Security Considerations

Security considerations involved in the use of OnePacs

All information transmitted to or utilized within the OnePacs system is protected by security measures that meet or exceed all standard requirements, including the requirements of the Health Insurance Portability and Accountability Act (HIPAA). This is true for the free version as well as for paid version of OnePacs.

In particular:

- OnePacs enters into a standard HIPAA Business Associate Agreement with all individuals, groups, and institutions sending studies to OnePacs.
- All data transmitted over the Internet to or from any aspect of the OnePacs system is always encrypted using an AES symmetric key encryption with secure socket layer (SSL) or transport layer security (TLS) key exchange.
- Studies transmitted to OnePacs are encrypted using the Advanced Encryption Standard (AES), the current national data encryption standard of the United States, with key exchange negotiated using transport layer security (TLS) with public key encryption.
- All web connections to the OnePacs Web Servers are encrypted using https: protocols. Study downloads using the OnePacs Study Retriever are also performed via HTTPS:
- The OnePacs storage devices and servers are protected by physical security measures that include keycard-protected access to the physical devices, such that unauthorized personnel can not physically access any of the equipment.
- A dedicated hardware firewall protects the array of OnePacs devices and is monitored 24/7 for evidence of intrusion attempts
- Data at the Web Server cluster is stored on a dedicated networked attached storage device which is behind the OnePacs hardware firewall, and which is dedicated exclusively to the OnePacs server cluster. All data is continuously mirrored to a backup storage device.
- The hosting facility and any other vendors doing business with OnePacs who may have a need to access protected health information (PHI) have signed Business Associate Agreements obligating them to appropriately protect confidential PHI.
- The OnePacs data center has the following certifications: SSAE16 Type II SOC1, SOC2, SOC3, Safe Harbor.
- All Protected Health Information will be systematically deleted from all OnePacs storage devices and all backup devices if any entity utilizing the OnePacs system decides to stop using OnePacs. This responsibility of OnePacs is embodied as a contractual obligation in our Application Service Provider agreement with all parties using OnePacs.
- Information about user account security is available on the Security Policies page.