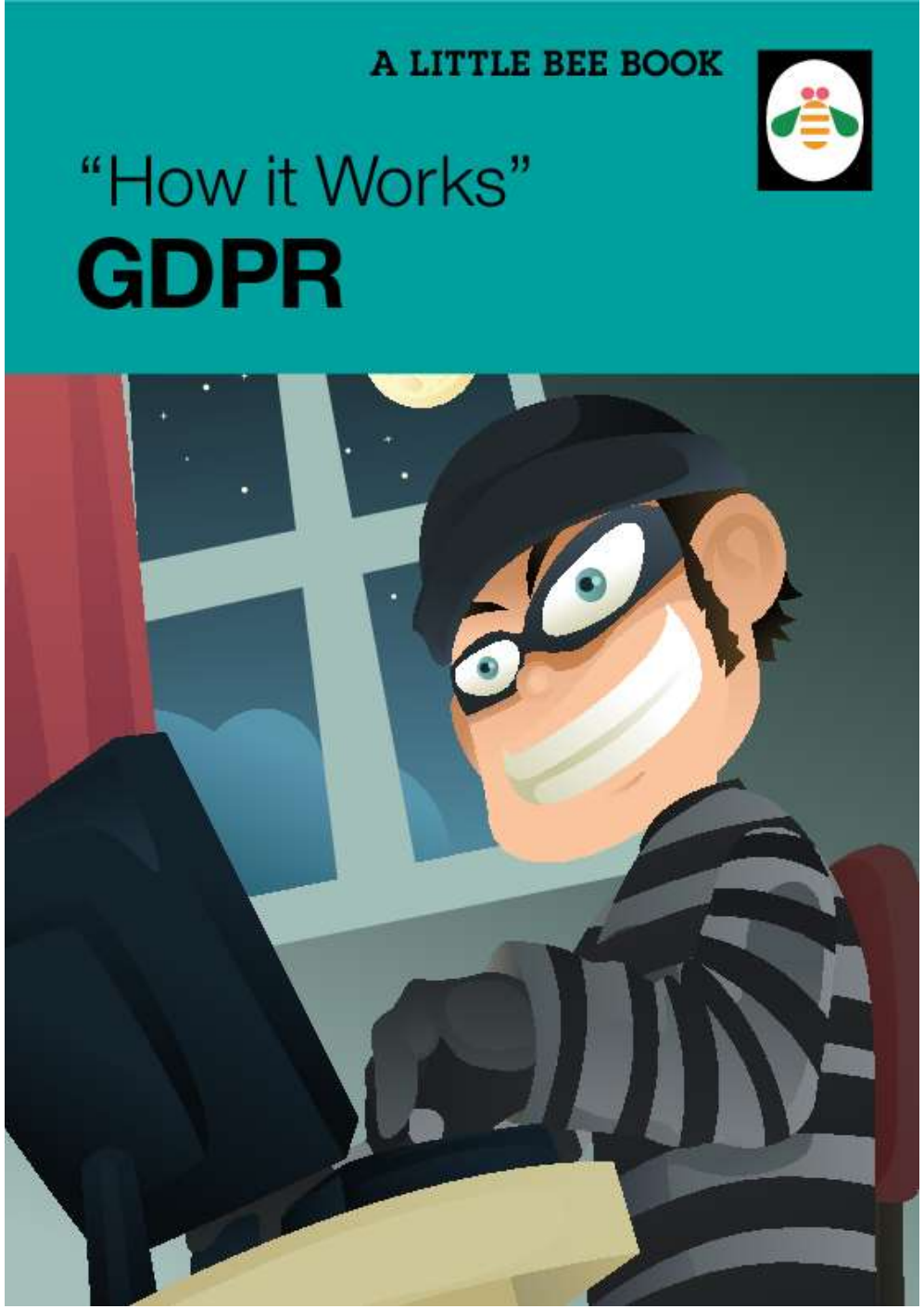


General Data Protection Regulation – EU

UK = ICO

25 May 2018

Compliance is not a choice

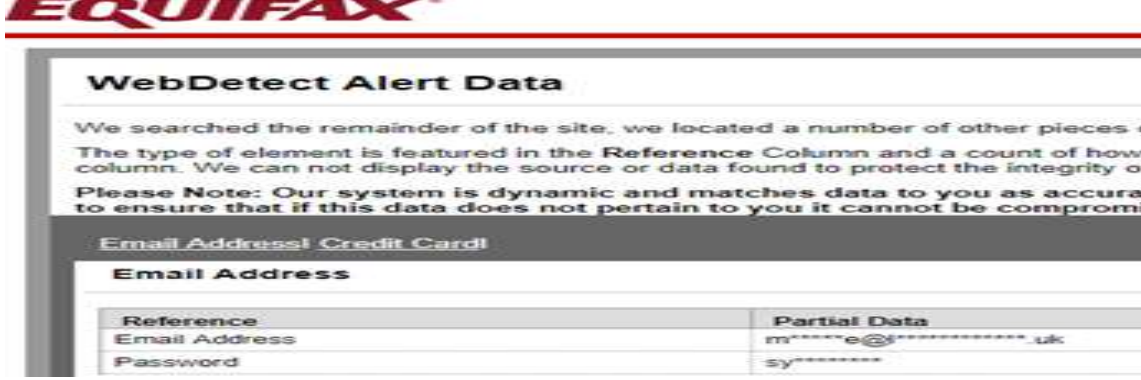
Time is short

Nicholas Lee

with thanks to IBM slideshare

The Problem

- Personal Experiences
  - Mobile Phones
  - Redirected Mail
  - Jessop Loan
  - Talk Talk Phone calls
  - Microsoft calls
  - Security checks
  - Blind copy emails to Nigeria
  - Email and correct password
    - 41 Trillion Year strength
  - Credit Card
    - Copied in Carpet Land
    - Use of stored Card



- 23% increase year on year
  - Fastest growing area of crime
- Ransonware
  - WannaCry, Petya
- Credit agency Equifax
  - 146 million records
  - 700,000 UK users
- The Dark Web PodCast
  - Cybercriminals – Teams
- Hospital
  - Ransonware, virus,
  - Unauthorised access
  - Loss of patient data
  - Theft of computers/laptops

After four years of debate, the General Data Protection Regulation (GDPR) was ratified by the European Union during April 2016 and has now become law, although member states have a two-year period to implement it into national law.

This means that companies will be expected to be fully compliant from **25 May 2018**. The regulation is intended to establish one single set of data protection rules across Europe.

Organisations outside the EU are subject to this regulation when they collect data concerning any EU citizen.

GDPR is designed to give individuals better control over their personal data held by organisations, and may lead many to appoint a Data Protection Officer.

Personal data is defined as any information relating to a person who can be identified directly or indirectly. This includes online identifiers, such as IP addresses and cookies, if they are capable of being linked back to the data subject.

Indirect information might include physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual.

There is no distinction between personal data about an individual in their private, public or work roles – all are covered by this regulation.

50% of global companies say they will struggle to meet the rules set out by Europe unless they make significant changes to how they operate.

There will be a substantial increase in fines for organisations that do not comply with this new regulation.

Penalties can be levied up to the greater of ten million euros or two per cent of global gross turnover for violations of record-keeping, security, breach notification and privacy impact assessment obligations.

These penalties are doubled to twenty million euros or four per cent of turnover for violations related to legal justification for processing, lack of consent, data subject rights and cross-border data transfers.

Companies will be required to “implement appropriate technical and organisational measures” in relation to the nature, scope, context and purposes of their handling and processing of personal data. Data protection safeguards must be designed into products and services from the earliest stages of development.

These safeguards must be appropriate to the degree of risk associated with the data held and might include:

- Pseudonymisation and/or encryption of personal data
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems
- Restoring the availability of, and access to, data in a timely manner following a physical or technical incident
- Introducing a process for regularly testing, assessing and evaluating the effectiveness of these systems.

A key part of the regulation requires consent to be given by the individual whose data is held. Consent means “any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed”.

Organisations will need to be able to show how and when consent was obtained. This consent does not need to be explicitly given, it can be implied by the person’s relationship with the company. However, the data obtained must be for specific, explicit and legitimate purposes.

Individuals must be able to withdraw consent at any time and have a right to be forgotten; if their data is no longer required for the reasons for which it was collected, it must be erased.

When companies obtain data from an individual, some of the areas that must be made clear are:

- The identity and contact details of the organisation
- The purpose of acquiring the data and how it will be used
- Whether the data will be transferred internationally
- The period for which the data will be stored
- The right to access, rectify or erase the data
- The right to withdraw consent at any time
- The right to lodge a complaint.

The regulations demand that individuals must have full access to information on how their data is processed and this information should be available in a clear and understandable way.

Individuals can make requests, and these must be executed “without undue delay and at the latest within one month of receipt of the request”.

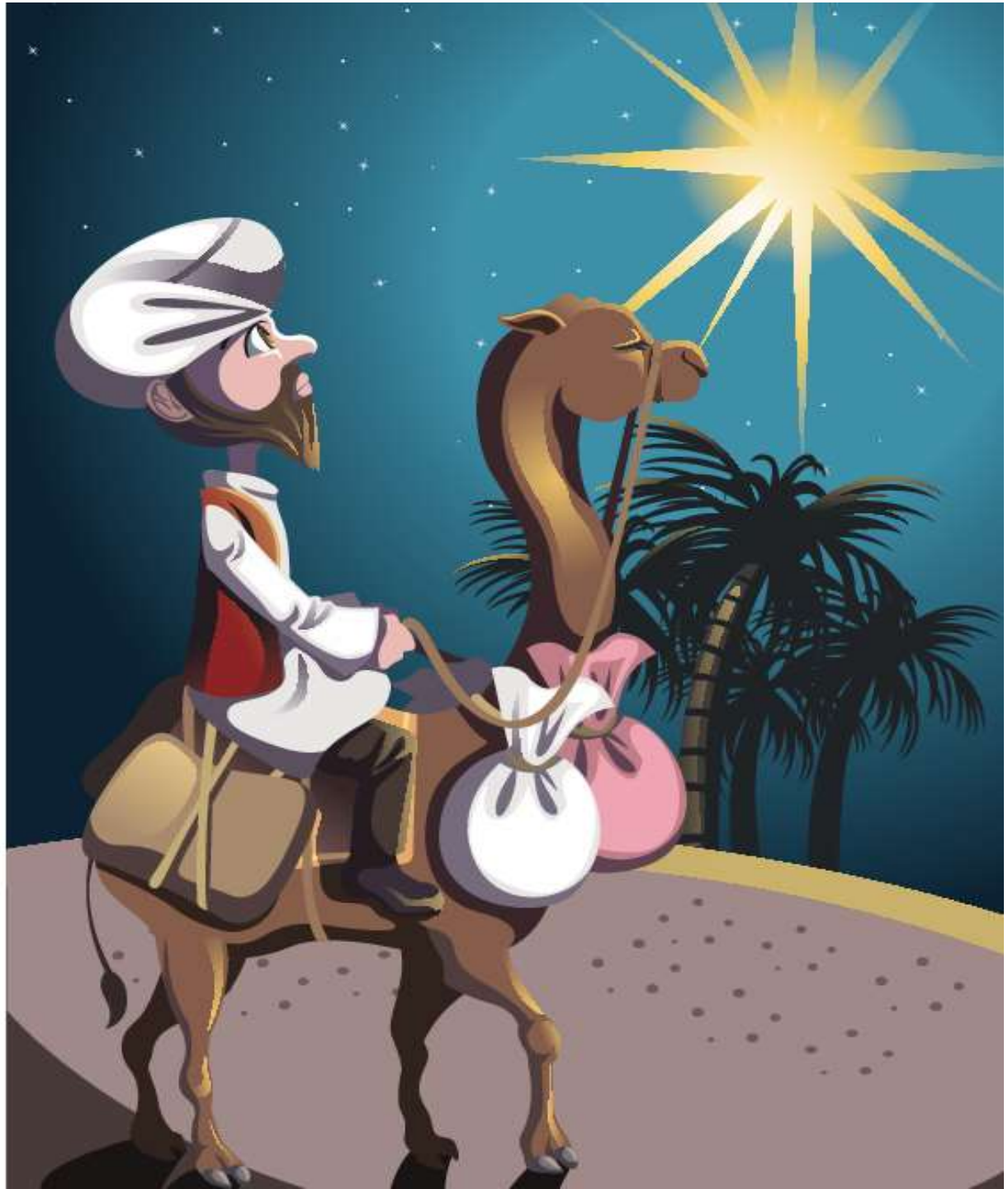
Where requests to access data are manifestly unfounded or excessive then small and medium-sized enterprises will be able to charge a fee for providing access.

Companies must report breaches of security "leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

In the event of a personal-data breach, companies must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it" if the breach is likely to "result in a risk for the rights and freedoms of individuals".

In March 2016, the UK Information Commissioner's Office (ICO) published *Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now*. Some of these steps for organisations are summarised next.

1. Ensure key departments are aware that the law is changing, and anticipate the impact of GDPR.
2. Document what personal data is held, where it came from and with whom it is shared.
3. Review current privacy notices, and make any necessary changes.
4. Review procedures to address the new rights that individuals will have.
5. Plan how to handle requests within the new time frames, and provide the required information.
6. Identify and document the legal basis for each type of data processing activity.
7. Review how consent is sought, obtained and recorded.
8. Make sure procedures are in place to detect, report and investigate data breaches.
9. Designate a Data Protection Officer to take responsibility for data protection compliance.

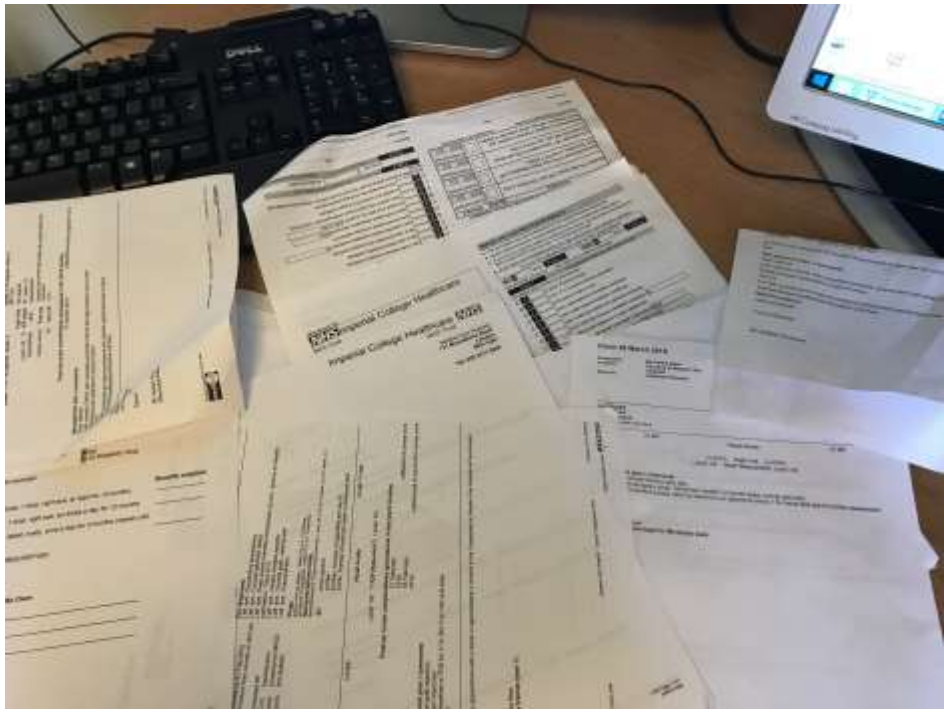


Passwords

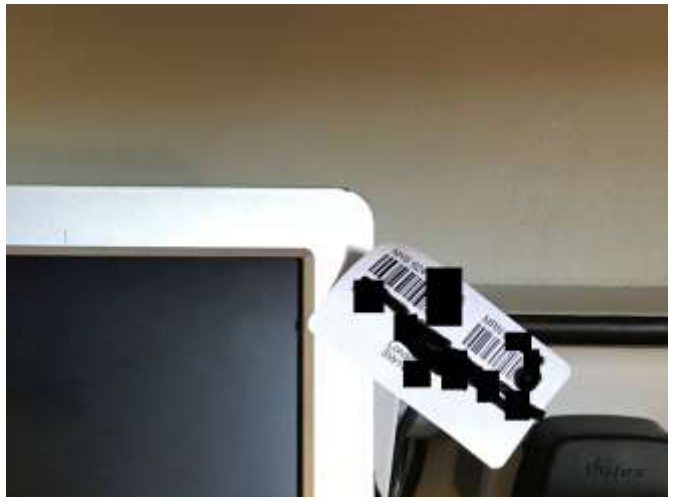
- Top 2017 of 5 million leaked
  - 123456, Password, 12345678, qwerty
  - 12345, 123456789, letmein, 1234567, football, iloveyou, admin, etc
- Problem is Adoption of Strong passwords
- NO agreement amongst Applications
- Long passwords – typo errors
- Unique for each site – Memory
- Frequent changing
- Secure passwords no better if they are stolen

- Unique Password for each Site/App
  - Password generator
  - https://howsecureismypassword.net/
- Unique User name for each site
- Double authentication
- Avoid simple passwords always
- Use a Password Manager across platforms
  - PC - Mobile phone - Tablet
- Use you phone to Store
  - Password Managers
  - In Phone book
    - Weak if hacker gains access.
- Backup
  - Retrieve via Email
  - Analogue back up – hand written- Secure in safe
  - Battlestar Galactica

What can you do?
Personal Data protection



- Data Theft, Phising, Scams, Phone calls is rife
- Be very Suspicious
  - Pause – Stop – No rush – Challenge all Calls
  - Sign up to Consumer credit reporting agencies and fraud prevention services
    - UK 3 main ones Experian, Callcredit (Noodle), Equifax
      - – add password to Credit checks
    - Cifas Protection Register
  - Secure passwords
  - Secure user names not nicklee@leemedical.co.uk but Customer1@yahoo.com
  - Encrypt your hard drive
    - Windows Professional includes Bitlocker for free – use it!
    - Vercrypt is new version of Truecrypt – free
  - Multiple secure back ups – Cloud storage
- We all have responsibility to protect data
  - If you see this – Confidential bin



Lock it or Loose it!

Main things for us is to

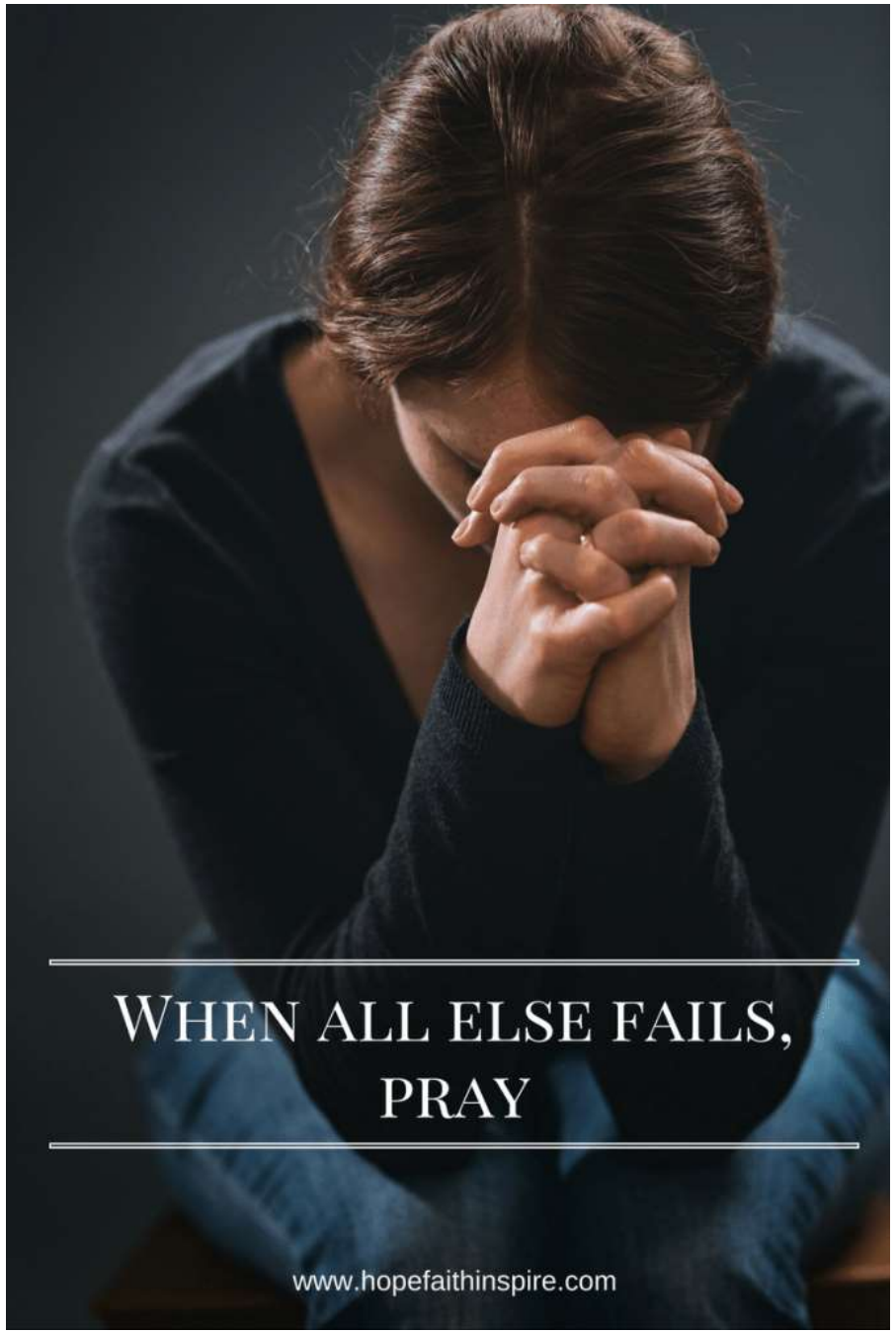
- ensure all patient data is secure and backuped off site (need to document where)
- your software is secure
- your secretary asks each patient for permission to hold their details and explains why they are holding each bit eg name and address so can communicate with them - need to document they have verbally agreed and then also follow up with paper work for them to sign which explains about the act, why you hold info and their details also if they want any reports to be sent to other professionals to name
- any old patients you are ok with but it is new ones and any follow ups - need to ensure their details are correct
- under GDPR they have right to see what you hold on them and to have details removed - right to be forgotten only with health this does not apply but you have to state how long you will hold info for and how you will remove /dispose it
- ensure all info sent to hospitals is secure - safe haven for faxes ,letters sent with private and confidential and any emails encrypted
- need contracts with any place you send patient data to eg bishopswood to ensure they look after and secure your patient data as you are responsible for it
- any medical equipment that you put any patient details on including name that you ensure it is kept safe and secure and encrpted where possible (for all equipment including pcs you need to do a Data Protection and Privacy Impact Assessment (eg attached)

also need to have policies which we bought from simple-docs

they are on the business section and if search GDPR they should come up but you do need to pay £35
https://simply-docs.co.uk/Home
we used the employee data protection policy, data protection policy and data processing agreement for hospitals, accountants, our software, medisoft etc

some other useful sites i read
https://www.whitepapers.em360tech.com/wp-content/uploads/GDPR-Implications-of-the-GDPR-in-Healthcare-042717-d1.pdf
https://www.ipexpoeurope.com/content/download/10060/143925/file/Egress%20white%20paper%20-%20Healthcare%20and%20the%20EU%20GDPR.pdf

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance
https://ico.org.uk/for-organisations/health/
http://www.rlb-law.com/briefings/healthcare/gdpr-lawful-grounds-processing-data/



Thanks to IBM Slide Share
Michele – Data Controller

https://www.itgovernance.co.uk/

GPDR Toolkit, documents

ICO Blog
https://iconewsblog.org.uk/