PROGESPLUS

Cabinets de radiologie :

Données de santé : comment répondre aux dernières normes de sécurité ?

- ☑ Comment sécuriser l'infrastructure informatique d'un cabinet de radiologie ?
- ☑ Comment assurer sa mise en conformité avec les dernières préconisations gouvernementales de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ?

BESOIN D'UN ACCOMPAGNEMENT ?

03.20.64.63.63

WWW.BLUE-SERVE.COM

THÉMATIQUES

1. Comment sécuriser l'infrastructure informatique d'un cabinet de radiologie ?
2. Comment assurer sa mise en conformité avec les dernières préconisations gouvernementales de l'ANSSI ?
3. Comment réagir en cas de cyberattaque pour protéger ses données de santé ?
4. Témoignage client : IMANORD - Imagerie médicale
5. L'infogérance au service des cabinets de radiologie
6. Faites le choix d'un partenaire de proximité

1. Comment sécuriser l'infrastructure informatique d'un cabinet de radiologie ?

Quels réflexes et outils adopter pour sécuriser mon environnement de travail et protéger les données de santé qu'il contient ?

Les données de santé font partie des informations les plus sensibles et, en conséquence, devant être les plus sécurisées. Selon la CNIL « les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique *(y compris la prestation de services de soins de santé)* qui révèlent des informations sur l'état de santé de cette personne ».

- Listez votre matériel et vos logiciels
- Réalisez des mises à jour régulières
- Installez un antivirus performant
- Installez un firewall adapté
- Adoptez la double authentification
- Contrôlez la validité de chaque lien
- Contrôlez chaque droit d'accès
- Réalisez des sauvegardes régulières
- Gérez strictement vos mots de passe
- Séparez le personnel du professionnel

2. Comment assurer sa mise en conformité avec les dernières préconisations gouvernementales de l'ANSSI ?

Adoptez les bons réflexes

Mieux vaut prévenir que guérir : cet adage s'applique également en matière de cybersécurité. Il vous est tout à fait possible de sécuriser votre environnement de travail en respectant des gestes simples, et en mettant en place les bons outils. Ces bons réflexes d'hygiène numérique vont de l'installation d'un antivirus performant à la mise en place de sauvegardes régulières en passant par l'instauration de la double authentification.

Menez une politique de sensibilisation

Pour que ces bons réflexes soient efficaces, il faut qu'ils soient partagés. Chaque professionnel de santé doit donc avoir connaissance des gestes à respecter et des outils à utiliser pour exercer son activité en toute sécurité. Ces bonnes pratiques doivent être régulièrement diffusées et mises à jour : de la formation initiale et de l'entrée au sein de l'établissement de santé jusqu'à la fin de l'activité de chaque collaborateur.

Réalisez des sauvegardes régulières

Une cyberattaque est presque toujours synonyme de données indisponibles. Lorsqu'il s'agit de données de santé, l'impossibilité d'accéder à ces informations sensibles peut représenter un risque majeur. C'est pour cette raison qu'il est important de réaliser des sauvegardes régulières de l'ensemble de vos fichiers afin de pouvoir les restaurer le cas échéant.

2. Comment assurer sa mise en conformité avec les dernières préconisations gouvernementales de l'ANSSI ?

Mettez en place un PRA

Le plan de reprise d'activité, ou PRA, vous permet d'assurer la poursuite de vos activités, même en mode dégradé, et ce lors d'une attaque majeure. Ce plan prend la forme d'un document reprenant l'ensemble des étapes à respecter pour la relance de votre système le plus rapidement et efficacement possible.

Mettez en place un PCA

Distinct du plan de reprise d'activité (PRA), le plan de continuité d'activité, ou PCA, est au cœur de la pérennité de tout établissement de santé. Celui-ci vise à identifier les menaces qui pèsent sur un établissement, ainsi que les impacts potentiels de ces menaces. Le PCA vient ainsi en réponse à un contexte de crise et prévoit des réponses appropriées à chaque situation pour assurer le maintien de l'activité en haute disponibilité.

3. Comment réagir en cas de cyberattaque pour protéger ses données de santé ?

Ne cédez pas à la panique et avertissez, de façon immédiate, votre responsable informatique ou le partenaire extérieur ayant en charge la gestion de votre cybersécurité et de vos infrastructures informatiques.

Ne paniquez pas

Déconnectez vos machines du réseau

Mettez en place votre PRA et/ou PCA

Contactez rapidement l'ARS

Déclarez l'accident au Ministère de la Santé

Ne payez jamais de rançon

Déposez une plainte officielle

Avertissez dans les 72h la CNIL

Réalisez un audit de votre infrastructure

Réalisez les actions correctives

Utilisez vos sauvegardes

4. Témoignage client :
IMANORD - Imagerie médiale - Hauts-de-France

En tant que Cadre de santé et référent métier j'étais à la recherche d'un prestataire informatique qui comprenne nos problématiques liées à la sécurisation et à la performance de notre infrastructure et de nos logiciels métiers. Notre problématique centrale, en tant qu'experts en imagerie médicale, est en effet de garantir le fonctionnement optimal de nos deux principaux logiciels métiers : le RIS *(Radiological information system)* qui nous permet de gérer l'ensemble de nos patients, de la prise de rendez-vous jusqu'à la facturation, ainsi que le PACS *(Picture archiving and communication system)* qui contrôle l'ensemble de l'imagerie médicale et gère les antériorités de nos patients.

Nous avons fait le choix de confier notre projet de mise en œuvre de l'infrastructure serveur à Blue Serve : leurs experts ont su répondre à tous les points clés et exigeants de notre cahier des charges afin de nous proposer une infrastructure informatique entièrement adaptée.

Cette confiance envers leurs experts informatiques est le fruit d'une longue collaboration. Nous leurs avons confié, dans un premier temps, la gestion de notre parc client, puis de nos serveurs applicatifs (identification, gestion des fichiers et des imprimantes), puis de nos serveurs métiers. En tant que prestataire informatique référent Blue Serve est le garant de l'optimisation et de la bonne tenue de notre réseau pour les échanges de données entre nos différentes applications métiers, qu'il s'agisse de respecter le standard d'échange DICOM, le HL7, etc.

Pour résumer, j'apprécie tout particulièrement la réactivité de leur hotline et leurs maintenances préventives sont un vrai plus pour nos établissements : nous avons aujourd'hui divisé par 3 le nombre d'interventions pour dépannage sur site.

Leurs services sont également suffisamment agiles pour suivre l'évolution constante d'IMANORD. En parallèle, leurs équipes sont également l'interface avec nos autres prestataires informatiques tels que Orange Business Security ou les différents éditeurs métiers (Fuji Healthcare, Siemens, etc). C'est un vrai gain de temps pour nous !

Nous avons donc trouvé un partenaire informatique compétent, capable de gérer nos serveurs, nos différentes modalités (IRM, scanner, radiographie) et assurer le bon lien entre nos machines, les ordinateurs de nos différents praticiens et nos serveurs, tout cela au service de nos patients !

David Ternoy
Cadre de santé

imanord
imagerie médicale

5. L'infogérance Blue Serve au service des cabinets de radiologie

Que peut apporter un prestataire d'infogérance unique pour la gestion de l'informatique au sein de mon cabinet de radiologie ?

Nos experts Blue Serve ont développé un contrat d'infogérance informatique vous permettant de disposer de prestations adaptées et sécurisées. Ce Contrat Sérénité vous permet d'avoir l'assurance que, chaque jour, votre cabinet de radiologie puisse accéder à ses outils informatiques essentiels au suivi de vos patients.

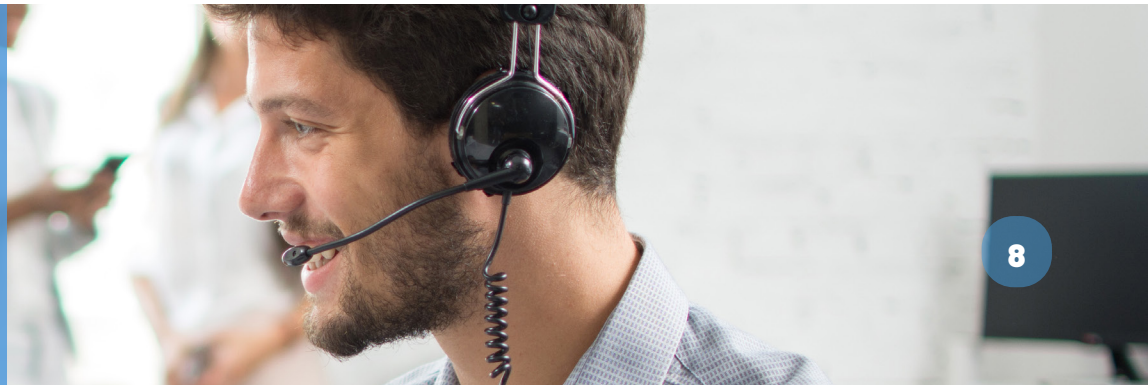
AUDIT
COMPLET SUR SITE

PRÉVENTION
MAINTENANCES RÉGULIÈRES

DÉPANNAGE RAPIDE
SUR SITE OU À DISTANCE

HOTLINE DÉDIÉE
A VOTRE ÉCOUTE

1 contrat d'infogérance pour tous les besoins informatiques de votre cabinet



6. Blue Serve : votre partenaire informatique de proximité

Grâce à une implantation géographique stratégique, qui s'est construite grâce à **l'ouverture de 3 agences à Lille, Lyon et Nantes,** nous sommes au plus proche de vous afin de vous accompagner tout au long de votre développement.

Dédié aux professionnels de santé

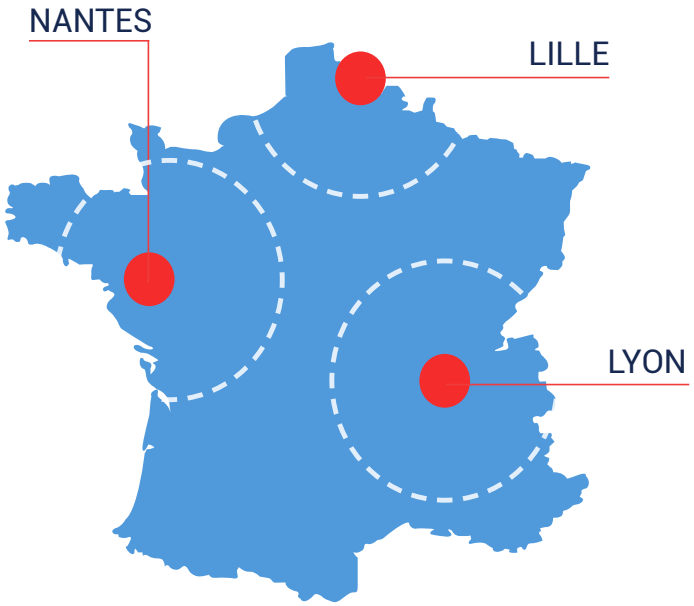
Audit et rédaction du dossier technique

Maintenances préventives et dépannages illimités

Budget annuel fixe et dimensionné selon vos besoins

Hotline dédiée à vos demandes de dépannage

+80% de clients satisfaits ou très satisfaits de leur contrat



Vous avez besoin d'informations sur notre contrat d'infogérance ?

Contactez-nous

Par mail à l'adresse **blueserve@proges.com**

Par téléphone au **03.20.64.63.63**

PROGESPLUS
Lille - Lyon - Nantes

Siège social :
2, Rue de la République
59780 - Willems