| ALERT | Healthcare Ransomware attacks increased 278% in five years | |

Protecting patients' private information is not only important but required by law. In the five-year period from 2018 to 2023, ransomware attacks increased 278%.

How does HIPAA require you to protect your patients' Protected Health Information (PHI)?

- **Encryption** – all data containing PHI must be encrypted – don't forget emails containing PHI.
- **Malware detection software** – systems containing PHI must be protected by up-to-date malware detection software.
- **Firewall** – your firewall must effectively track and filter potentially harmful traffic from the Internet to protect PHI.
- **Robust User authentication** – All HIPAA covered entities must determine the level of PHI access for each workforce member and limit access to only that information. In addition, each workforce member, including employees, interns, work-study students, and temporaries must sign a confidentiality agreement.

The effectiveness of the measures must be monitored. Check with your I.T. company or person to make sure they have implemented these basic measures and any additional device or media controls to guard against unwanted access to your patients' PHI..