Cleartext Systems

Data Security

How to avoid getting fined for a breach of the GDPR…

ISO 9001:2015

Crown Commercial Service Supplier

The CIA principle: Confidentiality, Integrity and Availability

IT systems that help

- Data encryption technology
  - Symmetric encryption, asymmetric encryption
- Secure email and file sharing solutions
  - Egress Switch, OpenPGP (Gnu Privacy Guard), PGP (Symantec)
- Data classification
  - janusSEAL protective marking,
  - Expiration dates, ‘no eyes required’ archive purging
- Secure by design
  - No plain text, data versioning and expiry
  - Password strength, non re-use & expiry dates
  - Tested backups and business continuity systems

Confidentiality, Integrity : The goal is to keep your data secure, and stored safely and within the correct jurisdiction

Is your customer data secure?

- How does encryption work….

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
s	z	a	g	b	l	r	c	j	n	q	d	h	w	x	v	e	p	u	k	m	t	f	i	y	o

- Substitution cipher example

c	s	w	g	y		f	j	v	b	u		s	p	b		r	p	b	s	k					

- This one is easily broken, why?

Processes and procedures that help

- Enforce policy based access control
  - Staff vetting, ensure correct access levels, don’t forget to revoke
  - Demand password protected lock screens with password specs
- Regular system and software patching and updates
  - Don’t run old software, the NHS saw the consequences
- Periodic policy based planned data archiving and purging of old data
- Periodic assessment of data location and number of copies
- Staff training on data protection and data security
- Regular ‘fire alarms’ to test loss of access to data and systems readiness
  - Do business continuity systems work
  - Can you and tour staff still work!

Availability: Who has access and when, and can they access it when they need to

Cleartext Systems

Questions?

ISO 9001:2015

Crown Commercial Service Supplier

Passworded file sharing is not a solution in all cases as you give ‘availability’ to the man in the middle, the bad gut