAQ for answers to their design, implementation, test and validation issues. This success will be measured by the feedback received on the questions posted. Developers will be encouraged to contribute new questions, comment on existing questions and provide review of published answers.

## *Project Objectives / Deliverables / Target Dates*

| | |
|---|---|
| Objective: publicise the FAQ on the HL7 wiki<br>Deliver a refereed white paper at the end of each year summarizing the FAQ questions/answers | End of 12 month cycle |
| Publication 1 and Wiki posting of the evolving FAQ. | End of 12 month cycle |
| Publication 2 and Wiki posting of the evolving FAQ. | End of next 12 month cycle |
| Publication 3 and Wiki posting of the evolving FAQ. | End of next 12 month cycle |

## Contributions

David Gobuty, February 4, 2013

**mHealth Identification**

*What is identification in the realm of MHealth Devices?*

Identification enables the device to present controls and displays tailored to the work the user intends to perform with it. It also links the identification to the record of actions performed using the device.

*How does identification differ from authentication?*

Identification begins to form a link between the device and a specific user (or users), while authentication raises likelihood to an acceptable level that the user (or users) are who they claim to be.

*Why require an identification step?*

Identification can enable presentation of role-specific controls and displays. In this way it can manage access to controls and displays for which an identified user is not privileged to use or see. For example, identification as a general user can preclude changes to the audit record, a privilege that would be available only to an administer user (whose identification would be added to the audit record as the one who made the change).

*Is identification necessary for a personal MHealth device?*

Identification can occur concomitantly with authentication providing the number of users is small (one or two individuals), provided the automated identification controls against change to sensitive audit records. Identification can require specific action to gain privilege to use controls and view displays that should be reserved when the single user wants to acting as an administrator. This can prevent inadvertent changes to device settings or audit records.

*Does a MHealth device need an identification step if used by more than one person?*

Yes, because the audit record must contain the identification of the user responsible for the recorded event.

*How is identification used in a MHealth device?*

Identification enables role-based management of controls, displays and privilege available to a specific user.

*Can identification and authentication be performed in a single step?*

In personal MHealth devices, where the user population is small (one or two individuals), the identification and authentication steps can be performed in a single action, provided there are measures in place to control against manipulation of audit records.

Nadine Contribution

1. Can identification be tied to SIM (Subscriber Identity Module) card of the user mobile device?
   This would enable the user to access Personal health Records from his/her device.

2. What are the safeguards to protect the patient's data if the device is stolen?

3. What kinds of authentication/authorization could be used in this scenario to verify that the person accessing the information is actually the intended user?

4. Can biometrics be used?
5. Will the data be encrypted during transit?
6. Will the data be encrypted at rest?
7. How do you prevent replication of PHR data onto unsecure platforms or environments?

jBrandt Contribution
There are new platforms that are entering the discussion such as Samsung SAFE that provide an environment of security. There are also companies such as Box that claim that their systems are HIPAA compliant. We may want to look into what this really means for the security of PHI

Discussion with Nathan
I'm not sure I understand your question Jeff. When you say "organizations" do you mean such as eligible providers?

If so, then if patient data passes through the app developers systems in any way, then according to the recent Omnibus they would need to have a BA in place with them. If it is only that the application is being purchased and installed locally then I would think not. In that case, providers would just need to make sure that the general contract for the purchase confirms that it passes all OCR requirements and would need to.

What Box seems to be implying though is that data stored by them for your organization is HIPAA compliant. This is the quote from their literature: "Box supports HIPAA and HITECH compliance following the Department of Health and Human Services' publication of the Omnibus Final Rule in January of 2013. Box also signs HIPAA Business Associate Agreements (BAAs) with customers."

On Fri, May 24, 2013 at 11:24 AM, J Brandt <jbrandt@comsi.com> wrote:
There are a lot of apps on the market that claim security, however there is not way to confirm. Box with sign a BA with the developers; I assume organizations should have BA with the App developers??
Jeff

**John Moehrke, John (GE Healthcare) Contribution**

I would like to see something even more fundamental. I presented the following at the HL7 meeting in the Security wg free Wednesday tutorial. It speaks of very basic mobile device security and points at NIST 800 documents for details. This helps set the ground work for the later discussion on specifics of user identity, and application identification...

http://healthcaresecprivacy.blogspot.com/2013/05/security-tutorials-on-mhealth-security.html

# List of useful References

### *Tutorial*

http://healthcaresecprivacy.blogspot.com/2013/05/security-tutorials-on-mhealth-security.html

### *Standards*

### *Industry Agreements*

### *HL7 Organization*