Centre universitaire de santé McGill

McGill University Health Centre

Projet OPAL

Enjeux en matière de sécurité de l'information

Mars 2016
v. 1.0

CONFIDENTIEL CUSM

Pondin Lacina Koulibaly
Arnaud Palisson, PhD
Conseillers, Sécurité de l'information
Gouvernance en sécurité de l'information

Cette page a été laissée vierge intentionnellement.

SOMMAIRE

Il a été demandé à notre service d'évaluer les enjeux de sécurité de l'information du projet *MUHC Oncology Patient Application* (*OPAL*), en cours de développement au *Centre du cancer des Cèdres* du CUSM.

1 Fonctionnalités de l'application

À cette fin, nous avons effectué diverses recherches et mené des entretiens avec l'équipe du projet et le service de soutien de *Firebase*,. Il en ressort les éléments suivants.

Dans sa **version initiale**, l'application *OPAL* échangera – entre les serveurs du CUSM et l'application installée sur l'appareil mobile du patient – les informations suivantes :

- Renseignements personnels du patient :
  - Nom, prénom
  - Photo
  - Numéro de dossier médical
  - Adresse courriel
  - Numéro de téléphone
- Données sur les rendez-vous :
  - Type de rendez-vous
  - Date
  - Nom du médecin concerné
  - Lieu du rendez-vous
  - Bouton d'enregistrement (avec affichage des délais d'attente)
- Informations de diagnostic
  - Diagnostic
  - Degrés
  - Étapes,…
- Planification du traitement :
  - Date
  - Tâche à effectuer
- Documentation
  - Notes du médecin
  - Plan de traitement (avec affichage des délais d'attente)
  - Images documentant l'établissement du traitement
  - Rétroaction du patient, par questionnaire, sur des questions non médicales (retour d'expérience sur l'application *OPAL*,…)

Dans une **version ultérieure**, l'application devrait comprendre également les informations suivantes :

- Résultats de tests sanguins
- Messages échangés entre le patient et le médecin (par messagerie instantanée)
- Échange de documents (textes, images, vidéos) en pièce jointe de ces messages instantanés
- Rétroaction du patient, par questionnaire :
    - retour sur le traitement
    - retour d'expérience sur le service de cancérologie.

On compte donc diverses **informations confidentielles** (renseignements personnels et de nature médicale) qui font l'objet d'une protection accrue aux termes de la législation relativement à leur hébergement sur une plateforme infonuagique telle que *Firebase*.

2 Enjeux de confidentialité

2.1 Localisation du site physique d'hébergement des données dans *Firebase*

La base de données *Firebase* est hébergée sur des serveurs de la compagnie du même nom, affiliée à *Google*. Il est impossible de déterminer avec certitude dans quel(s) pays se situent ces serveurs (qu'ils soient opérationnels ou éventuellement de redondance).

Toutefois, cela ne constitue pas un obstacle à l'utilisation de la solution *Firebase*, dès lors que les informations sensibles qu'elles traitent sont adéquatement protégées.

2.2 Protection des données

En effet, le projet *OPAL* prévoit deux couches de chiffrement :

2.2.1 Chiffrement symétrique avant transfert

Avant d'être envoyées vers *Firebase*, les informations sont chiffrées :

- par le *listener*, sur les serveurs du CUSM
- par l'application, sur l'appareil mobile du patient.

L'algorithme de chiffrement est AES 128.

Ce chiffrement est opéré par le CUSM et **non par la solution infonuagique elle-même**. Cela permettrait au projet de respecter les exigences légales et jurisprudentielles en la matière.[1]

[1] Nicolas Vermeys, Julie Gauthier et Sarit Mizrahi, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec*, Laboratoire de cyberjustice, document de travail no 11, 10 juillet 2014, p. 131-132.

2.2.2 *Chiffrement asymétrique du transfert*

Les échanges entre *Firebase* et le *listener* d'une part, et l'application d'autre part, sont sécurisés par le protocole TLS 1.2.

En outre, il faut signaler que les informations transitant par *Firebase* y demeurent pour une durée extrêmement limitée, variant entre :

- une fraction de seconde[2] – lorsque la connexion entre l'application et le *listener* fonctionne correctement –
- et cinq minutes – lorsque la connexion est perdue en cours de transfert. Le système prévoit l'effacement automatique des informations à l'expiration de ce délai.

2.2.3 *Pas de chiffrement après transfert*

Une fois les informations transmises à l'application de l'appareil mobile, elles sont stockées localement de la façon suivante :

- Les fils de données (*string data*) sont conservés en mémoire locale de l'appareil
- Les documents sont conservés en mémoire "persistante".

Dès que l'usager déconnecte l'application OPAL, la mémoire locale est effacée, mais la mémoire persistante demeure. Cette mémoire persistante n'étant accessible que depuis l'application, il ne serait pas possible d'y accéder une fois OPAL déconnectée.

Toutefois, il ne s'agit pas là d'un volume chiffré mais seulement verrouillé, ce qui signifie que si l'appareil mobile est débridé (procédé de *jailbreak*), il serait alors possible d'accéder aux données de la mémoire persistante depuis l'*iPhone*.

Le problème existe à l'identique avec l'application *Android*.

Dès lors, il est nécessaire que ce volume de mémoire soit **chiffré**.

2.3 Exploitation des données par *Google*

Même s'il le souhaitait, *Firebase* (*Google*) ne serait pas capable d'exploiter les informations transitant par ses systèmes, car elles sont chiffrées par le CUSM avec un robuste algorithme de cryptage.

[2] Ce que nous avons pu constater *de visu*, lors d'une démonstration effectuée par les responsables du projet.

2.4 Gestion des accès

2.4.1 Identification

Le patient se connecte à *OPAL* en entrant dans l'application :

- un identifiant : son adresse courriel
- un mot de passe :
  - ce dernier est établi par le patient lors de son enregistrement dans le système, à l'hôpital. Le mot de passe est **conservé après hachage** (via SHA-256) en deux exemplaires :
    - dans le module de gestion des usagers du système, sur les serveurs du CUSM ;
    - dans l'application de l'appareil mobile du patient.
  - ultérieurement, la connexion se fait après comparaison du *hash* du mot de passe entre l'application et le module de gestion des utilisateurs.

2.4.2 Authentification sécurisée

Pour l'heure, il n'est pas prévu d'option permettant de remplir automatiquement le champ du mot de passe dans la boîte de connexion de l'application. Le patient doit donc toujours entrer ce mot de passe pour s'authentifier.

Le projet *OPAL* ne prévoit pas de système de double authentification. Il est vrai que cela serait difficile à mettre en place :

- Un système de code de vérification envoyé par SMS ou généré via une solution de type *Google Authenticator* serait en effet sans intérêt, étant donné que l'application fonctionnerait sur le même appareil…
- Un système plus sécuritaire compliquerait l'utilisation de l'application, lui faisant perdre son but initial de communication simplifiée entre patient et médecin.

2.4.3 Gestion des mots de passe

La création du mot de passe se fait à l'origine dans les locaux de l'hôpital. Il doit s'agir d'un mot de passe relativement fort, comprenant lettres majuscules et minuscules, chiffres et caractères spéciaux.

Si le patient oublie son mot de passe, la procédure de remplacement est la suivante :

1. Depuis la page d'accueil de l'application, le patient demande un nouveau mot de passe.
2. *Firebase* génère un mot de passe temporaire et l'envoie par courriel au patient.
3. Le patient se connecte à l'application avec ce mot de passe temporaire. Ce dernier ne lui permet pas de s'authentifier : il ne peut donc pas encore accéder aux informations-patient.

4. L'application lui demande son numéro d'assurance-maladie, lequel est alors utilisé pour chiffrer les informations entre, d'une part, l'application et, d'autre part, le système au CUSM (qui connaît ce numéro). De son côté, *Firebase* ne peut pas déchiffrer les informations puisqu'elle ne connaît pas cette information.
5. Le système hébergé au CUSM s'assure que ce numéro d'assurance-maladie est correct.
6. Dans l'affirmative, une question de sécurité est choisie au hasard, en fonction des informations fournies par le patient lors de son enregistrement initial.
7. Si la réponse à cette question est correcte, le système demande au patient son nouveau mot de passe.

Ce système nous semble **raisonnablement sécuritaire si et seulement si le patient a adéquatement sécurisé son appareil mobile, comme doit lui enjoindre de le faire le formulaire de consentement qu'il signe lors de son enregistrement dans l'application**.

Dans le cas contraire, ce système de vérification nous paraît problématique. En effet, si une personne non autorisée détient l'appareil mobile et accède à une session utilisateur, en parcourant les courriels, applications et/ou les comptes de réseaux sociaux du patient, elle sera vraisemblablement capable de récupérer :

- son numéro d'assurance-maladie,
- la réponse à la question de sécurité (la majorité des questions de sécurité du projet sont de celles dont les réponses peuvent être trouvées via le téléphone du patient).

Si l'option des questions de sécurité devait être conservée pour le projet OPAL, il conviendrait alors de trouver d'autres questions.[3]

2.4.4 Maintien de la connexion

La connexion via *Firebase* est maintenue :

- jusqu'à ce que l'utilisateur de l'application mobile déconnecte explicitement en pressant le bouton *Déconnexion*.
- Jusqu'à l'expiration d'un laps de temps déterminé. Présentement, cette durée est fixée à 24 heures. Il nous apparaît impératif de **ramener cette durée à quelques minutes**, après cessation de toute activité de l'utilisateur sur l'application.

[3] *Cf.* annexe 1.

2.5 Consentement du patient

Comme nous l'avons mentionné plus haut, le système d'obtention d'un nouveau mot de passe peut constituer une vulnérabilité.

Dès lors, **il est essentiel que le patient sécurise l'accès à son appareil mobile. Cet enjeu pourrait être réglé dans le cadre du consentement exprimé par le patient lors de son enregistrement dans le projet et à l'installation de l'application sur son appareil.**

Le formulaire de consentement devrait en effet clairement signaler au patient :

- qu'il existe un risque qui ne peut pas être réduit à zéro dans le fonctionnement de l'application en elle-même,
- qu'il existe un risque plus notable d'accès à ses informations via l'appareil mobile et qu'il doit donc s'assurer de protéger adéquatement son appareil contre l'accès d'une tierce personne, en activant une solution de verrouillage de l'appareil. Dans le cas contraire, le CUSM ne saurait être tenu responsable d'un éventuel accès aux informations du patient par un tiers via l'application.

Il est également **fortement souhaité** de prévoir, au lancement de l'application, l'apparition d'une fenêtre surgissante rappelant à l'usager qu'il doit verrouiller l'accès à son appareil.

2.6 Application pour médecin

2.6.1 Visionneuse AppDB via Citrix

Le projet *OPAL* ne prévoit pas le recours à *l'Active Directory* du CUSM pour gérer les accès des médecins. Pour l'heure, ceux-ci se connectent au système via un portail web de l'application, accessible sur un poste informatique du CUSM.

À l'avenir, il est prévu que les médecins puissent utiliser ce portail sur un appareil mobile via *Citrix*, en passant par la plateforme *IRIAS3*, ce qui nécessite qu'ils entrent leur identifiant et leur mot de passe tels qu'enregistrés dans l'*Active Directory* du CUSM. Les informations consultées le sont directement dans *AppDB*, sans sortir du CUSM (donc sans passer par *Firebase*).

Il faut noter que les médecins ne peuvent alors accéder qu'aux informations d'**un seul patient à la fois**, en entrant l'identifiant du patient dans l'application.

Il est prévu que cette session *Citrix* soit automatiquement fermée après cinq minutes d'inactivité.

2.6.2 Application OPAL pour médecin

En revanche, il est **prévu ultérieurement d'implanter une version de l'application à destination des médecins**. Celle-ci leur permettrait de visualiser l'ensemble des informations de tous leurs patients. Se pose alors clairement le problème de la sécurisation de l'appareil par le praticien, sans commune mesure avec l'application-patient. En effet :

- le patient n'accède – via l'application – qu'à ses seules informations, tandis que le médecin accèderait aux informations de tous ses patients ;
- le patient a expressément déclaré accepter le risque d'une consultation illégitime de ses informations, ce qui protège le CUSM contre d'éventuelles poursuites. Mais une telle mesure de protection n'est pas envisageable pour les cas où une tierce personne non autorisée accèderait aux informations des patients via l'application mobile du médecin.

La sécurisation de l'application-médecin devra faire l'objet d'une nouvelle évaluation, préalablement à sa mise en production.

3 Intégrité

Bien qu'il existe une journalisation collectant toutes les actions des patients connectés à l'application, le *log* en lui-même devra être également protégé. Il s'agit d'éviter tout accès (ou modification) non autorisé des activités journalisées par des personnes de confiance disposant d'un niveau élevé de privilèges ou d'un compte *administrateur*.

4 Disponibilité

OPAL est une solution qui a été développée en interne au CUSM. Si un soutien adéquat n'est pas mis en place pour résoudre les éventuelles pannes de service (internes ou externes), il pourrait y avoir un impact sur la qualité du service fourni aux usagers.

En cas de panne de *Firebase*, l'équipe sera-t-elle prête à assumer les risques ? Sachant qu'elle fonctionnera en mode de service *non payant*, un processus ou une alternative devrait être mis en place afin d'éviter une indisponibilité de service aux usagers. Dans l'ensemble, un processus de notification aux usagers lors des incidents ou problèmes devrait être élaboré. N'oublions pas que le département prévoit plus de 3 000 nouveaux usagers par année.

Par ailleurs, la solution met en relation plusieurs systèmes applicatifs via des équipements ou engins d'interfaces. Une mauvaise configuration ou paramétrage de ces composants pourrait compromettre la disponibilité des données et avoir un impact sur la qualité et le service fourni aux patients.

Autre enjeu à signaler, celui du transfert de connaissance. Étant donné que le développement de la solution est fait en interne, sans une gestion adéquate du transfert de connaissance, on pourrait s'exposer à des risques d'indisponibilité de la solution (bogues, pannes liées aux mises à jour, défaut de processus ou de documentation, etc.).

5 Recommandations

5.1 Version initiale de l'application[4]

A. Lors de l'enregistrement du patient pour l'utilisation de l'application, s'assurer que le formulaire de consentement que signe ledit patient mentionne expressément le risque d'accès non autorisé à ses informations sur son appareil mobile, de même que la nécessité pour lui de sécuriser l'accès audit appareil.

B. Instaurer une fenêtre surgissante à chaque lancement de l'application, rappelant au patient qu'il doit sécuriser adéquatement son appareil mobile.

C. Prévoir une déconnexion automatique de l'application mobile après l'écoulement de cinq minutes sans activité de l'utilisateur sur ladite application.

D. Chiffrer le volume "*sandbox*" qui recueille et conserve les documents en mémoire persistante sur l'appareil mobile.

E. Pour la réinitialisation du mot de passe, prévoir des questions de sécurité dont la réponse n'est pas susceptible d'être trouvée sur l'appareil mobile du patient (via ses courriels, ses documents, ses applications ou ses comptes de réseaux sociaux en ligne).

F. Obtenir l'autorisation de la DSP et des Archives médicales pour l'utilisation des informations de nature médicale sur des équipements mobiles.

G. Contacter les Archives médicales pour établir les lignes directrices que le médecin devra suivre avant de déterminer s'il peut envoyer une information au patient.

H. Prévoir un plan d'action où les rôles et responsabilités seront déterminés afin de pouvoir intervenir en cas d'interruption de service, qu'elle soit de l'interne ou de l'externe (*AppDB*, connexion à l'application, gestion des accès, etc.).

I. Établir et clarifier les fonctions de soutien et de maintenance à travers les points suivants :
   - la gestion des changements
   - la gestion des incidents et des problèmes
   - le niveau de service (SLA)
     - heures régulières d'assistance ou de support et aussi en dehors des heures ouvrables.
     - contact du centre de support (Téléphone, Email, etc.)
     - disponibilité du système en % de temps
     - type de support (24/7 ou autre)
     - établissement du niveau de priorité en cas d'incident ou de problème.
     - description du service d'urgence hors des heures de travail.

[4] *Cf.* tableau récapitulatif à l'annexe 2.

  - processus d'émission d'un billet (incident /problème)
  - notification des maintenances planifiées
- le service non fourni (service qui n'est pas pris en compte par le support)
- surveillance et alertes
- évaluations ou audits annuels.

J. Disposer d'une documentation complète de la solution dans sa globalité :
- code source et interfaces de programmation,
- manuels pour les utilisateurs, l'administrateur système et le personnel de soutien,
- mise à jour de l'architecture technologique et logicielle.

K. L'équipe de développement devra s'assurer de prévoir parallèlement :
- un environnement de test et
- la réalisation de tests (performance, intersystème, de stress, de confirmation, d'endurance, de charge),
- un environnement de production,
- une procédure de retour en arrière (*rollback* or *backout*) en cas de problème des mises à jour.

afin de garantir la disponibilité de service lors des mises à jour ou correction des erreurs logicielles (bogues).

L. Avant sa mise à production, la solution OPAL devra faire l'objet d'un test de vulnérabilité supervisé par les *Services informatiques (sécurité opérationnelle)*.

M. S'assurer de mettre en place une surveillance pour prévenir les éventuels dysfonctionnements des serveurs redondants (*fail over*).
- Effectuer des tests de *fail over* une fois par année.

N. La solution OPAL doit permettre l'envoi des fichiers de journalisation au système de gestion centralisé des logs (SIEM) du CUSM.

O. Dans le cadre d'une mise en production de la solution OPAL, nous recommandons fortement la souscription à un mode de service payant afin de répondre aux exigences de disponibilité de la solution.

5.2 Versions ultérieures de l'application

P. Faire procéder à une réévaluation par notre service en cas de modification significative de l'application (mise à jour, ajout/activation de nouvelles fonctionnalités,…) et ce, préalablement à sa mise en production.

Q. Pour éviter une disparité trop grande entre les différentes façons de conserver les notes au dossier, s'assurer que ce qui est reçu via l'application puisse être intégré au dossier OACIS. Il conviendra donc de contacter (après les Archives médicales) le groupe OACIS pour assurer le transfert de ces informations de la façon la plus appropriée.

R. Concernant **l'application-médecin**, prévoir un système de sécurisation spécifique afin d'éviter l'accès non-autorisé aux informations des patients du praticien depuis son appareil mobile et le faire évaluer par notre service **avant** sa mise en production.

S. Prévoir une déconnexion automatique de la visionneuse sous *Citrix* après l'écoulement de quelques minutes sans activité de l'utilisateur sur ladite application.

Annexe 1. Propositions de questions secrètes sécuritaires

L'application OPAL permet une réinitialisation du mot de passe en recourant à des questions secrètes.

Toutefois, cette procédure peut être réalisée depuis un appareil mobile tel qu'un téléphone intelligent. Or, ce type d'appareil est susceptible de contenir ou de donner directement accès à un nombre **considérable** d'informations personnelles à son détenteur.

Par conséquent, les questions secrètes doivent être particulièrement bien choisies. En effet, toute personne malintentionnée qui se retrouverait en possession de l'appareil mobile du patient ne doit pas être en mesure d'obtenir la réponse à la question secrète, grâce aux informations glanées sur ledit appareil.

Voici quelques exemples de question secrète qui nous paraissent plus sécuritaires, compte tenu de ce contexte très particulier :

- Quel est le prénom de l'aînÉE de vos neveux et nièces ?
- Quel est le prénom de l'aînÉ de vos neveux et nièces ?
- Quel est le nom de jeune fille de votre grand-mère maternelle ?
- Quelle était la destination lors de votre premier voyage en avion ?
- Quel est le prénom de votre meilleur ami d'enfance ?
- Quel était votre sportif préféré durant votre enfance ?

Annexe 2. Suivi des recommandations pour la version initiale de la solution OPAL

N°	Recommandations	Enjeux	Services à impliquer
A	Le formulaire de consentement doit mentionner expressément le risque d'accès non autorisé à ses informations sur son appareil mobile, de même que la nécessité pour lui de sécuriser l'accès audit appareil.	Confidentialité des renseignements personnels et de santé du patient	Gouvernance en sécurité de l'information (GSI)
B	Instaurer une fenêtre surgissante à chaque lancement de l'application, rappelant au patient qu'il doit sécuriser adéquatement son appareil mobile.		Développement OPAL
C	Prévoir une déconnexion automatique de l'application mobile après l'écoulement de cinq minutes sans activité de l'utilisateur sur ladite application.		Développement OPAL
D	Chiffrer le volume "*sandbox*" qui recueille et conserve les documents en mémoire persistante sur l'appareil mobile.		Développement OPAL
E	Pour la réinitialisation du mot de passe, prévoir des questions de sécurité dont la réponse n'est pas susceptible d'être trouvée sur l'appareil mobile du patient (via ses courriels, ses documents, ses applications ou ses comptes de réseaux sociaux en ligne).		GSI Développement OPAL
F	Obtenir l'autorisation de la DSP et des Archives médicales pour l'utilisation des informations de nature médicale sur des équipements mobiles.		DSP Archives médicales
G	Contacter les Archives médicales pour établir les lignes directrices que le médecin devra suivre avant de déterminer s'il peut envoyer une information au patient.		Archives médicales Développement OPAL
H	Prévoir un plan d'action où les rôles et responsabilités seront déterminés afin de pouvoir intervenir en cas d'interruption de service, qu'elle soit de l'interne ou de l'externe (*AppDB*, connexion à l'application, gestion des accès, etc.).	Disponibilité de la solution	Développement OPAL

I	Établir et clarifier les fonctions de soutien et de maintenance à travers les points suivants :
	• la gestion des changements
	• la gestion des incidents et des problèmes
	• le niveau de service (SLA) :
	  ○ heures régulières d'assistance ou de support et aussi en dehors des heures ouvrables.
	  ○ contact du centre de support (Téléphone, Email, etc.)
	  ○ disponibilité du système en % de temps
	  ○ type de support (24/7 ou autre)
	  ○ établissement du niveau de priorité en cas d'incident ou de problème.
	  ○ description du service d'urgence hors des heures de travail.
	  ○ processus d'émission d'un billet (incident /problème)
	  ○ notification des maintenances planifiées
	• le service non fourni
	• la surveillance et les alertes
	• procéder à des évaluations ou à des audits une fois par année.
		Disponibilité de la solution	Développement OPAL

J	Disposer d'une documentation complète de la solution dans sa globalité : • code source et interfaces de programmation, • manuels pour les utilisateurs, l'administrateur système et le personnel de soutien, • mise à jour de l'architecture technologique et logicielle.	Disponibilité de la solution	Développement OPAL
K	L'équipe de développement devra prévoir parallèlement : • un environnement de test et • la réalisation de tests (de performance, intersystèmes, de stress, de confirmation, d'endurance, de charge), • un environnement de production,	Disponibilité de la solution	Développement OPAL

	• une procédure de retour en arrière (*rollback* or *backout*) en cas de problème des mises à jour. afin de garantir la disponibilité du service lors des mises à jour ou correction des erreurs logicielles (bogues).		
L	Avant sa mise à production, la solution OPAL devra faire l'objet d'un test de vulnérabilité supervisé par les *Services informatiques (sécurité opérationnelle)*.	Confidentialité des renseignements personnels et de santé du patient – Intégrité des informations – Disponibilité de la solution	Services informatiques (sécurité opérationnelle)
M	S'assurer de mettre en place une surveillance pour prévenir les éventuels dysfonctionnements des serveurs redondants. Effectuer des tests de *fail over* une fois par année.	Disponibilité de la solution	Services informatiques
N	La solution OPAL doit permettre l'envoi des fichiers de journalisation au système de gestion centralisé des logs (SIEM) du CUSM.	Intégrité et non-répudiation	Services informatiques
O	Dans le cadre d'une mise en production de la solution OPAL, souscrire à un mode de service payant afin de répondre aux exigences de disponibilité de la solution		Développement OPAL
P	Faire procéder à une réévaluation par GSI en cas de modification significative de l'application (mise à jour, ajout/activation de nouvelles fonctionnalités,…) et ce, préalablement à sa mise en production.		Développement OPAL GSI Services informatiques