ACADÉMIE NATIONALE DE MÉDECINE

# Les attaques des systèmes informatiques des hôpitaux mettent en danger la vie des patients[1]

## Communiqué de l'Académie nationale de médecine

**10 octobre 2024**

Les cyber-attaques sont de nouvelles formes de criminalité dont sont victimes de nombreuses personnes, ainsi qu'un nombre croissant d'organismes publics ou privés. Depuis le milieu des années 2010, les cybercriminels se sont attaqués aux hôpitaux (1), dans un but de vandalisme ou de déni de service, ou pour exiger une rançon, l'insertion d'un rançongiciel altérant la bonne marche de services ou équipements essentiels (2) en rendant inutilisables les données des systèmes.

En France, en 2021, 1 582 établissements de santé ont été victimes d'une attaque, soit un établissement sur six, deux fois plus qu'en 2020. En 2023, les plus grands hôpitaux publics ont été ciblés (hôpital de la Pitié-Salpêtrière et hôpital Saint-Antoine à Paris, hôpitaux de l'Assistance Publique-Hôpitaux de Marseille et des Hospices Civils de Lyon). Les établissements privés n'ont pas été épargnés. En février 2024, l'hôpital d'Armentières a été la cible d'une cyberattaque avec une demande de rançon qui a eu pour conséquence la fermeture du service des urgences durant 24 heures (3).

Au-delà de l'extorsion de fonds ou du coût lié au renforcement de la sécurité du système d'information d'un hôpital, ces cyber-attaques mettent en danger la vie des patients, de plusieurs façons : retard à la prise en charge des urgences ; atteinte du bon fonctionnement de dispositifs d'assistance vitale, par exemple au bloc opératoire ou en réanimation ; allongement du délai de mise en œuvre de certaines procédures diagnostiques ou thérapeutiques.

Des études récentes ont documenté l'impact de ces attaques sur le retard des soins aux patients, par exemple dans la prise en charge des accidents vasculaires cérébraux (4) ou d'un cancer (5). Une attaque récente de l'hôpital Guy's et St Thomas' à Londres (6) a illustré ces graves conséquences : annulation d'opérations chirurgicales ; impossibilité de procéder à des transfusions sanguines, les données requises ayant été effacées ; obligation de transférer des patients dans d'autres hôpitaux.

Face à l'accroissement des attaques informatiques contre les établissements de santé, des actions sont engagées dans de nombreux pays qui relèvent, au niveau national, des autorités en charge de la sécurité intérieure, de la cybersécurité et de la justice et, au niveau de chaque établissement de santé, du renforcement de la sécurité des systèmes d'informations et de la sensibilisation de ses personnels à ce risque.

[1] Communiqué de la Plateforme de Communication Rapide de l'Académie.

**CONTACT PRESSE : Virginie Gustin +33 (0)6 62 52 43 42 virginie.gustin@academie-medecine.fr**
**ACADÉMIE NATIONALE DE MÉDECINE**, 16 rue Bonaparte - 75272 Paris cedex 06
**Site** : *www.academie-medecine.fr* / **Twitter** : *@Acadmed*

**Compte tenu de la gravité potentielle de ces attaques sur la santé des patients, l'Académie nationale de médecine souligne :**

- La nécessité de documenter les impacts sanitaires de ces attaques sur les patients pris en charge ou en attente de prise en charge ;
- L'indispensable sensibilisation et formation aux risques des cyber-attaques pour tous les professionnels de santé usant du numérique dans les établissements de santé ;
- En complément des mesures de renforcement de la cybersécurité prévues dans le plan incitatif CaRE (7, 8), la vigilance extrême requise concernant les compétences spécifiques en cybersécurité des agents en charge des services informatiques ;
- La nécessaire préparation de tous les établissements de santé, par des mesures d'anticipation et d'organisation, pour assurer la continuité des activités en cas d'attaque, soit en mode dégradé, soit via un dispositif de coopération, préparé et testé à l'avance, entre établissements de santé ;
- Le caractère pénal des cyber-attaques des hôpitaux qui, au-delà de l'extorsion de fonds ou du vandalisme, constituent une mise en danger de la vie d'autrui, éventuellement un homicide.

**Références**


1. Argaw, S.T., Bempong, N.E., Eshaya-Chauvin, B. *et al.,* The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC Med Inform Decis Mak,* 2019*,* 19, 10.
2. Williams P.A., Woodward A.J., Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, *Med Devices Evid Res*, 2015, Jul 20.8: 305-16
3. Lemaignen J., Romain M. : Cyberattaques dans les hôpitaux, Le Monde, 7 décembre 2022
4. Dameff C., Tully J., Chan T.C. *et al.*, Ransomware attack associated with disruptions at adjacent emergency departments in the US, *JAMA*, 2023: 6(5) e 2312270
5. Keogh R., Harvey H., Brady C. *et al*., Dealing with digital paralysis: surviving a cyberattack in a national cancer center, *Journal of Cancer Policy,* 2024, 39, 100466
6. https://www.theguardian.com/society/article/2024/jun/11/cyber-attack-on-london-hospitals-to-take-many-months-to-resolve?CMP=Share;
7. Agence du numérique en Santé, Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social 2023, 2024, https://esante.gouv.fr/sites/default/files/media_entity/documents/observatoire-incidents-cybersecurite-sante-2023.pdf
8. Agence du numérique en Santé, Cybersécurité accélération et Résilience des Etablissements (CaRE), https://esante.gouv.fr/strategie-nationale/cybersecurite, consulté le 18 juillet 2024



**CONTACT PRESSE : Virginie Gustin +33 (0)6 62 52 43 42 virginie.gustin@academie-medecine.fr**
**ACADÉMIE NATIONALE DE MÉDECINE**, 16 rue Bonaparte - 75272 Paris cedex 06
**Site** : *www.academie-medecine.fr* / **Twitter** : *@Acadmed*