

# QERSI-S

## Questionnaire d'Évaluation des Risques pour le Système d'Information de Santé

Dates	Versions	Descriptions
06/2013	V0.1	Adaptation de l'outil au contexte des établissements de santé.
09/2013	V1.0	Prise en compte des retours d'expérience des participants à la formation TéléSanté Centre.
06/2014	V1.5	Prise en compte des retours d'expérience des formations assurées par l'APSSIS.
09/2014	V2.0	Ajout de métriques pour affiner la partie appréciation des risques (convergence avec la norme ISO 27005 : Gestion des risques en sécurité de l'information).

## Abréviations utilisées dans le document

SI : Système d'Information de Santé  
MOA : Maîtrise d'Ouvrage désigne le promoteur métier  
MOE : Maîtrise d'œuvre désigne le chef de projet SI  
CIL : Correspondant Informatique et Libertés  
DICP : Disponibilité, Intégrité, Confidentialité, Preuve

## Objectifs du QERSI-S

Ce questionnaire, réalisé par le GCS TéléSanté Centre et l'APSSIS, et inspiré d'un travail initial de la CNAM-TS, permet d'analyser les risques qu'un système fait porter à un établissement de santé. Le système étudié peut être une application nouvelle, l'évolution d'une application ancienne, ou une organisation humaine.

Tout projet de système d'information doit bénéficier d'une analyse formalisée qui informe le référent sécurité de l'établissement et les moyens d'y répondre. Le QERSI-S est réputé connu du responsable de traitement, par sa maîtrise d'ouvrage.

La conduite de la démarche de sécurité est de la responsabilité de la maîtrise d'ouvrage. Le chef de projet de la maîtrise d'ouvrage remplit de manière exhaustive les sections 1 à 5, et joint tout document utile à la compréhension du système à analyser.

Le référent sécurité rend son évaluation dans la sixième section du QERSI-S. Il estime si l'analyse limitée du QERSI-S est suffisante pour éliminer des risques majeurs, et il répond en formulant des objectifs de sécurité à la maîtrise d'ouvrage, qu'elle transmettra à la maîtrise d'œuvre pour implémentation.

**Dans le cas où la sensibilité du projet engage des risques majeurs pour l'établissement, il est important de mener une analyse approfondie conforme à la méthodologie de l'ISO 27005.**

## Démarche de la prise en compte de la sécurité dans les projets

L'analyse de risques doit être réalisée en amont des spécifications du cahier des charges, à la phase d'expression des besoins, dès que les informations et les fonctions traitées par le futur système sont connues.

Elle permet notamment :

- 1 - d'estimer l'importance du risque pour le système d'information dans au moins quatre critères de sécurité : disponibilité, intégrité, confidentialité ainsi que preuve et contrôle (DICP).
- 2 - d'identifier les points faibles du système au regard des menaces mises en évidence
- 3 - d'élaborer les mesures de sécurité permettant d'amener le risque à un niveau acceptable
- 4 - d'informer le responsable du projet des risques résiduels

## Guide de remplissage

### Description du questionnaire

Le questionnaire contient huit sections. Les cinq premières sont à remplir par le chef du projet métier, la sixième est réservée au référent sécurité, la septième à la maîtrise d'œuvre et la dernière au CIL ou responsable du traitement.

**Section 1 - Profil du projet :** cette section permet de décrire le futur système et son contexte réglementaire, humain et stratégique. Cette description permet d'estimer les moyens organisationnels, techniques et juridiques à mettre en œuvre pour la sécurité. Il est souhaitable d'associer un schéma du processus.

**Section 2 - Disponibilité :** cette section estime les dommages consécutifs à l'interruption du fonctionnement de l'application ou du système. Chaque question propose un choix de cinq durées d'arrêt. Il s'agit d'estimer l'impact le plus important, puis de désigner la durée à partir de laquelle l'impact devient inéluctable. Les questions D9 à D11 concernent la continuité d'activité, au sens de la nécessité de reconstruire les informations qui n'auraient pas pu être traitées pendant l'arrêt du système.

**Section 3 - Intégrité :** cette section analyse les conséquences de la perte ou de la modification de l'information traitée ou produite par le système, c'est-à-dire : dans quelle mesure ces événements peuvent tromper l'utilisateur et nuire au processus métier.

**Section 4 - Confidentialité :** cette section couvre les dommages inhérents à une fuite d'information accidentelle ou volontaire (perte de confidentialité) aboutissant à une plainte ou une révélation publique.

**Section 5 - Preuve :** cette section permet de décrire un besoin particulier de preuve pour le projet. En l'absence de besoin spécifique décrit par le chef de projet, ce critère sera étudié par le référent sécurité en fonction des réponses apportées dans les autres sections.

**Section 6 - Réserve à l'estimation du risque par le référent sécurité :** cette section permet au référent sécurité de faire une première évaluation de la sensibilité du projet, à la lecture des réponses du chef de projet apportées dans les sections précédentes. Il s'agit d'une appréciation d'expert, qui peut donc diverger par rapport à l'expression de la maîtrise d'ouvrage.

**Section 7 – Observations de la maîtrise d'œuvre :** cette section recueille les préconisations techniques de la maîtrise d'œuvre, au regard des sections précédentes.

**Section 8 – Observations du Correspondant Informatique et Libertés :** dans la dernière section, le CIL (à défaut, le responsable du traitement) donne son avis sur la prise en compte des enjeux de la CNIL, et fait des préconisations sur les formalités adéquates pour le projet.

Pour toute question sur ce formulaire, vous pouvez contacter le référent sécurité de votre établissement.

### Glossaire

<i>Disponibilité</i> : propriété qu'une information ou un système soit accessible en temps voulu.	<i>Intégrité</i> : propriété d'assurer l'exactitude de l'information.
<i>Preuve</i> : propriété de pouvoir imputer sans équivoque les actions d'une personne ou entité. Nécessaire aux utilisateurs pour accorder leur confiance dans l'information fournie.	<i>Menace</i> : acte ou événement pouvant entraîner un impact négatif sur le système d'information ou à l'activité supportée par celui-ci.
<i>Confidentialité</i> : propriété que l'information ne soit pas accessible aux individus, entités ou processus non autorisés.	<i>Risque</i> : description d'un scénario de menace et des pertes auxquels il peut aboutir.
<i>Données à caractère personnel</i> : information permettant l'identification d'une personne physique de manière directe ou indirecte.	

## Échelles de risque utilisées dans le questionnaire

Les échelles proposées dans ce questionnaire sont données à titre d'exemple, vous pouvez les remplacer par d'autres qui seraient déjà utilisées dans votre établissement.

L'importance du risque pour l'établissement est exprimée dans une échelle allant de NC (pas d'impact) à 4 (impact intolérable). La réponse doit être fournie en envisageant le pire des scénarii.

Le tableau suivant permet d'estimer la hauteur des effets engendrés par un événement redouté, il présente les conséquences possibles.

Tableau 1 : Echelle d'impact

Valeur d'impact	Patient	Social & organisation	Financier	Responsabilité / juridique	Réputation / image
<b>1 – Mineur</b>	Gêne / inconfort pour un patient	- Gêne ponctuelle dans la prise en charge de patients, ou l'activité - Démotivation des acteurs / perte de temps	Perte financière sans impact significatif pour le responsable du traitement	Absence de plainte ou plaintes sans suite	Evènement peu ou pas médiatisé, sans effet ou effet négligeable sur l'image de l'organisme.
<b>2 – Significatif</b>	- Perte de chance pour un patient - Effet indésirable limité et réversible sur un patient	- Surcharge de travail et/ou désorganisation modérée mais temporaires dans la prise en charge des patients - Conflit social - Interruption ou ralentissement temporaire de certaines activités	Perte financière avec des impacts importants pour le responsable du traitement	Contentieux	Dégradation passagère d'image ou de confiance dans l'acteur de santé ou le service offert
<b>3 – Important</b>	- Perte de chance pour une population - Soins inadéquats et/ou report de soins pour un patient entraînant une mise en danger immédiate du patient (atteinte sévère) et/ou une prolongation de la durée d'hospitalisation et/ou une ré intervention avec ou sans perte de chances	- Désorganisation importante et durable de l'activité entraînant une perte significative d'activité et/ou une replanification des soins ou un recours à des organismes tiers. Conflit social paralysant l'établissement	Perte financière avec des impacts importants pour le responsable du traitement	Atteinte à la vie privée d'un patient Condamnation pénale et/ou financière.	- Perte d'image ou de confiance dans l'acteur de santé ou le service offert - Mise en cause de la stratégie de l'organisme détenteur du système ou d'un organisme tiers
<b>4 – Critique</b>	- Mise en danger d'une population / Menace du pronostic vital - Atteinte irréversible ou décès d'un ou plusieurs patient(s)	- Arrêt prolongé d'une part importante ou de toute l'activité. - Arrêt du projet - Fermeture de l'établissement	Perte financière mettant en cause la pérennité du responsable du traitement	- Condamnation pénale et/ou financière - Atteinte à la vie privée d'une population - Risques judiciaires	- Rejet définitif de l'acteur de santé ou du service offert - Mise en cause de l'existence de l'organisme détenteur du système ou d'un organisme tiers

La vraisemblance des scénarii d'incident pour l'établissement est exprimée dans une échelle allant de 1 (exceptionnel) à 4 (quasi certain). La réponse doit être fournie au regard des incidents déjà produits, de la complexité de mise en œuvre des événements redoutés et des mesures de sécurité effectives.

Le tableau suivant permet d'estimer la force d'occurrence d'un événement redouté, il présente les niveaux possibles.

Tableau 2 : Echelle de vraisemblance

Niveau	Libellé	Description
1	Exceptionnel	Théoriquement possible, pas de cas rencontré par ailleurs, ou réalisable dans des conditions particulières, très difficiles à obtenir, nécessitant des moyens et compétences très importants. Evénement très rare s'il s'agit d'un accident (une occurrence sur une période de plusieurs dizaines d'années).
2	Peu probable	Cas déjà rencontré une ou plusieurs fois, rarement (une occurrence sur une période d'une dizaine d'années) pour un incident d'origine involontaire, ou réalisable dans des conditions difficiles pour une malveillance, avec nécessité de personnes organisées, très compétentes et disposant de moyens importants, ou malveillance présentant peu d'intérêt pour son auteur.
3	Plausible	Cas rencontré assez fréquemment (une occurrence sur une période d'une à plusieurs années) par ailleurs, pouvant se produire avec probabilité pour un incident d'origine involontaire, ou réalisable dans des conditions occasionnelles pour une malveillance, par des personnes ou organisations dotées de moyens limités.
4	Quasi certain	Cas auquel le système est de toute façon confronté, fréquent (plusieurs fois par an), s'il s'agit d'un incident d'origine involontaire ou réalisable facilement et avec un intérêt évident s'il s'agit d'une malveillance.

L'estimation des niveaux de risques permet d'assigner une valeur unique aux événements redoutés et permet ainsi de les classer. Les niveaux de risques tiennent compte à la fois de la gravité de l'impact et de la vraisemblance de l'événement. Ainsi, un événement ayant un impact très fort ne présentera pas un niveau de risque élevé si son occurrence est faible.

Le tableau suivant permet d'orienter le traitement des risques, les risques de niveau « Fort » devant faire l'objet d'un traitement prioritaire.

Tableau 3 : Echelle de niveau de risques

<b>Niveau d'impact</b>					
Critique	Modéré	Fort	Fort	Fort	
Important	Limité	Modéré	Modéré	Fort	
Significatif	Limité	Modéré	Modéré	Modéré	
Mineur	Limité	Limité	Limité	Limité	
	<i>Exceptionnel</i>	<i>Peu probable</i>	<i>Plausible</i>	<i>Quasi certain</i>	<b>Niveau de vraisemblance</b>

## Echelle de classification des informations pour la confidentialité

### Avertissement

L'échelle de classification ci-dessous, conforme à la Politique Ministérielle de sécurité des systèmes d'information, permet d'estimer le besoin de confidentialité d'une information. Des exemples illustratifs sont proposés. Cependant la finalité, l'étendue du projet, sa durée, le nombre d'utilisateur, la population concernée, le volume ou encore l'attractivité particulière des données sont autant de critères qui peuvent modifier le besoin de confidentialité d'une information dans le contexte particulier d'un projet.

Tableau 4 : Echelle de classification des informations pour la confidentialité

Niveau	Libellé	Exemples
4	<b>Secret</b> (Loi Informatique et Libertés, données sensibles)	<p><b>Informations nominatives :</b></p> <ul style="list-style-type: none"> <li>- Informations de santé : pathologie, antécédents familiaux, observation médicale,</li> <li>- situations ou comportements à risques</li> <li>- Informations relatives aux infractions, condamnations ou mesures de sûreté</li> <li>- Informations relatives à des suspicions de fraudes ou d'infractions</li> <li>- Origines raciales ou ethniques, opinions politiques, philosophiques, religieuses, appartenances syndicales des personnes, la vie sexuelle</li> </ul> <p><b>Informations non nominatives :</b></p> <ul style="list-style-type: none"> <li>- Informations liées à l'organisation et à la stratégie de l'organisme, dont la révélation aurait un impact critique sur la conduite de ses missions</li> <li>- Informations liées aux mécanismes de fraudes et aux failles ou vulnérabilités de sécurité, dont la révélation pourrait être exploitée pour nuire aux missions de l'organisme</li> <li>- Données relevant du patrimoine scientifique et technique d'infrastructures vitales.</li> </ul>
3	<b>Confidentiel</b> (Loi Informatique et Libertés, données à caractère personnel directes)	<p><b>Toute information nominative ne rentrant pas dans la classe « secret » et notamment :</b></p> <ul style="list-style-type: none"> <li>- NIR, Etat-civil, identité, données d'identification (nom, prénom, adresse, photographie, date, lieu de naissance),</li> <li>- Appréciation sur les difficultés sociales des personnes</li> <li>- Informations d'ordre économique et financière (revenus, situation financière)</li> <li>- Vie personnelle : habitude de vie, situation familiale et sociale</li> <li>- Vie professionnelle : CV, Situation professionnelle, Scolarité, formation, Distinction</li> <li>- Informations biométriques : contour de la main, empreintes digitales, réseaux veineux, iris de l'œil, reconnaissance faciale, reconnaissance vocale, autre procédé</li> </ul>
2	<b>Restreint</b> (Loi Informatique et Libertés, données à caractère personnel indirectes)	<ul style="list-style-type: none"> <li>- Données de localisation (déplacement, données GPS, GSM, etc) par satellite, par téléphone mobile ou autre (adresse IP, logs, etc)</li> <li>- Identifiants des terminaux, Identifiants de connexions, Information d'horodatage...</li> <li>- procédures, description de processus, instructions, Intranet</li> <li>- enregistrements non nominatifs (dates, heures, actions, états, etc.)</li> <li>- informations personnelles que le salarié a identifiées explicitement comme tel dans le système d'information</li> <li>- Données de connexion</li> </ul>
1	<b>Public</b> (Hors Loi Informatique et Libertés)	Informations ayant vocation à être publiées : éditoriaux, publication Extranet, statistiques publiables, campagnes de communication, etc.

## Exemples de solutions en fonction de la classification de l'information à protéger

Les moyens de protection de l'information sont proportionnels à la vraisemblance du risque tel que perçu par le responsable du traitement. Ces protections traitent l'accès, le transfert, le stockage et déterminent la trace utile laissée par l'utilisateur. Les exemples ci-dessous illustrent l'effort de protection en fonction du niveau de confidentialité, dans une liste non exhaustive et dont la pertinence doit être étudiée dans chaque projet.

Tableau 5 : Exemples de solutions habituellement utilisées pour la protection des informations

Niveau	Libellé	Recommandations
4	<b>Secret</b>	Contrôle d'accès par authentification forte Diffusion à une population restreinte dont la liste est tenue à jour Contrôle de pertinence de la demande d'accès (rebond) Trace détaillée des accès et des actions, y compris consultation Protection éventuelle par chiffrement de l'information et du transfert
3	<b>Confidentiel</b>	Contrôle d'accès par identification et mot de passe renforcé Liste des profils ayant un droit d'accès Gestion des habilitations répondant aux bonnes pratiques Trace des accès et des actions entraînant un risque Protection du moyen de transfert
2	<b>Restreint</b>	Contrôle d'accès par identification et mot de passe Liste des domaines ayant un droit d'accès Trace des accès
1	<b>Public</b>	Pas de besoin de contrôle d'accès

Renseignements sur le demandeur			Téléphone
R1	Direction / responsable		X
R2	Nom du projet (pour la MOA)		
R3	Numéro / code du projet		
R4	Chef de projet métier (MOA)		
R5	Chef de projet SI (MOE)		

## 1. Profil du projet

Tableau 6 : facteurs de sensibilité du projet

#	Thème	Réponse de la maîtrise d'ouvrage
R6	Domaine du projet ou du service	<input type="checkbox"/> Interne à l'établissement <input type="checkbox"/> Relation avec l'extérieur <input type="checkbox"/> Pilote, expérimentation <input type="checkbox"/> Projet organisationnel <input type="checkbox"/> Autre :
R7	Echanges envisagés	<input type="checkbox"/> Au sein de l'établissement <input type="checkbox"/> Entre établissements de santé <input type="checkbox"/> Avec des entités non établissements de santé <input type="checkbox"/> Autre :
R8	Réseau envisagé	<input type="checkbox"/> Réseau interne <input type="checkbox"/> Internet <input type="checkbox"/> VPN <input type="checkbox"/> Autre :
R9	Sensibilité maximum de l'information traitée	<input type="checkbox"/> Informations à caractère personnel : données nominatives, médicales, sociales... <input type="checkbox"/> Informations internes à l'établissement : financières, comptables, contractuelles, ressources humaines <input type="checkbox"/> Autre :
R10	Utilisateurs	<input type="checkbox"/> Personnel de l'établissement : professionnels de santé (soignants, médicaux, paramédicaux, ...), administratifs... <input type="checkbox"/> Personnel extérieur : patients, professionnels de santé (médecine de ville, établissements de santé, médico-social, ...), personnel en formation...
R11	Nombre d'utilisateurs estimé	
R12	Partenaires extérieurs	<input type="checkbox"/> CPAM <input type="checkbox"/> Mutuelles <input type="checkbox"/> Prestataires <input type="checkbox"/> Trésorerie <input type="checkbox"/> ARS <input type="checkbox"/> GCS E-santé <input type="checkbox"/> Autres établissements de santé <input type="checkbox"/> Autres :
R13	Importance stratégique pour la Direction Générale	<input type="checkbox"/> Stratégique <input type="checkbox"/> Prioritaire <input type="checkbox"/> Normale Date de mise en œuvre :



#	Thème	Réponse de la maîtrise d'ouvrage
R14	Réglementations applicables	<input type="checkbox"/> Données à caractère personnel (si oui, voir également R15 à R18) <input type="checkbox"/> Données de santé à caractère personnel (si oui, voir également R15 à R18) <input type="checkbox"/> Réglementations financières & comptables  Préciser les décrets ou articles (décret hébergeur, décret confidentialité) :
R15	Avis CNIL	<input type="checkbox"/> A Demander <input type="checkbox"/> Demandé <input type="checkbox"/> Obtenu <input type="checkbox"/> Non nécessaire
R16	Moyen de collecte des données à caractère personnel	<input type="checkbox"/> Fichier interne / externe <input type="checkbox"/> Requête <input type="checkbox"/> Questionnaire Précisez :
R17	Information des personnes	<input type="checkbox"/> Sur le questionnaire <input type="checkbox"/> Journal interne <input type="checkbox"/> Sur le site web <input type="checkbox"/> Affiche <input type="checkbox"/> Recueil de consentement <input type="checkbox"/> Autre :
R18	Estimation de la population concernée	Nombre estimé :

R19 : décrivez brièvement le projet, sa finalité et ses contraintes.

Projet :
Finalité :
Contraintes :

R20 : Classifiez (selon l'échelle proposée Tableau 4) en quatre niveaux les informations saisies, traitées et restituées par le système ?

Niveau	Informations traitées	Origine (base de données, organisme...)	Destinataire (base de données, organisme...)	Durée de conservation
Secret				
Confidentiel				
Restreint				
Public				

R21 : Listez les acteurs (ou les rôles) dans le traitement, et leurs droits d'accès sur les niveaux d'informations du système ? (Aucun accès  $\emptyset$  ; accès en Lecture uniquement ; accès en lecture et Écriture.)

Acteurs (utilisateurs et partenaires extérieurs)	Niveaux d'informations			
	Secret	Confidentiel	Restreint	Public
	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.
	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.
	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.
	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.
	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.	<input type="checkbox"/> $\emptyset$ <input type="checkbox"/> L. <input type="checkbox"/> É.

R22 : Quelles sont les principales fonctions de votre système, en termes de processus ? Décrivez le processus de manière chronologique :

N°	Etapes	Principales actions ou fonctions du processus
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
...		

R23 : Indiquez où se procurer la documentation du projet (références documentaires, liens) et le schéma du processus :

R24 : Autres informations utiles à la compréhension du système :

## 2. Risques liés à une perte de disponibilité

Évaluez les conséquences de l'arrêt prolongé du système, dans le pire des cas, et précisez dans quel délai ces conséquences deviendraient insupportables. **Se reporter aux tableaux 1, 2 et 3.**

Impact					Vraisemblance				Niveau de risque		
4 Critique	3 Important	2 Significatif	1 Mineur	NC Pas d'impact	4 Quasi certain	3 Plausible	2 Peu probable	1 Exceptionnel	Fort	Modéré	Limité

Tableau 7 : Conséquences d'une perte de disponibilité

#	Type d'impact	Événement redouté / Description	Impact (1 à 4 ou NC)	Vraisemblance					Vraisemblance	Niveau de risque	Commentaires
				< 1 heure	< 4 heures	1 jour	1 à 7 jours	≥ 1 semaine			
D1	Décisions de pilotage	L'arrêt du fonctionnement nuit à des décisions de gestion et de pilotage de l'Établissement.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D2	Perte de traitements en cours	L'arrêt du fonctionnement affecte des traitements en cours (prescription, mouvements des patients, liquidations).		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D3	Fraude	L'arrêt du fonctionnement peut entraîner une fraude (usurpation d'identité ou de droit).		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D4	Confiance du public	L'arrêt du fonctionnement porte atteinte à l'image publique ou la réputation de l'établissement auprès de ses patients, partenaires et fournisseurs.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D5	Surcoûts	L'arrêt prolongé du système entraîne des surcoûts (perte d'antériorités, redondance d'exams...).		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D6	Responsabilité légale	L'arrêt de fonctionnement conduit au non-respect de dispositions légales, réglementaires ou contractuelles.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D7	Conséquences pour le personnel	L'arrêt de fonctionnement a un impact sur le bien-être ou la motivation du personnel.		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
D8	Variations du besoin de disponibilité dans le temps	A quel moment le besoin de disponibilité est-il maximum ?		<input type="checkbox"/> Permanent <input type="checkbox"/> Période :							
D9	Besoin de reconstruction après reprise	Une fois le système redémarré, faudra-t-il reconstruire les données entrantes qui n'auraient pas été traitées pendant l'interruption ?		<input type="checkbox"/> Oui <input type="checkbox"/> Non							
D10	Reconstruction <u>avant</u> reprise	Faudra-t-il, avant de redémarrer, reconstruire au préalable les données entrantes non traitées pendant l'interruption ?		<input type="checkbox"/> Oui <input type="checkbox"/> Non							
D11	Délai de reconstruction (si « oui » à D9 ou D10)	Dans quel délai devra t-on reconstruire l'information non traitée pendant l'interruption ?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

D12 Commentaires éventuels :

### 3. Risques liés à une perte d'intégrité

Évaluez les conséquences d'erreurs dans l'information ou de modifications malveillantes visant à tromper les utilisateurs, dans le pire des cas. **Se reporter aux tableaux 1, 2 et 3.**

Impact					Vraisemblance				Niveau de risque		
4 Critique	3 Important	2 Significatif	1 Mineur	NC Pas d'impact	4 Quasi certain	3 Plausible	2 Peu probable	1 Exceptionnel	Fort	Modéré	Limité

Tableau 8 : Conséquences d'une perte d'intégrité

#	Type d'impact	Événements redoutés	Impact (1 à 4 ou NC)	Vraisemblance	Niveau de risque	Commentaires
11	Erreurs de gestion	Des modifications non autorisées de l'information ou des informations erronées entraînent des décisions de gestion faussées.				
12	Perte de traitements en cours	Des modifications non autorisées de l'information ou des informations erronées entraînent l'interruption ou l'annulation de traitements en cours (liquidation, avis, instructions, etc.)				
13	Malveillance	Des modifications non autorisées de l'information peuvent survenir par une malveillance.				
14	Confiance du public	Les erreurs ou les modifications non autorisées d'information portent atteinte à l'image publique ou la réputation de l'ES auprès de ses patients, partenaires et fournisseurs.				
15	Surcoûts	Les erreurs ou les modifications non autorisées de l'information entraînent des surcoûts - par exemple pour rechercher les erreurs et reconstruire l'intégrité d'informations perdues ou corrompues.				
16	Responsabilité légale	Les erreurs ou les modifications non autorisées de l'information conduisent au non-respect de dispositions légales, réglementaires ou contractuelles.				
17	Conséquences psychologiques pour le personnel	Les erreurs ou les modifications non autorisées de l'information ont un impact sur la confiance du personnel dans le système - par exemple les utilisateurs ne se fient plus au système et organisent des solutions de contournement.				

18 Commentaires éventuels :

## 4. Risques liés à une perte de confidentialité

Evaluez les conséquences d'une divulgation accidentelle ou intentionnelle de l'information, dans le pire des cas. **Se reporter aux tableaux 1,2 et 3.**

Impact					Vraisemblance				Niveau de risque		
4 Critique	3 Important	2 Significatif	1 Mineur	NC Pas d'impact	4 Quasi certain	3 Plausible	2 Peu probable	1 Exceptionnel	Fort	Modéré	Limité

Tableau 9 : Conséquences d'une divulgation

#	Type d'impact	Événements redoutés	Impact (1 à 4 ou NC)	Vraisemblance	Niveau de risque	Commentaires
C1	Image de l'établissement	La divulgation porte atteinte à la crédibilité de l'établissement auprès de ses patients et partenaires.				
C2	Fraude	La divulgation permet d'exploiter financièrement une faille du système d'information (génération d'un chantage, reventes d'informations).				
C3	Surcoûts	La divulgation entraîne une dépense financière (remise aux normes, pénalités).				
C4	Responsabilité légale	La divulgation est en contradiction avec la loi, un règlement ou un contrat.				
C5	Conséquences pour le personnel	La divulgation porte atteinte au bien-être ou à la motivation du personnel.				

C6 Commentaires éventuels :

## 5. Audit, besoin de preuves et de traces

Evaluez les conséquences d'une absence de preuves du bon fonctionnement du système, dans le pire des cas. **Se reporter aux tableaux 1, 2 et 3.**

Impact					Vraisemblance				Niveau de risque		
4 Critique	3 Important	2 Significatif	1 Mineur	NC Pas d'impact	4 Quasi certain	3 Plausible	2 Peu probable	1 Exceptionnel	Fort	Modéré	Limité

Tableau 10 : Analyse du besoin de preuve

#	Type d'impact	Événements redoutés	Impact (1 à 4 ou NC)	Vraisemblance	Niveau de risque	Commentaires
P1	Contentieux, fraudes	L'absence de preuves issues du système empêche la recherche des responsabilités.				
P2	Fraude interne, reniement d'action, absence de journalisation du fonctionnement	La modification accidentelle ou délibérée des preuves du fonctionnement du système a des conséquences légales, financières ou sur le fonctionnement du système.				
P3	Responsabilité légale	La divulgation des traces ou preuves peut porter atteinte à l'établissement.				

Si le besoin de preuves est un enjeu particulier du projet, merci de le préciser :

## 6. Evaluation Sécurité du Système d'Information

(réservée au référent sécurité)

Direction	
Application ou projet	
Date	

Niveau de risque max		Référent sécurité
3	Fort <input type="checkbox"/>	Nom :
2	Modéré <input type="checkbox"/>	Téléphone :
1	Limité <input type="checkbox"/>	Courriel :

Analyse non réalisée / demande d'informations complémentaires :

Tableau 11 : Evaluation du système à partir des informations fournies par la maîtrise d'ouvrage

DICP global	D	I	C	P
Évaluation d'ensemble du niveau de risque				
Délai global critique d'interruption				
Besoin de reconstruction de l'information	Avant :		Après :	
Demande d'avis CNIL à envisager				

Tableau 12 : Actions recommandées pour le projet en l'état des informations transmises

Préconisations
<input type="checkbox"/> <b>L'analyse peut se limiter au présent Questionnaire</b> Les principaux objectifs de sécurité à atteindre sont : <ul style="list-style-type: none"> <li><input type="checkbox"/> Confidentialité</li> <li><input type="checkbox"/> Intégrité</li> <li><input type="checkbox"/> Disponibilité</li> <li><input type="checkbox"/> Preuves et contrôles</li> </ul>
<input type="checkbox"/> <b>L'analyse doit être approfondie pour pouvoir exprimer les besoins en sécurité</b> ou bénéficier de mesures complémentaires : <ul style="list-style-type: none"> <li><input type="checkbox"/> Mener une analyse de risques approfondie</li> <li><input type="checkbox"/> Prévoir un audit avant déploiement</li> <li><input type="checkbox"/> Prévoir un audit après le déploiement</li> <li><input type="checkbox"/> Organiser une instance de suivi Sécurité Système d'Information</li> <li><input type="checkbox"/> Rédiger une procédure de secours détaillée</li> <li><input type="checkbox"/> Mener l'action suivante :</li> </ul>

Demandes transmises ou à transmettre au directeur de projet		
Demande de transmission des documents projet	<input type="checkbox"/> Oui	<input type="checkbox"/> Non
Demande d'intégrer le référent sécurité à la liste de diffusion des comptes rendus des réunions du projet	<input type="checkbox"/> Oui	<input type="checkbox"/> Non
Demande de rendez-vous, date :	<input type="checkbox"/> Oui	<input type="checkbox"/> Non

Remarques ou référence documentaire :

## 7. Préconisations techniques (réservé à la maîtrise d'œuvre)

La section 7 peut ne pas être renseignée si une analyse approfondie a été demandée en section 6

	Nom / Service	Téléphone	Courriel
Intervenant			

Tableau 13 : Principaux moyens de traitement et de protection envisagés

### Se reporter au Tableau 5.

Dans le cas où le système relève de la Loi informatique et libertés du 6 janvier 1978 (cf. question R15), les éléments techniques suivants sont requis pour éclairer le Correspondant Informatique et Libertés (CIL).

Au-delà de la simple description de moyens, les préconisations de solutions doivent répondre aux enjeux de la CNIL : l'usage anormal ou illégitime, la modification non souhaitée et la disparition des données à caractère personnel, ainsi que l'impossibilité ou l'erreur dans l'exercice du droit d'accès et de rectification. Les solutions doivent considérer tous les supports du système : matériel, logiciel, transferts, papiers, personnes.

#### T1 Identification et authentification

- Carte de professionnel de santé ou d'établissement (CPx)
- Profils d'habilitation détaillés
- Login et mot de passe pour les menus : annulation, consultation et gestion de base
- Autres ou précisions :

#### T2 Echanges de données

En interne :

- Liaison informatique (messagerie, serveurs, interfaces)
- Sauvegarde des données sur le serveur
- Support physique (CD, DVD, clef USB, DD)
- Autres ou précisions :

En externe :

- Liaison informatique (messagerie, serveurs de partenaires)
- Support physique (CD, DVD, clef USB, DD)
- VPN
- Liaisons sécurisées
- Autres ou précisions :

#### T3 Journalisation

- Identifiant du poste de travail     Identifiant de l'utilisateur
- Date/heure de connexion     Date/heure de déconnexion
- Opération effectuée en :  Consultation     Création     Mise à jour     Suppression     Autre
- Référence des données accédées
- Autres ou précisions :

#### T4 Hébergement des données

- Interne à l'établissement
- Externalisé
- Externalisé chez un hébergeur agréé données de santé

Précisez :

T5 Description des solutions, par le chef de projet SI (MOE) :

## 8. Observations du CIL, à défaut du responsable de traitement

	Nom / service	Téléphone	Courriel
CIL			

Ce chapitre est à renseigner par le Correspondant Informatique et Liberté (CIL) de l'organisme.

Tableau 14 : Prise en compte des enjeux CNIL

	Centres d'intérêt CNIL	Niveau	Commentaires
L1	Caractère identifiant des données traitées	<input type="checkbox"/> Aucun <input type="checkbox"/> Faible <input type="checkbox"/> Fort	
L2	Préjudice potentiel pour les personnes identifiées	<input type="checkbox"/> Aucun <input type="checkbox"/> Faible <input type="checkbox"/> Fort	
L3	Maîtrise du droit d'accès des personnes identifiées aux données les concernant	<input type="checkbox"/> Insuffisant <input type="checkbox"/> Satisfaisant	

Tableau 15 : Préconisations du CIL

L4 Formalités préalables	L5 Recommandations
<input type="checkbox"/> Aucune  <input type="checkbox"/> Inscription au registre  <input type="checkbox"/> Demande d'avis  <input type="checkbox"/> Demande d'autorisation	Nature de la recommandation : <input type="checkbox"/> Finalités  <input type="checkbox"/> Données  <input type="checkbox"/> Durée de conservation  <input type="checkbox"/> Sécurités  <input type="checkbox"/> Information des instances représentatives du personnel

L6 Commentaire du CIL :