Information Privacy and Security (IPS) at vRad

Virtual Radiologic (vRad) may only use or disclose protected health information (PHI) as allowed by the Privacy and Security Rules and by various state laws. The Privacy and Security Rules were implemented to carry out the goals of the Health Insurance Portability and Accountability Act (HIPAA) and recognize that "HIPAA compliance" is an end-state that requires training, mitigation and team member sanctions as appropriate for violation of the Privacy and Security Rules. The following provides background on ways vRad has implemented the Privacy and Security Rule requirements.

Management & Leadership

vRad's executive management provides clear and strong support of vRad's information privacy and security (IPS) activities. vRad's patient-first culture and executive leadership help ensure a successful IPS program. Shannon Werb, is the Security Officer, and Karen Scott, compliance director and assistant general counsel, is the Privacy Officer. Several compliance and security personnel also support the Security and Privacy Officers' compliance activities. Our Privacy Policy can be viewed at: https://www.vrad.com/privacy-policy/

Enterprise-wide Responsibilities

IPS responsibilities flow throughout the vRad organization. IPS training occurs at the time of hire, regularly throughout the year through privacy- and security-related briefings, and through additional, refresher training. IP&S is incorporated in informal and formal training for job tasks that deal with PHI. Workforce sanctions are imposed as appropriate for violations of IPS policies.

IPS Risk Assessment

vRad performs regular IP&S risk assessments, including gap analysis. Our risk assessments and plans for addressing gaps are re-addressed as needed as our technologies and processes change. Special Publications in the 800 series from the National Institute of Standards and Technology (NIST) and other publications have informed the risk analyses and paths vRad has chosen to protect PHI. These resources include, but are not limited to:

- 800-111, Guide to Storage Encryption Technologies for End User Devices
- 800-113, Guide to SSL VPNs and
- Department of Health and Human Services (HSS) Guidance on Portable Devices

IPS Policies & Processes

vRad has written IPS policies to address potential threats to PHI security, HIPAA, HITECH (Health Information Technology for Economic and Clinical Health Act) and other applicable legal requirements. vRad ensures all members of the workforce with access to PHI clear a background check at the time of hire, or if their role changes to one involving access to PHI, then prior to the role change. We make reasonable efforts to only use, disclose, and request the minimum PHI necessary to accomplish tasks on behalf of our affiliated covered entities, client facilities, and on behalf of Virtual Radiologic Professionals (VRP), the practice that may have patients in common with our client facilities. vRad has business associate subcontractor agreements with vendors that may have access to PHI, and vRad is a business associate to covered entities across the country, as well as to VRP.

Access, Authorization & Technical Controls

vRad maintains administrative and technical controls to support IP&S procedures. Controlling and validating a person's access to facilities, workstations, devices and systems is important. vRad is conscientious about physical and environmental controls in areas containing PHI, such as our data centers, which are based solely in the United States. Role-based systems access, strong password requirements, automatic log-off, encryption and termination procedures are examples of these controls.

Securing PHI

vRad makes every effort to comply with standards approved by HSS for encryption, data destruction and other methods of securing PHI. We have implemented security measures to guard against and detect malicious software. For example, our mobile devices, workstations and data transfers to a recipient outside of our network use NIST-approved encryption to protect PHI. We have a Breach Notice protocol in the event there is ever a suspected Breach of PHI, as Breach is defined by HITECH. Our data backup and disaster recovery plans provide for emergency mode operation and comply with the Security Rule's contingency plan requirements.

How does vRad technology keep patient data secure?

After a patient is scanned, the images are encrypted and transmitted from a PACS (picture archiving and communication system), scanning device, or gateway system via a secure VPN (virtual private network) tunnel to vRad PACS. The data is physically located in one or more US-based data centers. The facility's radiologic technologist logs into the secure, online RIS (radiology information system) using a user-specific log-in and strong password for order validation. vRad's software routes images and related data via a 256-bit SSL (secure sockets layer) connection to the radiologist's system. Reports may be transmitted by fax, via an HL7 interface, or downloaded through vRad's RIS. If a user needs a password reset, vRad makes reasonable attempts to validate the user's identity before issuing a new password.

Are VPNs safe?

Under the Security Rule, entities can choose which technologies make sense for their environment while being secure enough to prevent improper access. vRad uses a VPN technology that is FIPS 140-2 compliant, as recommended by NIST and used by the U.S. government. This VPN architecture allows unrelated sites that have a third party in common to encrypt all traffic between the sites. vRad uses SSL VPNs for securing centralized data accessed by remote authorized users.

How can vRad help my facility's compliance efforts? Because our image storage and other technologies are cloud based, the data is physically located in our secure, enterprise-class data centers, not locally. Therefore, clients using vRad technologies have fewer facility management duties around compliance. Workstation access, internal password management and other typical controls remain with you, but there are no servers for you to manage, no encryption software or malware detection costs, and vRad undertakes the burden of securing your PHI while it is on our systems, whether in motion or at rest.