Apploi's Data Security Checklist for Healthcare

Saving sensitive information? Take a minute to ask yourself: Is this data...

- Saved on an encrypted platform?
  - Encryption scrambles data so only authorized viewers can view it. When storing sensitive information online, make sure you're using an encrypted platform. That way, if information is intercepted, it won't be readable.
- Backed up to another location?
  - Important information should be saved twice: once to a primary digital location, and once to another digital or physical location that is carefully locked away or encrypted. Make sure this secondary location is protected and inaccessible to unauthorized viewers.
- Accessible to the people who need it?
  - Add user permissions to the small team of people who actually need to access it. This might include HR, talent acquisition, or whoever is responsible for onboarding.
- Made private for surplus users?
  - Take another look at user permissions. Do these people really need to access this information? If their access isn't actually important, remove them. You can always add them later.
- Allowed to be saved?
  - Do you have explicit written permission to save this data? Check for authorization before saving any sensitive information. Keep this authorization in a safe place, along with other records.