BlockMRS Design

(A) = application layer

Any time you need to encrypt with a public key, it means create a new public-private key pair.

1. Update your own data

1. Create master record, or find existing master record and update
2. Encrypt file with public key
3. Store to IPFS
4. Get hash from IPFS
5. Sign hash with private key
6. Publish signed hash to blockchain alongside public key
7. (A) cache block id

2. Share data with doctor

1. Find latest master record *(A) hopefully cached*
2. Verify the record
3. Decrypt IPFS file
4. Copy desired information
5. Create a new public-private key pair
6. Encrypt with the new public key, the doctor's public key, and any other recipient's public keys
7. Store to IPFS and get hash
8. Publish signed hash to blockchain alongside your and any recipient's public keys.
9. (A) Send block ID to doctor

3. Doctor modifies patient data

1. (A) Requests data from patient
2. Find latest record that includes the patient's and doctor's public key
3. Verify record
4. Decrypt IPFS file
5. *Appointment occurs*
6. Make modifications to the patient's record
7. Encrypt file with patient's and doctor's public keys
8. Store to IPFS and get a hash
9. (A) Send hash to patient
10. (A) *Patient does (1), with the update being the diff of the master record and the doctors modifications.*