TOP **HIPAA VIOLATION** ISSUES

Here are the eight most commonly reported HIPAA violations and how RDEE helps shield you against such threats.

Threat
Keeping Unsecured Records

In addition to being encrypted, Digital files on the RDEE network employs the most advanced user-authentication and access tracking available.

Threat
Lack of Employee Training

Employee HIPAA training is a requirement of the HIPAA law. RDEE features the most robust live, commercial and p2p, training content in the world- ensuring your staff remain fully trained and compliant.

Threat
Hacking

Hacking is a ubiquitous and formidable occupational hazard that threatens the healthcare industry's data integrity whether stored locally or via cloud, costing tens of millions of dollars yearly. RDEE's proprietary encrypted, decentralized ledger and network technology makes it "hack-proof".

Threat
Loss or Theft of Devices (Laptops/Phones/Tablets)

All hardware, computers and phones etc, are subject to the possibility of loss or theft. RDEE is completely hardware-free!

RDEE'S SECURITY AND HIPAA ADVANTAGES

Radiologex
Healthcare Happens Here™

Threat
Unencrypted Data

RDEE adds an additional and ESSENTIAL layer of security with state-of-the-art data encryption.

Threat
Sending PHI To wrong Contact

RDEE's patent-pending permissioned governance and private keys allow for specific send/receive requests, error-proof.

Threat
Unauthorized Release of Information

Sorry we can't fix humans yet to force honesty, but ALL unauthorized access attempts are detailed and immutably recorded on the RDEE blockchain.

Threat
Gossiping / Sharing PHI

Sorry we can't fix humans yet.