Analyse des Risques liés à la sécurité de l’information selon la norme ISO 27005 d’un cabinet d’ophtalmologie

1. Présentation de l’entreprise

Nous allons réaliser une analyse des risques liée à la sécurité de l'information de l'entreprise OphtaVision. Il s'agit d'un cabinet d'ophtalmologie situé dans le centre-ville d'une ville moyenne (environ 30 000 habitants).

Deux amis ophtalmologues ont cofondé cette entreprise. Ils ont recruté une assistante médicale qui les aide dans la réalisation des examens classiques de vue et deux secrétaires qui s'occupent de prendre les rendez-vous, d'accueillir les patients, de gérer les dossiers et d’encaisser les paiements.

Quels services offrent-ils ?

- Des consultations ophtalmologiques
- Des examens de la vue (fond d’œil, OCT, etc.)
- Une prise de rendez-vous en ligne ou par téléphone
- Le stockage des dossiers médicaux de leurs patients au format électronique

Quel est leur environnement informatique ?

Pour réaliser leur activité ,ils disposent d’une petite infrastructure informatique :

- Un ordinateur portable pour chaque employé.
- Des équipements médicaux connectés (OCT, rétinographe, tonomètre)
- Une imprimante
- Un scanner
- Une box
- Un terminal de paiement

A cela s’ajoute :

- Un abonnement Office 365 pour chaque ordinateur
- Un logiciel de gestion pour les dossiers des patients qui inclut un site web et un outil de prise de rendez-vous en ligne
- Un abonnement Internet

Quelles sont les exigences légales et réglementaires du cabinet en ce qui concerne la sécurité de l’information ?

1. Le Règlement Général sur la Protection des Données (RGPD)

Le RGPD, qui est la réglementation européenne en matière de protection des données personnelles, impose des exigences strictes en matière de collecte, de traitement, de stockage et de sécurité des données personnelles des patients. Le cabinet d'ophtalmologie, en tant que responsable du traitement des données, doit respecter plusieurs principes :

- Principe de minimisation des données : Le cabinet ne doit collecter que les données nécessaires à l'exercice de son métier.
- Principe de confidentialité : Les données personnelles doivent être traitées de manière confidentielle. Seules les personnes autorisées (personnel médical et administratif) peuvent y avoir accès.
- Sécurisation des données : Le cabinet doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données contre les accès non autorisés, les pertes, les destructions ou les fuites.
- Consentement éclairé des patients : Avant de collecter et de traiter des données, les patients doivent être informés de leurs droits et donner leur consentement éclairé pour le traitement de leurs données personnelles, y compris pour le partage éventuel avec d'autres professionnels de santé.
- Droits des patients : Les patients ont des droits concernant leurs données, tels que le droit d'accès, de rectification, de suppression, de portabilité et d'opposition au traitement de leurs données. Le cabinet doit être en mesure de répondre à ces demandes dans les délais imposés par la réglementation.

2. Le code de la Santé Publique (CSP)

En plus du RGPD, la Loi Informatique et Libertés et le Code de la santé publique en France imposent des exigences spécifiques pour la protection des données de santé. Selon l'article L1110-4 du Code de la santé publique, les professionnels de santé sont tenus de respecter la confidentialité des informations concernant les patients et leur santé.

Le cabinet doit donc prendre toute les mesures nécessaires pour garantir la sécurité des informations médicales, telles que les dossiers médicaux électroniques (DME).

3. La Certification Hébergeur de Données de Santé (HDS)

Si le cabinet utilise un prestataire pour héberger ses données, ce qui est son cas avec le logiciel de gestion des données patients qu’il a, il doit s’assurer que son hébergeur dispose de la certification HDS.

Quelles sont les attentes des co-fondateurs quant à leur demande d'analyse des risques liés à la sécurité de l'information ?

Les co-fondateurs ont demandé cette analyse, tout d'abord pour s'assurer que leur traitement des données est conforme aux exigences réglementaires.

C'est aussi un moyen pour eux de garantir à leurs patients que leurs informations personnelles et médicales sont correctement protégées, et de le mettre en avant sur leur site web pour se démarquer de la concurrence.

Enfin ils veulent protéger leur système contre les cyberattaques (comme les ransomwares) qui pourraient compromettre leurs données et perturber leur activité.

Cette analyse portera donc sur l'ensemble du système d'information en lien avec la clientèle du cabinet.

Quels sont leurs critères pour mener cette analyse de risque ?

L'appétence au risque du cabinet est moyenne. Les cofondateurs veulent adopter une approche équilibrée, où la sécurité ne doit pas entraver l'efficacité de leur travail au quotidien.

Les critères pour déterminer la vraisemblance et les conséquences des risques identifiés seront des critères qualitatifs (faible, moyen, élevé).

Le niveau de risque sera également défini avec les critères qualitatifs suivants :

Vraisemblance / Conséquence	**Faible**	**Modérée**	**Élevée**
Faible	Faible	Faible	Modéré
Modérée	Faible	Modéré	Élevé
Élevée	Modéré	Élevé	Critique

En fonction de ces niveaux de risque, il sera défini un ordre de traitement des risques en se basant sur les critères suivants :

- **Faible** → Peu préoccupant
- **Modéré** → À surveiller
- **Élevé** → Prioritaire
- **Critique** → À traiter immédiatement

2. Appréciation des risques liés à la sécurité de l'information de l'entreprise OphtaVision

Identification des risques

Quelles sont les données sensibles ?

- Les données personnelles des patients (Nom, prénom, adresse, téléphone)
- Les données médicales (Consultations, prescriptions, imageries)
- Les données financières (Facturation, numéro de sécurité sociale, mutuelle)

Quelles sont les menaces possibles ?

TYPE	MENACES	ORIGINE
Dommage physique	Incendie	E
	Dégât des eaux	A
	Destruction de matériel	A, D ,E
Perte de services essentiels	Perte de la source d'alimentation en électricité	A
	Panne du matériel de télécommunications	A
Défaillances techniques	Panne de matériel	A
	Dysfonctionnement d'un logiciel	A
Compromission d'informations	Divulgation non autorisées de données	A, D
	Corruption de données	D
	Vol de données	D
Compromission des fonctions	Erreur d'utilisation des systèmes informatiques	A
Cybermenaces	Attaque par ransomware	D
	Phishing	D
	Perte de données (absence de sauvegarde)	A
Sécurité physique	Accès non autorisé aux locaux ou équipements médicaux	D

A-→ accidentel ; D-→ Délibéré ; E → Environnemental

Quelles sont les mesures de sécurité existantes dans le cabinet ?

CATÉGORIE	MESURES EXISTANTES
Sécurité physique	- Locaux fermés à clé - Même clés pour tous - Système de vidéo surveillance + alarme
Gestion des accès	- Un compte Office 365 par utilisateur - Un seul compte pour le logiciel de gestion des dossiers
Protection des données	- Stockage des dossiers dans le cloud - Pas de sauvegarde locale - Logiciel de gestion des dossiers certifié HDS
Sécurité réseau	- Box Internet installée par l'opérateur - Mot de passe de la box personnalisée (pas le mot de passe par défaut)

	- Un accès Wifi uniquement pour les ophtalmologues et leurs employés
Protection contre les cyberattaques	- Antivirus par défaut (Windows Defender) - Mises à jour activées
Sécurisation des paiements	- Terminal de paiement relié à la box Internet
Surveillance et journalisation	- Suivi des accès aux données des patients non activé
Sensibilisation du personnel	- Formation à la confidentialité des données médicales

Quelles sont les vulnérabilités possibles ?

TYPE	**VULNERABILITES**
Matériel	- Pas de chiffrement des disques durs - Pas de verrouillage automatique des sessions
Logiciel	- Faille dans le logiciel de gestion des dossiers clients - Mauvaise gestion des mots de passe - Pas de double authentification - Pas de compte personnalisé avec des droits adaptés pour le logiciel de gestion des dossiers client
Personnel	- Absence de sensibilisation à la sécurité (ingénierie sociale, phishing…) - Pas de procédure de suppression de compte en cas de départ d'une personne - Risque d'erreur humaine
Site	- Accès non journalisé d'accès au site
Organisationnel	- Absence de consentement éclairé pour collecter, stocker ou traiter des données de santé - Pas de procédure pour gérer les demandes d'effacement, de rectification ou d'accès aux données.

Quels sont les scénarios de risque possibles ?

a) Risque technique / défaillance du système

Scénario 1 : panne matérielle d'un des ordinateurs portables → le salarié n'a plus d'accès aux données des patients, ni à l'agenda. Il ne peut plus travailler

Scénario 2 : panne d'accès à la connexion Internet → le cabinet ne peut plus fonctionner, perte de chiffre d'affaire

Scénario 3 : dysfonctionnement du logiciel de gestion des patients → les données des patients ne peuvent plus être consultées, ni modifiées

b) Risques liés à la cybersécurité

Scénario 4 *:* infection par un ransomware → les données se retrouvent chiffrées

Scénario 5 : un employé est victime de phishing, ses identifiants Office 365 et l'identifiant unique du logiciel des dossiers clients sont piratés donnant accès aux données confidentielles du cabinet et à la messagerie de la victime

Scénario 6 : attaque par force brute d'un des mots de passe, le compte est compromis.

Scénario 7 : attaque du site de prise de rendez-vous en ligne (attaque DDOS) saturant l'agenda des ophtalmologues avec de faux rendez-vous

c) Risques humains

Scénario 8 : envoi d'un email à une mauvaise adresse divulguant des données personnelles

Scénario 9 : départ d'un employé sans désactivation de son compte, ni changement du mot de passe du compte d'accès au logiciel de gestion des données des patients ; il peut alors continuer à accéder aux données

d) Risques physiques

Scénario 10 : incendie ou dégâts des eaux, destruction partielle ou totale du matériel et des locaux

Scénario 11 : vol ou perte d'un ordinateur portable, les données stockées n'étant pas chiffrées sur les ordinateurs, il peut y avoir une fuite de données

e) Risques liés à des tiers

Scénario 12 : le prestataire d'hébergement des données médicales (certifié HDS) subit une panne, rendant temporairement inaccessibles les données des patients.

Scénario 13 : Le prestataire d'hébergement de données médicales subit une **fuite de données** à cause d'une cyberattaque, compromettant la confidentialité des dossiers des patients

f) Risques Juridiques

Scénario 14 : Un patient demande l'effacement de ses données personnelles sensibles, mais la procédure interne de traitement des demandes est inexistante.

Scénario 15 : Un patient porte plainte à la CNIL après avoir découvert que ses données médicales ont été conservées sans information préalable, ce qui entraîne une sanction administrative et une atteinte à la réputation du cabinet.

Analyse des risques

SCENARIO	VRAISEMBLANCE	CONSÉQUENCES
1	MODÉRÉE Les ordinateurs ont 3 ans et bien qu'il y ait des mises à jour régulières avec Office 365, ils pourraient présenter des signes d'usure (système d'exploitation, disque dur, etc.). Mais la probabilité d'une panne matérielle est modérée car le matériel est encore relativement récent et entretenu.	ÉLEVÉES La panne entraînerait l'impossibilité d'accéder aux données patients et à l'agenda, ce qui stopperait une partie de l'activité du cabinet. Cela pourrait affecter le service et entraîner des pertes financières. Les données seraient inaccessibles, ce qui est un risque majeur.
2	FAIBLE Le cabinet utilise un opérateur fiable avec un contrat de maintenance.	ÉLEVÉES La perte de l'accès à Internet pourrait perturber l'activité du cabinet et entraîner une perte de revenus, en plus de nuire à la relation avec les patients.
3	FAIBLE Le logiciel a une bonne réputation, il y a des mises à jour régulières, les employés du cabinet ont été formés à son utilisation et ont accès à une hotline. Mais il n'y a aucune sauvegarde locale en cas de problème	ÉLEVÉES L'indisponibilité du logiciel bloque l'accès aux données essentielles pour l'activité du cabinet, ce qui peut entraîner une perte de chiffre d'affaires, une détérioration de la réputation et des problèmes juridiques si les données sont perdues.
4	ÉLEVÉE Le cabinet ne dispose que des solutions de sécurité de Windows Defender et d'Office 365 (le pack de base), les employés ne sont pas formés et il n'existe qu'une sauvegarde dans le cloud.	ÉLEVÉES L'infection par ransomware entraînerait une perte d'accès aux données, une interruption de service, des pertes financières, une atteinte à la réputation et des risques juridiques.
5	ÉLEVÉE Les salariés ne sont pas formés aux problématiques de phishing et il n'y a pas d'authentification multifacteurs	ÉLEVÉES Cela donnerait un accès non autorisé qui violerait la RGPD et la confidentialité des données médicales. Il y aurait des pertes financières, une atteinte à la réputation et des risques juridiques.
6	MODÉRÉE Il y a une politique de mots de passe qui demande des mots de passe complexes mais avec un changement une fois par an, mais il n'y a pas d'authentification multifacteurs et un compte unique pour le logiciel.	ÉLEVÉES En cas de récupération du mot de passe, le hacker peut accéder à toutes les données, ce qui violerait la RGPD et la confidentialité des données médicales. Il y aurait des pertes financières, une atteinte à la réputation et des risques juridiques.
7	FAIBLE Le cabinet s'appuie sur l'offre de son HDS qui a des solutions de sécurité pour les attaques DDoS	MODÉRÉES La prise de rendez-vous pourra continuer à se faire par téléphone mais nécessitera des mises à jour lorsque le HDS aura rétabli le bon agenda.
8	MODÉRÉE L'erreur est humaine mais les salariés sont formées à la confidentialité des données médicales	ÉLEVÉES La divulgation de données personnelles (en particulier des données médicales) peut entraîner des conséquences juridiques, réputationnelles et financières importantes.
9	ÉLEVÉE Il n'y a pas de responsable informatique. C'est l'un des deux ophtalmologues qui doit s'en charger et il n'existe aucune procédure écrite.	ÉLEVÉES Cela donne un accès non autorisé à des données sensibles, ce qui peut entraîner des conséquences juridiques, réputationnelles et financières importantes.

10	FAIBLE Le cabinet est dans un immeuble récent aux normes et il a une assurance	ÉLEVÉES Aucune activité n'est possible si les équipements médicaux sont endommagés
11	FAIBLE Les portables restent toujours sur place, dans des locaux fermés à clé, et le cabinet est équipé d'une alarme	ÉLEVÉES Si un portable était volé, les disques durs n'étant pas chiffrés, il y aurait une fuite de données sensibles, ce qui peut entraîner des conséquences juridiques, réputationnelles et financières importantes.
12	FAIBLE Le prestataire est fiable et a un contrat de SLA avec le cabinet	MODÉRÉES Cela entraîne une désorganisation du cabinet et une perte d'efficacité mais pas un blocage de l'activité
13	FAIBLE Les acteurs certifiés HDS sont bien protégés, mais les fuites de données existent malgré tout.	ÉLEVÉES Le cabinet reste juridiquement impliqué, cela peut donc avoir des conséquences juridiques graves et entacher l'image du cabinet.
14	MODÉRÉE Même si les demandes ne sont pas fréquentes, l'absence totale de procédure rend le risque réel dès la première demande.	ÉLEVÉES Le cabinet encourt des risques juridiques car non respect du RGPD, et des pénalités ainsi qu'une atteinte à sa réputation.
15	MODÉRÉE Étant donné qu'aucune information n'est fournie et que le public est de plus en plus vigilant, cela peut arriver	ÉLEVÉES Le cabinet encourt des risques juridiques et des pénalités ainsi qu'une atteinte à sa réputation.

Évaluation des risques

SCENARIO	VRAISEMBLANCE	CONSÉQUENCES	NIVEAU DE RISQUE
1	MODÉRÉE	ÉLEVÉES	ÉLEVÉ
2	FAIBLE	ÉLEVÉES	MODÉRÉ
3	FAIBLE	ÉLEVÉES	MODÉRÉ
4	ÉLEVÉE	ÉLEVÉES	CRITIQUE
5	ÉLEVÉE	ÉLEVÉES	CRITIQUE
6	MODÉRÉE	ÉLEVÉES	ÉLEVÉ
7	FAIBLE	MODÉRÉES	FAIBLE
8	MODÉRÉE	ÉLEVÉES	ÉLEVÉ
9	ÉLEVÉE	ÉLEVÉES	CRITIQUE
10	FAIBLE	ÉLEVÉES	MODÉRÉ
11	FAIBLE	ÉLEVÉES	MODÉRÉ
12	FAIBLE	MODÉRÉES	FAIBLE
13	FAIBLE	ÉLEVÉES	MODÉRÉ
14	MODÉRÉE	ÉLEVÉES	ÉLEVÉ

15	MODÉRÉE	ÉLEVÉES	ÉLEVÉ

Quel va être l'ordre de traitement des risques ?

Priorité 1 – à traiter immédiatement :

- **Scénario 4** *:* infection par un ransomware → les données se retrouvent chiffrées
- **Scénario 5** : un employé est victime de phishing, ses identifiants Office 365 et l'identifiant unique du logiciel des dossiers clients sont piratés donnant accès aux données confidentielles du cabinet et à la messagerie de la victime
- **Scénario 9** : départ d'un employé sans désactivation de son compte, ni changement du mot de passe du compte d'accès au logiciel de gestion des données des patients ; il peut alors continuer à accéder aux données

Priorité 2 - Prioritaire :

- **Scénario 1** : panne matérielle d'un des ordinateurs portables → le salarié n'a plus d'accès aux données des patients, ni à l'agenda. Il ne peut plus travailler
- **Scénario 6** : attaque par force brute d'un des mots de passe, le compte est compromis.
- **Scénario 8** : envoi d'un email à une mauvaise adresse divulguant des données personnelles
- **Scénario 14** : Un patient demande l'effacement de ses données personnelles sensibles, mais la procédure interne de traitement des demandes est inexistante.
- **Scénario 15** : Un patient porte plainte à la CNIL après avoir découvert que ses données médicales ont été conservées sans information préalable, ce qui entraîne une sanction administrative et une atteinte à la réputation du cabinet.

Priorité 3 – à surveiller :

- **Scénario 2** : panne d'accès à la connexion Internet → le cabinet ne peut plus fonctionner, perte de chiffre d'affaire
- **Scénario 3** : dysfonctionnement du logiciel de gestion des patients → les données des patients ne peuvent plus être consultées, ni modifiées
- **Scénario 10** : incendie ou dégâts des eaux, destruction partielle ou totale du matériel et des locaux
- **Scénario 11** : vol ou perte d'un ordinateur portable, les données stockées n'étant pas chiffrées sur les ordinateurs, il peut y avoir une fuite de données
- **Scénario 13** : Le prestataire d'hébergement de données médicales subit une **fuite de données** à cause d'une cyberattaque, compromettant la confidentialité des dossiers des patients

Priorité 4 – peu préoccupant :

- **Scénario 7** : attaque du site de prise de rendez-vous en ligne (attaque DDOS) saturant l'agenda des ophtalmologues avec de faux rendez-vous
- **Scénario 12** : le prestataire d'hébergement des données médicales (certifié HDS) subit une panne, rendant temporairement inaccessibles les données des patients.

3. Proposition de plan de traitement des risques identifiés

Plan de traitement des risques de priorité 1 : à mettre en œuvre immédiatement

Scénario 4 *:* infection par un ransomware

Stratégie : modifier le risque ; risque résiduel attendu : faible ; actions :

- Mettre en place un système de sauvegarde complémentaire à celui proposé par le fournisseur du logiciel

Options	Sauvegarde externalisée dans le cloud	Sauvegarde interne (NAS ou disque dur local dans les locaux)
Avantages	• Pas besoin de maintenance matérielle • Protection en cas d'incendie ou de vol • Pas besoin de compétences IT interne	• Contrôle total sur les données • Pas de coût autre que l'achat du matériel
Inconvénients	• Coût de l'abonnement • Besoin d'un fournisseur de confiance et conforme RGPD	• Risque de pertes de données en cas de vol ou d'incendie • Besoin de compétence IT pour le gérer
Responsable	Co-fondateur	Co-fondateur / prestataire IT (mise en œuvre et maintenance)
Temps de mise en œuvre estimé	1 à 2 jours (choix, souscription, configuration initiale)	3 à 5 jours (achat, configuration, tests, documentation)
Coût Estimé	Environ 10 à 20 €/mois selon l'offre	300 à 600 € en matériel (NAS + disques) + frais de prestataire IT

- Mettre en place un antivirus plus puissant que les solutions existantes dans le cabinet

Options	Installer une solution antivirus professionnelle	Migrer vers un abonnement Microsoft 365 Business Premium

Avantages	• Meilleure détection que l'antivirus Windows Defender • Supervision possible	• Intégration de Microsoft Defender for Business • Protection étendue (menaces, phishing, ransomware) • Facile à déployer car il existe déjà un abonnement Microsoft
Inconvénients	• Abonnement à souscrire séparément • Suivi des mises à jour requis	• Coût plus élevé qu'un abonnement standard • Nécessite un petit temps de configuration initial
Responsable	Co-fondateur	Co-fondateur (avec aide de Microsoft ou d'un prestataire)
Temps de mise en œuvre estimé	1 jour	1 à 2 jours
Coût Estimé	Environ 25–40 € / an / poste	Environ 18 € / mois / utilisateur (au lieu de 7 € pour un abonnement basique)

- Sensibiliser le personnel aux risques de ransomware

Options	Formation en ligne	Formation en présentiel avec un formateur
Avantages	• Souplesse d'organisation (chacun peut la suivre à son rythme) • Moins coûteuse • Accessible à tout moment pour réviser	• Plus engageante et interactive • Réponses aux questions en direct • Meilleure mémorisation pour certains profils
Inconvénients	• Moins d'interactivité • Nécessite de l'autodiscipline	• Plus coûteuse • Nécessite de bloquer un créneau commun • Moins de flexibilité
Responsable	Co-fondateur	Co-fondateur / Formateur externe
Temps de mise en œuvre estimé	1 jour (choix de la plateforme, envoi des accès)	1 à 2 jours (choix du formateur, organisation de la session)
Coût Estimé	Environ 20–50 € / utilisateur selon la plateforme	Environ 500–800 € pour une session groupe avec un prestataire

Scénario 5 : phishing,

Stratégie : modifier le risque ; risque résiduel attendu : faible ; actions :

- Mettre en place l'authentification multifacteur (MFA)

Options	Authentification MFA avec Office 365	Authentification MFA avec un service tiers
Avantages	• Intégré à Office 365 • Facile à mettre en place	• Plus flexible • Solution éprouvée
Inconvénients	• Dépendance à l'environnement Microsoft	• Nécessite une gestion supplémentaire • Moins de dépendance à Office 365
Responsable	Co-fondateur / Microsoft	Co-fondateur / prestataire IT
Temps de mise en œuvre estimé	1 jour (configuration)	1 jour (installation, configuration)
Coût Estimé	Inclus dans l'abonnement Office 365	Gratuit ou faible coût selon l'outil choisi

- Demander un compte par utilisateur au prestataire HDS

Options	Compte individuel par utilisateur (identifiants distincts)
Avantages	• Traçabilité des actions • Révocation rapide si départ d'un employé • Moins de risques en cas de compromission
Inconvénients	• Gestion plus lourde (droits, créations, suppressions)
Responsable	Co-fondateur / prestataire HDS
Temps de mise en œuvre estimé	1 à 2 jours
Coût Estimé	5 à 15 €/mois/utilisateur

- Sensibiliser le personnel aux risques de phishing – commun avec l'action de sensibilisation à mener pour le scénario précédent

Scénario 9 : départ d'un employé sans désactivation de son compte

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action :

- Rédiger une procédure de départ (checklist simple)
  Contenu minimal de la procédure :
  Désactivation immédiate des comptes numériques (Office 365, logiciel patient, boîte mail pro…)
  Révocation des accès (agenda partagé, dossiers sur OneDrive, etc.)
  Récupération du matériel (badge, PC, téléphone pro…)
  Inconvénient : Repose sur la rigueur du personnel à l'appliquer
  Responsable : Le co-fondateur
  Temps de mise en œuvre estimé : 2–3 heures pour rédiger la procédure
  Coût estimé : aucun

Plan de traitement des risques de priorité 2 : à mettre en œuvre dans un délai de 3 à 6 mois

Scénario 1 : panne matérielle d'un des ordinateurs portables

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action :

- Avoir un poste de secours

Options	Maintien d'un ordinateur de back up dans les locaux	Possibilité de travail depuis un autre poste avec un compte utilisateur
Avantages	• Immédiatement disponible • Aucun délai d'intervention	• Ne nécessite pas d'achat supplémentaire • Facile à mettre en œuvre avec une bonne gestion des accès
Inconvénients	• Coût pour l'achat d'un poste supplémentaire • Inutilisé la plupart du temps	• Risque de confidentialité si les sessions ne sont pas bien cloisonnées • Un des salariés doit être absent
Responsable	Co-fondateur	Co-fondateur
Temps de mise en œuvre estimé	1 jour (achat et configuration)	1 jour (paramétrage des accès partagés et test)
Coût Estimé	500–800 €	Aucun

Scénario 6 : attaque par force brute d'un des mots de passe, le compte est compromis.

Stratégie : modifier le risque ; risque résiduel attendu : faible ; actions :

- Mettre en place l'authentification multifacteur (MFA) – voir action du scénario 5
- Demander un compte par utilisateur au prestataire HDS - voir action du scénario 5
- Sensibiliser le personnel à l'importance des mots de passe complexes – commun avec l'action de sensibilisation à mener pour les scénarios 4 et 5
- Renforcer la politique des mots de passe (Changement plus fréquent, Impossibilité de réutiliser les anciens mots de passe)
  Responsable : Le co-fondateur
  Temps de mise en œuvre estimé : 1–2 heures
  Coût estimé : aucun

Scénario 8 : envoi d'un email à une mauvaise adresse divulguant des données personnelles

Stratégie : modifier le risque ; risque résiduel attendu : faible ; actions :

- Sensibiliser le personnel – commun avec l'action de sensibilisation à mener pour les scénarios 4 et 5
- Activer un avertissement à l'envoi vers l'extérieur (via Outlook/Microsoft 365)

Options	Activer le message d'avertissement à l'envoi hors domaine
Avantages	• Rappel automatique • facile à déployer • pas de coût
Inconvénients	• Nécessite accès à l'interface d'administration Microsoft 365
Responsable	Co-fondateur (avec assistance si besoin) ou prestataire IT
Temps de mise en œuvre estimé	1 à 2 heures
Coût Estimé	Gratuit (inclus dans Microsoft 365) si pas de recours à un prestataire IT

- Chiffrer automatiquement des emails contenant des données sensibles

Options	Configurer une règle automatique de chiffrement dans Outlook (via Microsoft 365)
Avantages	• Renforce la sécurité • limite l'impact d'une erreur d'envoi
Inconvénients	• Configuration technique
Responsable	Prestataire IT
Temps de mise en œuvre estimé	2 à 3 heures
Coût Estimé	150–200 € si confié à un prestataire

Scénario 14 : demande d'effacement de ses données personnelles sensibles

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action :

- Rédiger une procédure dede traitement des demandes d'exercice de droits (effacement, accès, rectification…)
  Se baser sur le modèle de la CNIL
  Inconvénient : Repose sur la rigueur du personnel à l'appliquer
  Responsable : Le co-fondateur
  Temps de mise en œuvre estimé : 1 jour pour rédiger la procédure
  Coût estimé : aucun

Scénario 15 : plainte à la CNIL

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action :

- Rédiger une politique de confidentialité (sur le traitement des données) et l'afficher dans la salle d'attente
  Inconvénient : Nécessite un peu de veille réglementaire pour la rédiger correctement

Responsable : Le co-fondateur avec si besoin l'aide d'un expert en RGPD
Temps de mise en œuvre estimé : 1 jour pour rédiger la procédure
Coût estimé : aucun ; 200–300 € si recours à un expert.

Plan de traitement des risques de priorité 3 : à mettre en œuvre à moyen terme, quand les ressources le permettent

Scénario 2 : panne d'accès à la connexion Internet

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action : prévoir un deuxième accès Internet (en souscrivant par exemple à une offre avec un backup 5G intégré ; 5 à 15 € / mois selon le fournisseur)

Scénario 3 : dysfonctionnement du logiciel de gestion des patients

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action : prévoir un stockage autre des données pour continuer à y accéder - c'est une des actions nécessaires pour le traiter le risque du scénario 4 ; il peut également être envisagé de revoir le contrat avec le prestataire pour améliorer les garanties de disponibilité et les compensations en cas de dysfonctionnement.

Scénario 10 : incendie ou dégâts des eaux

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action : prévoir un stockage autre pour sauvegarder les données des patients ; c'est une des actions nécessaires pour le traiter le risque du scénario 4.

Scénario 11 : vol ou perte d'un ordinateur portable

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action : prévoir un chiffrement des disques durs avec Bitlocker (inclus dans Windows 11 Pro).

Scénario 13 : Le prestataire d'hébergement de données médicales subit une fuite de données à cause d'une cyberattaque

Stratégie : modifier le risque ; risque résiduel attendu : faible ; action : prévoir un stockage autre pour sauvegarder les données des patients ; c'est une des actions nécessaires pour le traiter le risque du scénario 4. Il peut également être envisagé de revoir le contrat d'assurance pour couvrir ce point.

Plan de traitement des risques de priorité 4

Stratégie : accepter les risques et les revoir régulièrement.

4. Conclusion et recommandations

L’analyse des risques menée pour le cabinet OphtaVision met en évidence plusieurs vulnérabilités pouvant avoir un impact significatif sur la confidentialité, l’intégrité et la disponibilité des données patients, ainsi que sur la continuité de l’activité. Afin de réduire efficacement les risques identifiés comme prioritaires, les recommandations suivantes sont proposées :

Dans un délai d’un mois maximum, il est fortement recommandé de :

- Mettre en place une solution de sauvegarde complémentaire, sécurisée et externalisée dans le cloud, sous un format lisible indépendamment du logiciel métier.
- Installer une solution antivirus professionnelle sur les postes.
- Organiser une formation d’une journée à destination de l’ensemble des salariés sur les risques cyber (ransomware, phishing, ingénierie sociale), les bons réflexes en ligne, l’importance des mots de passe robustes et de la double authentification.
- Activer l’authentification multi-facteurs (MFA) pour les comptes Office 365 et tout autre service critique.
- Demander la création de comptes individualisés auprès du prestataire HDS pour une traçabilité renforcée des accès.

D’ici 6 mois, les mesures suivantes pourront venir compléter la démarche :

- Renforcer la politique de mot de passe (fréquence de changement, impossibilité de réutiliser les anciens mots de passe, complexité minimale).
- Activer un message d’avertissement automatique lors d’un envoi d’email à un destinataire externe.
- Configurer le chiffrement automatique des emails contenant des données sensibles.
- Rédiger une procédure de départ des employés (désactivation des accès, remise du matériel, etc.) et formaliser une politique de confidentialité claire.
- Étudier la possibilité de mettre en place une connexion 5G de secours, en cas de coupure Internet.
- Activer le chiffrement des disques durs pour protéger les données en cas de vol ou de perte de matériel.

Enfin, il est recommandé de planifier une nouvelle revue des risques dans un délai d’un an, ou plus tôt en cas de changement significatif dans l’organisation (nouveaux outils, évolution du personnel, incident de sécurité, etc.), afin d’adapter les mesures de protection aux évolutions du contexte.

Fait à Paris , le 16 avril 20025

Odile FRANCHET
Consultant en sécurité des systèmes d’information – ofranchet@gmail.com