Governance and Compliance

Learning from the Private Sector

David Coverdale

egton

Governance Challenges

egton

Biggest risks

- Cyber risk – ransomware
- System breaches
- GDPR failings on Policy
- Loss of data
- Data requests

egton

General Data Protection Regulation (GDPR)

High Level requirements

- Only retain the minimum of personal information
- Only use for purpose intended
- Deletion of records – individual in control
- Policy, Procedure and Process

- Not identify the individual
  - Date of birth
  - Address
  - Roles of one or two people
  - National Insurance numbers

egton

IG Requirements

- **Information Governance Management**

- Establishing personal responsibility for ongoing IG compliance by named individuals.
- Creating and maintaining a coherent, actionable policy for IG management.
- Ensuring all staff contracts are written to clearly indicate IG responsibilities
- Ensuring relevant, up-to-date staff training and education for IG requirements.

- **The challenges here are not all that taxing if you routinely invest in training, and already have data governance and intellectual property protections baked into your contracts.**

egton

IG Requirements

- **Confidentiality and Data Protection**

- Strict adherence to the Data Protection Act (DPA), particularly in relation to obtaining consent from individuals before using or sharing their data.
- Ensuring that patient identifiable data continues to be treated under DPA and UK Department of Health rules even if the data is processed outside of the UK.
- Ensuring all access to confidential data is continuously monitored and audited.
- Developing and implementing any new processes, services, information systems, or other relevant information assets in a secure and structured manner.
- Ensuring all data transfers are secure and confidential.
- **Perhaps the biggest challenge for organisations here is ensuring they innovate in line with IG compliance.** This necessitates having fit-for-purpose policies in place for the development process to follow from initial scoping all the way to infrastructure management.

egton

IG Requirements

- Software solutions IG compliant – applies to in house.
- Information Security
- Maintaining a comprehensive information asset register.
- Creating and maintaining effective information security policy and procedures governing all ICT networks.
- Include mobile computing and teleworking provisions.
- Ensuring physical security measures are in place to guard against unauthorised access to data.
- Ensuring appropriate access control to operating systems and information assets, with managed access rights for all applicable users.
- Ensuring plans and procedures for successful business continuity in the event of power failure, system crash or any other disruption.
- Maintaining documented incident management reporting processes.

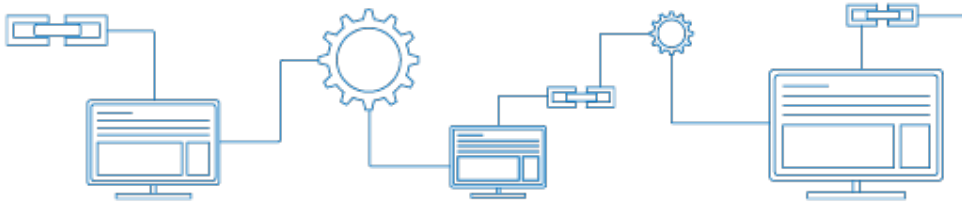
egton

GDPR - why it matters

- May 25th 2018
- €20M fines
- Global implications
- Will definitely remain post Brexit
- USA, RoY and Private sector have plans in place

egton

Rationale



- Individual is at the centre of compliance
- The centre of data protection
- Affects staff and patients
- All supplier products must comply
- All databases must comply

- **Consider how to achieve this with paper?**

egton

Unrequired data

- Basic identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

egton

What might a program look like?

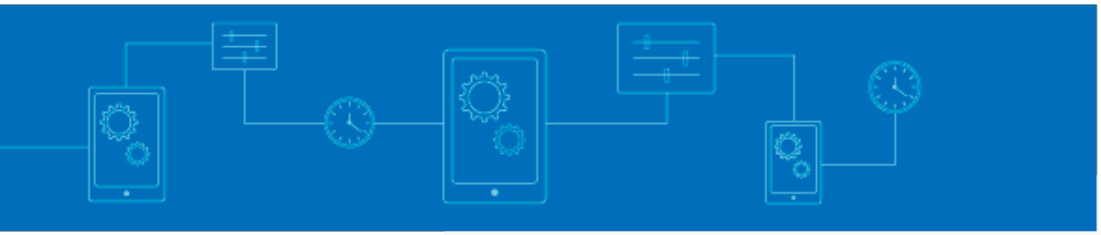
- Create awareness, knowledge and know the impacts.
- Document the personal data held.
- Check/change privacy notices.
- Can you manage/delete personal data in all formats?
- Set up procedures to handle new data access requests.
- Know the lawful basis for procuring data.
- Have clear process to seek, record, manage consents.
- Have a procedure to detect, report, investigate data breach.
- Understand the ICO code of practice.
- Implement Article 29.
- Assign data protection officers – a key role.
- Establish a data risk register – know your environment.

egton

Why do this?

- NMC midwife lost 3 x DVDs
- £150k fine and personal cost of £850
- Criminal record

egton

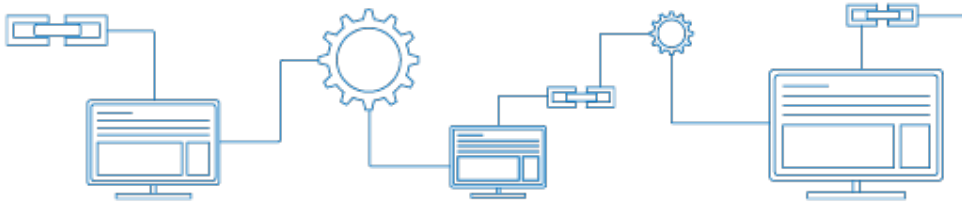


More reasons

- May not be covered by Cyber insurance
- Fines have increase 79 times from ICO in 3 yrs.
- GOSH £11,000
- Flybe £70,000
- Pharmacy2U £130,000
- GM Police £150,000
- Basildon Council £150,000
- CPS £200,000
- Talk Talk £500,000

egton

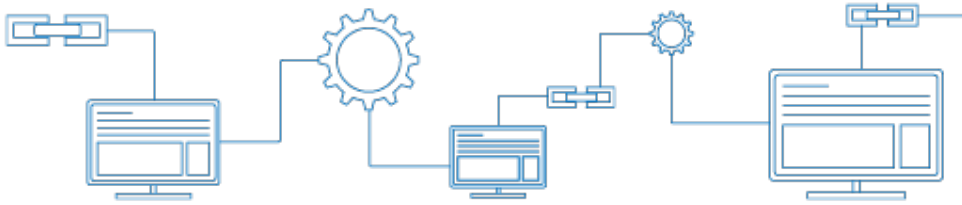
Egton program



- All products checked, updated and versioned.
- Register of risks to GDPR at board level.
- Funding allocated to implement mitigations.
- Bi-weekly report to executive.
- Individual must give explicit consent.
- Implied consent unlikely to survive.
- New granular level of consent in place.

egton

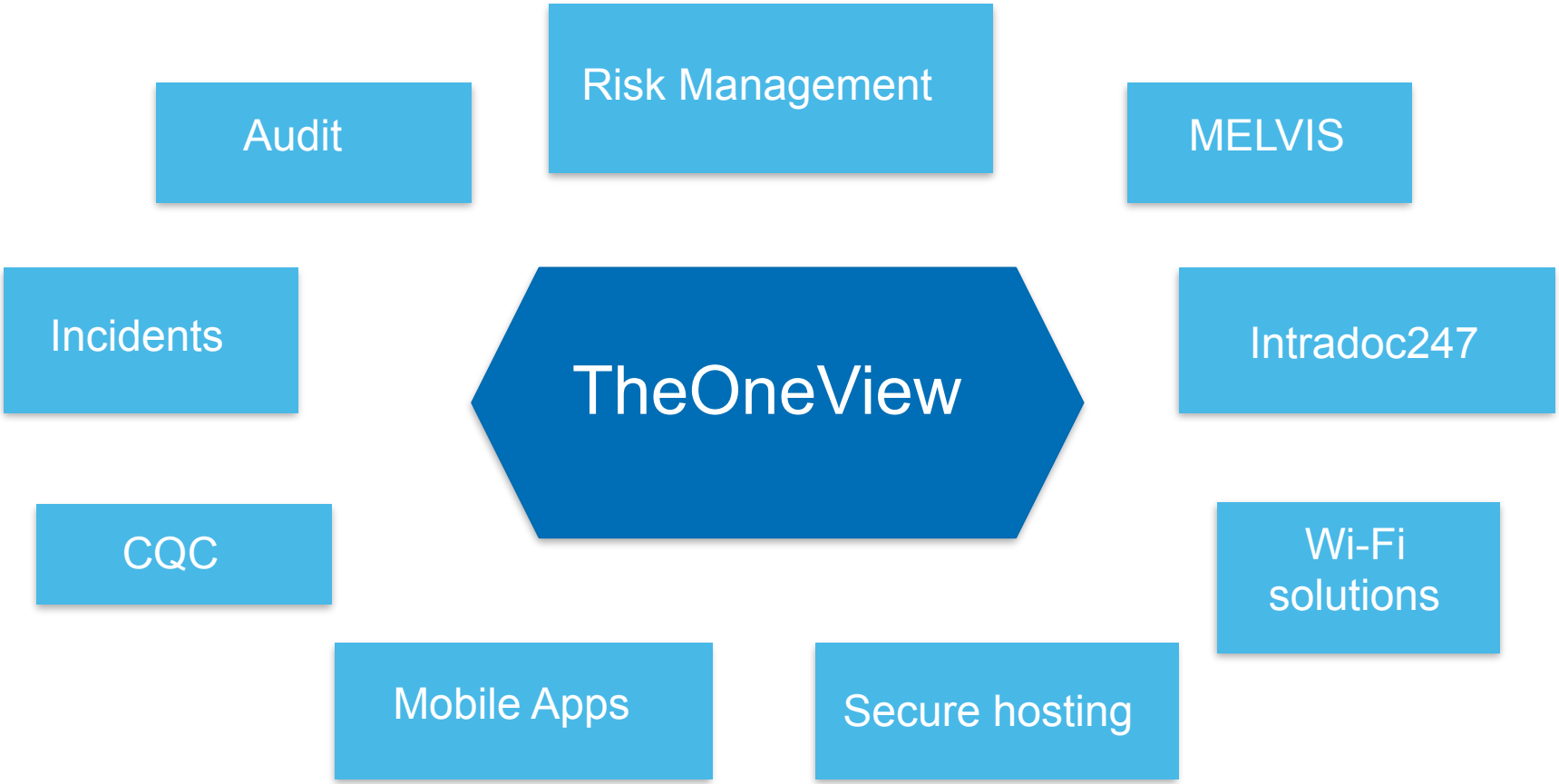
Commercial Learnings



- Be prepared - invest in knowledge and training.
- Validate all databases and systems.
- Validate non-systems based data.
- Develop an early framework.
- Consider governance technology platform.
- Consider mobile device capabilities.
- Go Digital.

egton

Egton Compliant Solutions



Summary

- Identify information and process owners
- Consider the impact of data breach
- Develop a framework for compliance
- Develop a plan to achieve compliance
- Consider all data and software used
- Consider platforms to enable monitoring
- Put the individual at the heart of data

egton

Thank you

David Coverdale

egton


DON'T
PANIC