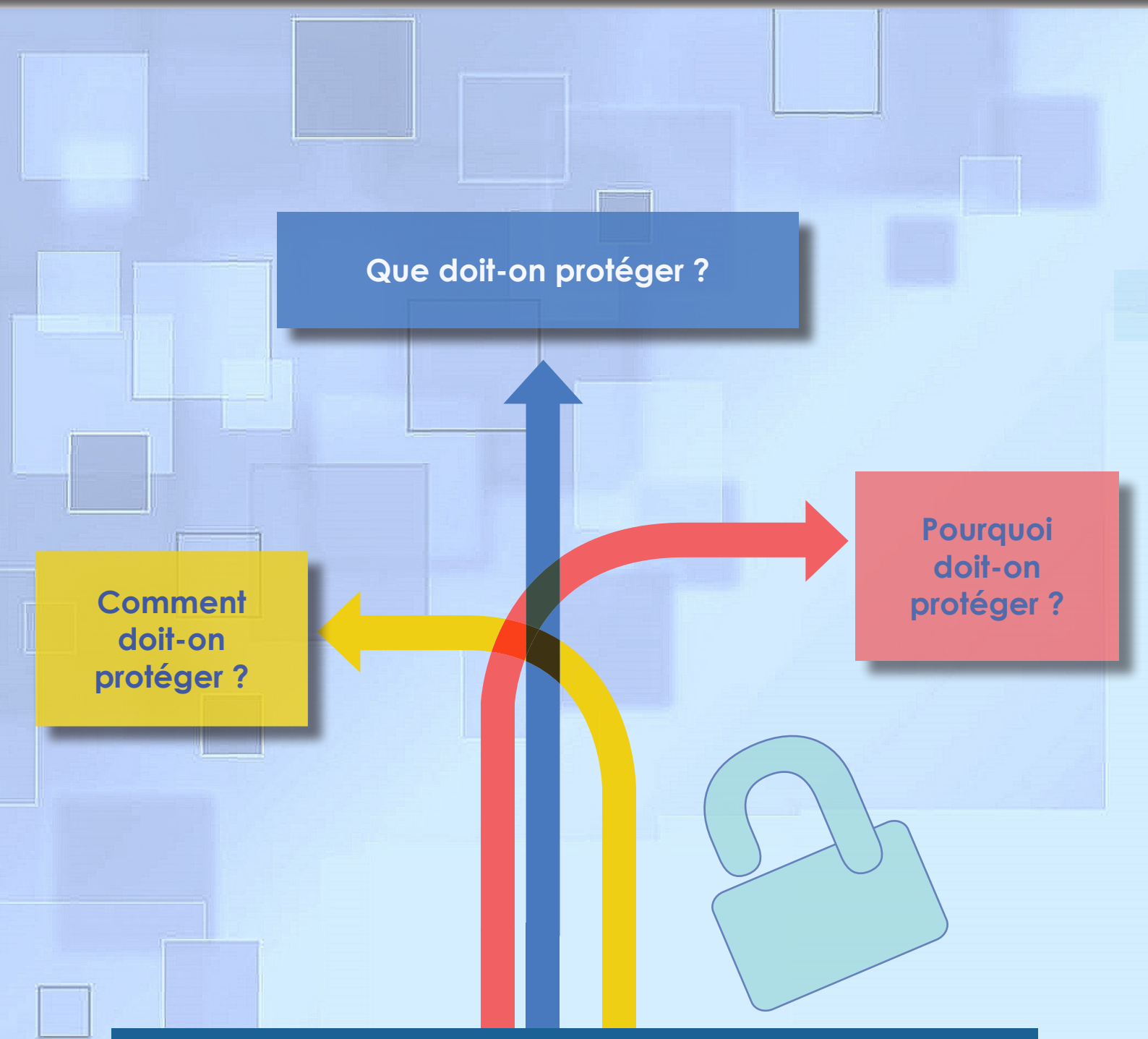
SÉCURITÉ DES SYSTÈMES D'INFORMATION

CE QU'IL FAUT SAVOIR

Mars 2015

Représentation, ressource et référence des Services de santé au travail interentreprises



Document à l'attention des directeurs de Service, présidents, CA et CC, responsables RH, responsables comptable, responsables Informatique, médecins coordinateurs et/ou CMT, secrétaires du CE,...

Que doit-on protéger ?

- Les données des adhérents et de leurs salariés,
- Les données du personnel du Service,
- La continuité de l'activité du Service,
- Les documents et les informations produits par le Service.

Pourquoi doit-on protéger ?

- Loi Informatique et Liberté (loi n° 78-17 du 6 janvier 1978),
- Rapport du Conseil National de l'Ordre des Médecins, de 2004, sur le dossier médical en médecine du travail (DMT),
- Arrêté du 5 mars 2004 de l'Agence Nationale d'Accréditation et d'Évaluation de Santé, sur l'accès aux informations concernant la Santé d'une personne, modalités pratiques et accompagnement,
- Code pénal, Code du travail, Code de la santé publique, Code de déontologie médicale,
- Recommandation de la HAS, de 2009, sur le dossier médical en Santé au travail (DMST).

Comment doit-on protéger ?

L'indispensable

Faire les déclarations CNIL obligatoires

Chaque traitement et/ou fichier contenant des données à caractère personnel doit être identifié et dûment déclaré auprès de la CNIL. Par exemple : le fichier du personnel des SSTI, le fichier des salariés suivis, le fichier des données médicales des salariés suivis, le fichier des entreprises adhérentes (s'il contient des données nominatives),…

Stocker les données de manière suffisamment sécurisée et séparée

Les données personnelles à caractère médical ne peuvent être stockées sur les mêmes supports que les données administratives et/ou les e-mails. De plus ces données doivent avoir un niveau de sécurité suffisant (par exemple être chiffrées). Cela implique aussi bien leur stockage en serveur central, que sur les postes utilisateurs ou encore sur les supports amovibles et dans les e-mails.

Sauvegarder les données de manière régulière, vérifiée et sécurisée

L'ensemble des données nécessaires au bon fonctionnement du Service doivent être sauvegardées sur des supports amovibles et externalisés. La sauvegarde doit avoir une procédure rigoureuse permettant un retour en arrière. Il doit également être envisagé le stockage de ces sauvegardes, ainsi que la sécurité des données qui y sont inscrites. Enfin, ces sauvegardes doivent être testées régulièrement « à blanc ».

Gérer les droits d'accès de façon maîtrisée, notamment au niveau des habilitations d'accès aux données médicales

Les accès aux lieux et aux données doivent être réglementés et compartimentés au « besoin de voir et/ou d'agir ». Des procédures strictes doivent être mises en place pour rendre inopérant tout accès inopiné d'un utilisateur ou d'un non-utilisateur à des espaces auxquels il n'aurait pas les droits. Enfin, l'ajout et le retrait d'utilisateurs doivent être correctement procédurés.

Rédiger une charte informatique

Il convient d'avoir une charte informatique encadrant l'usage et le non usage des outils technologiques au sein du Service.

Le nécessaire

Mettre en œuvre une sauvegarde patrimoniale (maximum 50 ans après la dernière exposition)

Les données médicales de suivi des salariés ont une durée maximale de conservation particulière, notamment dans le cas d'exposition à certains risques. Il convient de mettre en œuvre un processus particulier afin

de répondre à ces exigences. Attention : le processus de sauvegarde pour recouvrement ne répond pas aux mêmes besoins, il doit donc bien y avoir deux réflexions.

Gérer les codes malveillants (virus, hameçonnage,…)

Les outils utilisés et installés doivent être opérants, c'est-à-dire qu'ils doivent être maintenus à jour de manière extrêmement précise. Ils doivent pouvoir être mis en arrêt par les utilisateurs. De plus, des cloisonnements de réseaux sont à mettre en œuvre afin de limiter une éventuelle défaillance des outils de protection.

Sécuriser et surveiller les communications

Les communications entre sites, ou d'un site vers l'extérieur doivent être sécurisées de manière adéquate au besoin (VPN entre sites par exemple), et elles doivent faire l'objet d'une surveillance attentive afin de déceler toute intrusion ou comportement anormal.

Gérer et utiliser de manière sérieuse la traçabilité des accès

L'ensemble des actions, et particulièrement les actions ayant un impact direct ou indirect sur les données personnelles, doit être tracé ; les traces doivent être stockées séparément. Ces traces doivent être vérifiées régulièrement afin d'identifier des actions inopportunes ou malveillantes.

Mettre en place un Plan de Continuité d'Activité (PCA) adapté et testé

Un Service de santé au travail ne peut pas s'arrêter de fonctionner durablement, il convient donc de mettre en place un PCA conforme aux règles de l'art du moment. Ce PCA doit être régulièrement testé à blanc afin de ne pas être pris au dépourvu le cas échéant.

Avoir un système de management de la sécurité complet

L'ensemble des procédures de gestion de la sécurité du système d'information doit être documenté, afin que chacun puisse s'y référer en cas de doute sur l'action à faire.

Le conseillé

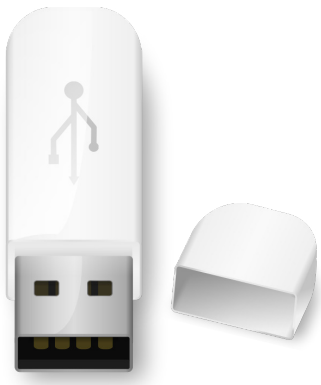
Sensibiliser les membres du personnel aux bonnes pratiques

Les inattentions ou les erreurs d'exécution peuvent être la source de dégâts majeurs, c'est pourquoi il convient de mettre en œuvre des cycles réguliers de sensibilisation aux bonnes pratiques pour le personnel.

Maîtriser la gestion des supports externes

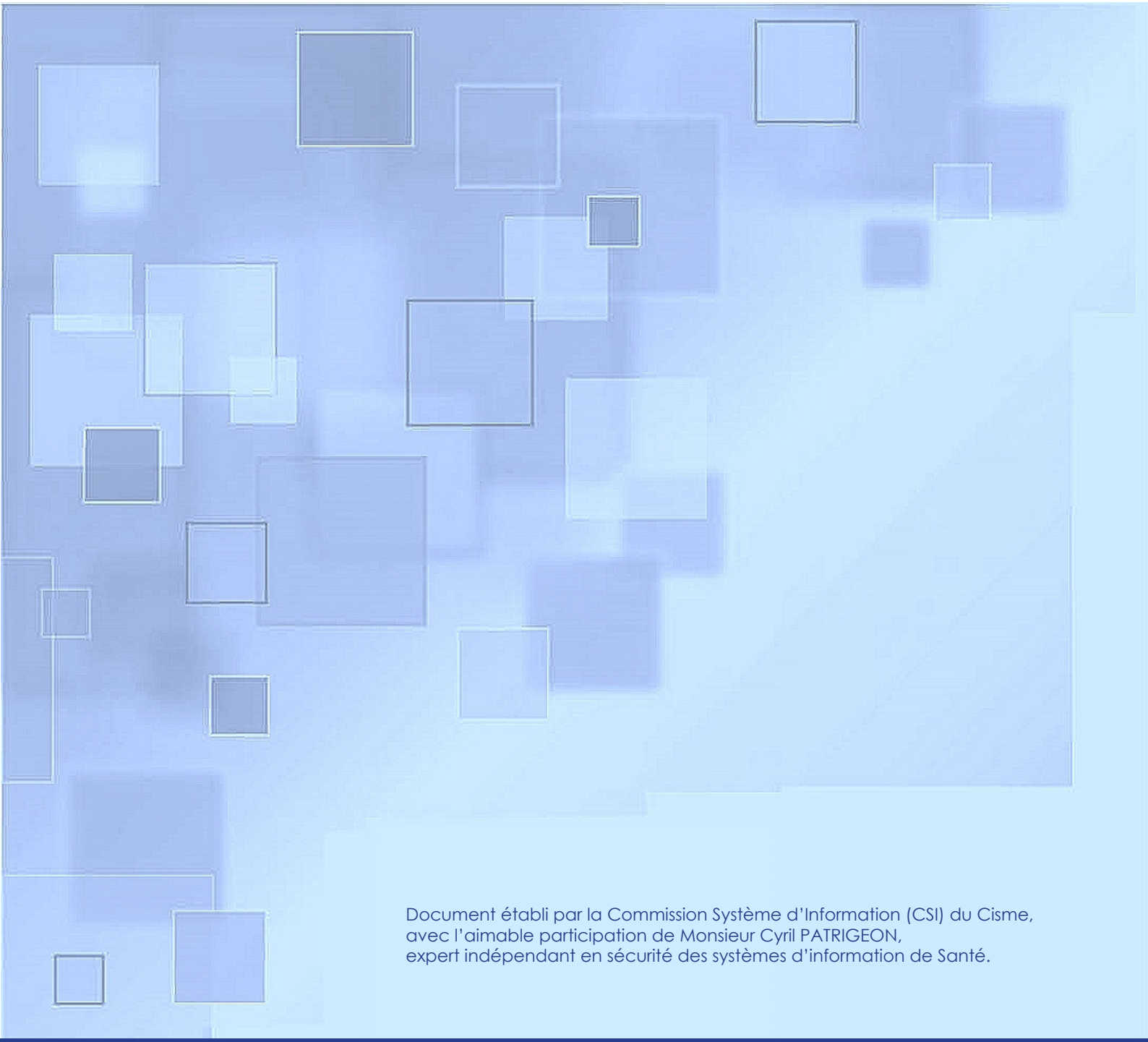
Dans le cas où les supports externes (clés usb, téléphones portables, CD, disques durs,…) ne peuvent êtres bannis de l'usage professionnel, il convient d'en maîtriser la gestion, notamment il faut bien identifier ce qui est permis et ce qui ne l'est pas, ainsi que les procédures idoines des données pouvant être stockées sur ces supports.

Gérer de manière cohérente la mise au rebut des supports de données sensibles



Les supports ayant accueilli, même de manière temporaire, des données sensibles, doivent avoir une gestion appropriée de mise au rebut. Il faut donc identifier tous ces supports (ne pas oublier la photocopieuse par exemple), et mettre en œuvre des processus de destruction opérants et suffisants.

10, rue de la Rosière - 75015 PARIS
info@cisme.org
www.cisme.org



Document établi par la Commission Système d'Information (CSI) du Cisme,
avec l'aimable participation de Monsieur Cyril PATRIGEON,
expert indépendant en sécurité des systèmes d'information de Santé.

Commission Système d'information du Cisme - Mars 2015