**Pick Your HIPAA Safeguards**

|  |  |  |
| --- | --- | --- |
| **Physical**  | **Technical**  | **Administrative** |
| Access controls, device and workstation security | Encryption at rest and in motion | Policies, auditing, and oversight |
| *Examples:*• Locks• Window bars• Roll-down shutters• Video surveillance cameras• Proximity cards• A locked drawer in a locked office with limited access controls • Locking portable devices in a safe when not in use• Steel doors | *Examples:*• Secure VPN access• Network storage for workforce usage• Encrypted USB portable flash drives• Encryption–wherever PHI can be stored and however it can be transmitted• Disabling or monitoring USB ports• Thin clients\* | *Examples:*• No cameras or phones in the workplace• Only purchasing department can buy USB drives (and only encrypted ones)• Incident response and reporting• Role-based access• Reporting of monitoring “up the chain” |

\*”Thin clients” are computers or computer terminals that connect to a server. They typically lack a hard drive, do not have peripherals or input/output ports, and cannot download or store information.

*Source*: Martha Ann Knutson, attorney, San Diego, Calif. Used with permission.