Checklist PRA / NIS2 – Édition 2026

Les points essentiels pour assurer la continuité des soins et la conformité réglementaire

Cette checklist a pour objectif d'aider les établissements de santé à évaluer de manière concrète le niveau de maturité de leur Plan de Reprise d'Activité (PRA) au regard des exigences opérationnelles et réglementaires actuelles, notamment NIS2 et HDS.

1. Gouvernance et pilotage du PRA

- ☐ Le PRA est formalisé dans un document à jour, validé par la direction
- ☐ Les rôles et responsabilités sont clairement définis (DSI, RSSI, direction, prestataires)
- ☐ Les coordonnées des acteurs clés sont accessibles même en situation dégradée
- ☐ Les décisions critiques (activation du PRA, communication, priorisation) sont clairement cadrées

2. Identification des systèmes critiques

- ☐ Les systèmes critiques ont été identifiés (SI médicaux, DPI, RIS/PACS, outils administratifs essentiels)
- ☐ Les dépendances techniques sont connues (réseau, hébergement, fournisseurs, cloud, énergie)
- ☐ Les priorités de redémarrage sont définies et documentées
- ☐ Les délais de reprise attendus (RTO) et les pertes de données acceptables (RPO) sont formalisés

3. Sauvegardes et capacités de restauration

- ☐ Les sauvegardes couvrent l'ensemble des données critiques
- ☐ Les sauvegardes sont protégées contre les ransomwares (immutabilité, cloisonnement)
- ☐ Des tests de restauration complets sont réalisés régulièrement
- ☐ Les résultats des tests sont documentés et corrigés si nécessaire

4. Procédures de reprise et modes dégradés

- [ ] Les procédures de reprise sont claires, accessibles et compréhensibles
- [ ] Des scénarios d'incidents réalistes ont été définis (ransomware, panne majeure, indisponibilité hébergeur)
- [ ] Les modes de fonctionnement dégradés sont connus des équipes métiers
- [ ] Les impacts sur la continuité des soins ont été anticipés

5. Conformité NIS2 : gestion et notification des incidents

- [ ] Une procédure de détection et de qualification des incidents cyber est en place
- [ ] Les délais de notification NIS2 sont connus et intégrés aux procédures
- [ ] Les canaux de communication internes et externes sont définis
- [ ] Les incidents font l'objet d'un retour d'expérience formalisé

6. Exigences HDS : disponibilité et protection des données de santé

- [ ] La disponibilité des données patients est garantie en cas d'incident
- [ ] Les engagements HDS sont intégrés dans le PRA
- [ ] Les accès aux données sont maîtrisés pendant les phases de reprise
- [ ] Les prestataires impliqués respectent les exigences HDS

7. Tests, exercices et amélioration continue

- [ ] Le PRA est testé régulièrement (tests techniques, exercices de crise)
- [ ] Les équipes sont sensibilisées et formées
- [ ] Les évolutions réglementaires et techniques sont intégrées au PRA
- [ ] Le plan est mis à jour après chaque test ou incident réel