Solutions

Each answer shows the steps, then the **result**.

2.1

- authentication checks who the user is: e.g. a student logs in with a password
- authorization decides what they may do: e.g. a student can read but not change grades

2.2

- it checks each packet against rules, such as allowed addresses, ports and protocols
- it blocks traffic that breaks the rules, keeping out unwanted or harmful connections

2.3

- a second factor, such as a code on the user's phone, is also needed
- a stolen or guessed password alone is then not enough to log in

3.1 D

- only the matching private key decrypts

3.2 B

- signed by a trusted authority

3.3 B

- the data can be restored without paying

3.4

(a) Any two threats, each with a matching countermeasure, e.g.:

- phishing for staff passwords; MFA and staff training
- interception of records sent to home; encryption over a VPN or HTTPS
- malware or ransomware; anti-malware, updates and offline backups

(b)

- the data travels over the public internet, where it can be intercepted
- encrypted records cannot be read without the key, protecting patient privacy

(c)

- the same key encrypts and decrypts, so it must reach every staff member without being intercepted
- with asymmetric encryption, each person publishes a public key for encrypting
- only their private key, never sent, can decrypt; often used to send the symmetric key safely

(d)

- **authorization**: access rights or permissions per user role