Site Hôpital Sécurité

## Types d’utilisateurs

### Les patients:

* Prendre rendez-vous (et tous ce qui s’en suit)
* Consulter ces rendez-vous
* Consulter son suivis
* Converser avec son médecin.

### Les médecins:

* Voir ces rendez-vous
* Voir la liste de ces patients et consulter leur suivi.
* Converser avec les autres médecins.
* Prescrire des ordonnances.

### L’administrateur:

* Gérer compte patients et médecins (ajouts et suppression).

## Les patients :

Une interface d’accueil. avec la liste des dernier rendez-vous.

Une page où il y a la liste de tous les rendez-vous pris, qui amène à un autre page d’ajout ou de modification de rendez-vous.

Une page pour consulter leur suivis. Les information seront trié par catégories, radiologie, ophtalmologie…

Une interface avec la liste des médecin avec qui il a déjà eu rendez-vous, qui amène à une fenêtre permettant de converser avec eu.

## Les médecins :

Une page d’accueil ayant la liste des rendez-vous non fait des trois prochain jour.

Une page ou il peut avoir la liste des patients avec qui il a déjà eu rendez-vous, et qu’il suit encore. Cette page amène à une autre qui permet de converser avec le patient sélectionné.

Mais elle peut aussi sur une page avec un formulaire d’ordonnance pour le patient sélectionné. Cette page est accessible depuis la page du rendez-vous du patient.

## L’administrateur :

Une page avec la liste des compte.cette page ramène à celle permettant de supprimer le compte de la personne sélectionnée.

Un onglet permet d’amener à une autre page permettant de créer un compte.

Une page pour la liste des service ainsi que celle de modification de celui sélectionné.

Une Page pour la maintenance des services.

# Sécurité

## Serveur

* Crypter le fichier /etc/phpmyadmin/config-db.php {mot de passe db}
* Protection par mot de passe Apache en utilisant un fichier .htacces et un fichier .htpasswd est très efficace. {NE PAS NOMMER LE FICHIER .htpasswd COMME CELA LUI METTRE UN NOM NON INTUITIF COMMENÇANT PAR .ht…}
* Protégez par FTP vos fichiers “style.css” et “index.php” avec les droits 404 ou 444. J’ai vu un cas de piratage du fichier style.css où le pirate avait modifié ce fichier pour afficher un pop-up.
* Dans apache : /etc/apache2/conf-available/security.conf
  + ServerSignature off
  + ServerTokens Prod