Spirit in mind

Registered Charity
No. 1055931-14

NHS
South West
Yorkshire Partnership
NHS Foundation Trust

What is GDPR?

* General Data Protection Regulation
* data protection law rebooted
* arrived 2016, enforced from 25 May 2018

What's it all about

* protecting people from each other
* by governing the use of personal data
* harmonising law across the EU

Spirit in mind

Registered Charity
No. 1055931-14

NHS
South West
Yorkshire Partnership
NHS Foundation Trust

What does it say

* fairness, lawfulness, transparency
* know what data, why, how, where
* consider impact to the individual

Principles based

* No instruction manual
* Not checklist
* Decisions needed

Registered Charity No. 1055931-14

NHS South West Yorkshire Partnership NHS Foundation Trust

* Strategic
* Ownership

Myths

* Consent must be informed, freely-given, specific
* Data Protection = Security - X
  * Fairness, rights, quality
* All about Comms - X
  * Don’t forget the background stuff
  * Just update Paperwork
  * Paperwork must match reality

Spirit in mind

Registered Charity No. 1055931-14

NHS South West Yorkshire Partnership NHS Foundation Trust

- Just buy a tool - X
  - Process culture AND systems
- Data "ownership" - X
  - Rights & obligations

What does GDPR mean for Comms?

- not much, if compliant with DPA & PECR
- and able to provide evidence
- and managing information carefully

Registered Charity No. 1055931-14

PECR (Prior Explicit Consent Required)

* for electronic marketing to individuals
* by email, phone, SMS, in-app message
* requires explicit prior consent

ePR

* consent for social media/in-app marketing
* consent for 3rd party cookies (browser)
* consent for digital fingerprinting, tracking

Registered Charity
No. 1055931-14

South West Yorkshire Partnership NHS Foundation Trust

GDPR + PECR =

* consent: higher standard
* evidence – what, how, when
* not to be confused with privacy info

Where to start

how to eat an elephant

....one bite at a time!

ID purposes of data use

* look at organisation's objectives/mission
* what do you do, and why?

* start with business process, not data

ID processing operations

* how does your organisation do its thing?
* where does data come from, go to?
* what do you do with it and how?

Lawful Basis

* probably legitimate interests or consent
* neither is “easier” or “simpler”

* data and rights must still be managed

Consent 1

* informed, freely-given, specific
* “no” means no (=no Plan B)
* doesn’t last forever (but can be renewed)

Consent 2

* ‘insert a tickbox’ is not enough
* explain processing and purpose(s)

Registered Charity
No. 1055931-14

South West Yorkshire Partnership NHS Foundation Trust

* consider whole ecosystem

Legitimate Interests

* assessment required – what interests?
* balance against rights, freedoms, risks
* provide or publish the assessment

Spirit in mind

Registered Charity
No. 1055931-14

NHS
South West
Yorkshire Partnership
NHS Foundation Trust

Social Media

* who has control of the data processing?
* 'in public' is still "personal data"
* record-keeping and risk management!

Privacy Information

* much more info required than for DPA
* must be clear, accessible, specific
* one-size fits none - you'll need several

Spirit in mind

Registered Charity
No. 1055931-14

NHS
South West
Yorkshire Partnership
NHS Foundation Trust

Do and Don't's Tip 1

Don't start rewriting privacy notices until you have mapped out purposes, processing operations and legal basis

Dos and Don'ts Tip 2

look very hard at your supply chain – contracts and assurance; are they going to drop you in it?

Dos and Don'ts Tip 3

Refresh/verify consent where needed, purge unsuppressed but unengaged contacts, consolidate suppression lists

Registered Charity
No. 1055931-14

Dos and Don’ts Tip 4

GDPR is not just about marketing – engage with wider organisation’s data protection programme

Azizur.rehman@swyt.nhs.uk

May 2018