Current legal issues in data and the protection market
Select74 9th October 2014

Steven Rhodes

Lawyer and Legal Consultant

Running Order

- **1. Data Protection Regulation on its way**
- **2. Big Data**
- **3. Care Data**
- **4. SARS GPRs**
- **5. Wet signatures**
- **6. Genetics**
- NB – High level of detail not possible here. Also, little case law in the UK because of FOS, so much guidance here is educated guesswork. **As always: make sure you rely only on legal advice from a lawyer who knows your own particular circumstances!**

Data Protection Regulation

Commission Regulation (EU) No 611/2013 of 24 June 2013 **on the measures applicable to the notification of personal data breaches** under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications [my emphasis]

- Concerned with the notification regime – but also with standards to protect against Cyber Crime
- I will deal with *highlights only* – Recital numbers are 'draft'
- Some things may be added in final document – but nothing will be taken away from the following.
- NB: *To be read in conjunction with draft General Data Protection Regulation 2012/0011 (COD) and other forthcoming data protection legislation*

Draft Article 1

- Applies to “providers of publicly available electronic communications services” This should include PCWs and direct sales websites.
- Check with your own lawyer to determine the status of your various business operations

Draft Article 2

- 2.1 “The provider shall notify all personal data breaches to the competent national authority.” [Information Commissioner’s Office – ICO]
- 2.2 within 24 hours and ‘where feasible’ with the Annex I data

Annex 1. Section1 Information

- Section 1
- 1. Name of the provider
- 2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
- 3. Whether it concerns a first or second notification
- *Initial information on the personal data breach (for completion in later notifications, where applicable)*
- 4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident
- 5. Circumstances of the personal data breach (e.g. loss, theft, copying)
- 6. Nature and content of the personal data concerned
- 7. Technical and organisational measures applied (or to be applied) by the provider to the affected personal data
- 8. Relevant use of other providers (where applicable)

Annex 1. Section2 Information

- Section 2 *Further information on the personal data breach*
- 9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):
- 10. Number of subscribers or individuals concerned
- 11. Potential consequences and potential adverse effects on subscribers or individuals
- 12. Technical and organisational measures taken by the provider to mitigate potential adverse effects
- *Possible additional notification to subscribers or individuals*
- 13. Content of notification
- 14. Means of communication used
- 15. Number of subscribers or individuals notified
- *Possible cross-border issues*
- 16. Personal data breach involving subscribers or individuals in other Member States
- 17. Notification of other competent national authorities
- OJ 2013 L173/82013 · Official Journal of the European Union · L173/8

Draft Article 3

- “When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual” (3.1) then Individual should be notified (3.2)
- “likely to adversely affect the personal data or privacy” takes into account: The nature of the data (3.2a) the Likely Consequences (3.2b) and the circumstances of the breach: ‘Was it theft?’ etc (3.2c)

Recital 6

- This notes that ALL data protection breaches should be notified to the IC but that the ICO will have discretion to identify which ones are serious.
- Therefore : look for forthcoming guidance from the ICO as to what level of breach they consider serious

Article 3

3.3 Notifications must be made ‘Without undue delay’

You should not delay notification to the client because you are waiting to hear back from the ICO, etc and you should include in the information in Annex II. Using plain English with no advertising, etc.

But! Article 4

- If you have encrypted your data or ‘hashed’ it you do not need to notify your clients of the data protection breach(although you still have to notify the ICO)
- But note Recital 17 “Implementing encryption or hashing should not be considered sufficient by itself to allow providers to claim more broadly they have fulfilled the general security obligation set out in Article 17 of Directive 95/46/EC. In this regard, providers should also implement adequate organisational and technical measures to prevent, detect and block personal data breaches.”

What does this mean for underwriters?

- Article 2 increases the reputational risk of
- A) Individual insurers, and
- B) The L&H sector generally
- In looking at relations with other bodies (DoH, BMA, ICO, etc) the insurance industry is less likely to get clearance for use of data/SARs etc. if it is the subject of repeated DP breaches/scandals

What other measures

- Recital 17 talks of “organisational and technical measures to prevent, detect and block personal data breaches” being needed in addition to encryption, etc. *This is not a new requirement – but it is emphasised in the recitals.* It marks cyber-attack as an increased risk.
- You must also ensure that you are looking at these risks properly and that you have a plan to deal with them.

A starter plan for ‘additional measures’

- 1 Understand your risks
- 2. Minimise them with basic procedures to retain data safely and stop unauthorised access
- Keep an eye on the threats out there
- Increase awareness in your workforce
- Make sure your governance is up to date, and
- Be prepared for breaches with a plan

Understand your risks

- For underwriters
- Make sure your own office is secure. E.g.:
  1.passwords to PCs handling medical data,
  2. USB ports
  3. Are your cupboards locked at he end of the day?

Consult: “Cyber Essentials” Issued by Dept for Business Innovation and Skills and match with 1. Guidance from FCA and 2. ICO regulation

Risks for Underwriters, (continued)

- These regulations mean this cannot be left to the IT department, because IT can't rate DP risks the way that underwriters can. So the 'organisational and technical measures' must be informed by you.
- Is your risk register up to date, and do you (the U/W) have input to it? Make sure 'Cyber-attack' is listed there and any additional risks on your data profile.

Big Data

- Directed to article by Hank George ‘Something “wicked” this way comes?’ December 2008
- He discusses ‘lifestyle based analytics’: “It would seem that this high-minded phrase relates to the deployment of financial transaction records such as purchases with credit cards and possibly in other ways as well – which can be grabbed from cyberspace in what I like to think of as mankind’s “Post-Privacy Era.”

Big Data Examples from Hank George

- Purchase of no exercise equipment but many books
- Dietary preferences
- Purchases of packets (cartons? –SR) of cigarettes
- Broccoli (good) Hot sauce (neutral) Mars Bars (bad!)

Hank George's Four tests

- Does it confer sufficient independent protective value?
- Is it affordable?
- Can it be done within the constraints imposed by our unique milieu?
- How will it be perceived by parties to the transaction?

Hank George's conclusion

- It is risky enough for underwriters to draw inferences from medical data e.g. the use of CEA (carcinoembryonic antigen) as a tumour marker when that test is not (then) clinically licenced. The use of inferential data should be treated with great suspicion.

The UK Position

- No DPA or equivalent in the US
- No Equalities Act in the US in the same way as UK because no Human Rights Act. US Federal rights law based on Constitution, other legislation/cases (e.g. anti-redlining laws) happen at state level
- Key further safeguards in the UK

SR proposed test

- Assume broad and valid consent to data gathering granted.
- But note 3rd DP Principle “Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which hey are processed”

Is it truly useful?

- Is the Big Data yield:
- 1 specific and accurate
- 2. capable of being reduced to a robustly defensible rating based on published data and best available medical research, etc.
- 3. telling you something that you should have got from the proposal form, etc.

Is it truly useful?

- If you cannot satisfy the truly useful test (as Hank George is suggesting) then inferential data gathering will fail under:
- Principle 3 DPA.
- Equalities act (if relating to a category of person falling under that Act).
- Possible claim under Human Rights Act right to privacy and family life: how can you consent to people holding untrue or speculative data about you?

If it is useful, should you have it?

- Encyclopaedia of Data Protection (Jay, et al) at 2-266/5:

Summary: once you process data to look for fraud, for example, the processes you use and the conclusions you draw then become new data; data which you should then disclose to the data subject.

Be clear in your proposal form – but even that may not be enough

- Contracts must allow specifically for inferential data to be gathered. But:
- 1. Are you complying with Principle 3?
- Is this ‘underwriting after the event’?
- Is this restricted to fraud ‘at the time of the proposal form’? If not, are you complying with s5 Consumer Insurance (Disclosure and Representations) Act 2012?

In Summary

The same principles apply to Big Data as to any other data

or

It really doesn't matter how big it is; it's what you do with it that counts.

SARS –v- GPRs

- Subject Access Requests (SARs) originally used as means for data subjects to check the data being held on them s.7 DPA 1998
- Now routinely used by some insurers instead of GPRs
- This has been queried by, amongst others, doctors/BMA. They have some points

Dr Paul Cundy

- Joint Chairman of the BMA and RCGP joint IT Committee. News item:
- “ICO to examine insurers use of GP Info”
- http://www.ehi.co.uk/news/EHI/9553/ico-to-examine-insurers
- Forms a useful summary of the issues

Dr Paul Cundy Article

- Aviva asked for copies of all the patient's medical records, excluding negative results for STIs "unless they have long-term health implications". Aviva would disregard any information not related to the application "unless the information will help us to make a more favourable decision".

Dr Paul Cundy Article

- Dr Cundy said he is concerned that insurance companies' use of SARs breaches the third principle of the Data Protection Act, which states that "personal data shall be adequate, relevant and not excessive in relation to the purpose…for which they are processed."
- "In the letter, they admit to receiving information that goes beyond their purpose, so they're breaking the law."

Response to Principle 3 Point

- SAR is not a request made by the insurer. It is a request made by the data subject who may then disclose that information to the insurer.
- However, the request to edit the SAR indicates its potential use. This must be covered by any relevant consent on the proposal form.
- Providing the use is “adequate, relevant and not excessive” this should not be a 3rd DP Principle breach

Dr Paul Cundy Article

- “An SAR is not designed for insurance purposes: the law is very clear that disclosure for insurance purposes needs to happen under a significantly different set of guidelines.”
- He added that patients cannot rely on assurances that the additional data obtained will not be used by the insurance company.

Response to Purpose of SARs Point

- The law is not clear that disclosure for insurance *must* happen under different guidelines. It is true that SARs were not designed for insurance. But the data subject has a right to a SAR and also to use of the data found in a SAR.
- An assurance not to use additional data obtained would certainly be binding on an insurer. [SR]

Dr Paul Cundy Article

- “I’m concerned that patients don’t fully understand what’s happening when they fill in this form.”
- An ICO spokesman told EHI it is “making enquiries” into how insurance companies are using SARs and whether their use fits with the Data Protection Act.

Response to Patient Awareness point

- This point is perfectly fair and pertinent. A patient's rights under s.7 are different from their consumer rights to obtain insurance at a good price.
- ICO yet to report on SARs. SR's guess is that informed consent is key:

Informed Consent and SARs

- SR's crystal ball gazing on SARs:
- 1. Data subject will not be obliged to send SAR to insurer
- 2. Insurer must undertake to destroy SAR at request of data subject, but may retain 'relevant info' (subject to Article 7(3) forthcoming General Data Protection Regulation)
- 3. Data subject may request a GPR, but be notified that this may cost more
- 4. 'Lower premium only' will become a standard term

Wet signatures

- Has been going on a very long time!
- Electronic signature can now be valid to bind a party at common law: *Golden Ocean Group Ltd v Salgaocar Mining Industries Pvt Ltd* [2012] 1 W.L.R. 3674 (Court of Appeal)
- A guarantee was created by emails which were *authenticated* by e-signature. The emails asked for a document to be prepared with guarantee terms. It was not prepared, but the Court said the email terms were sufficient to create a guarantee. Important point from Statute of Frauds of 1677.

Wet signatures

- EU legislative framework (the Directive on a Framework for Electronic Signatures (99/93/EC)) incorporated as Electronic Communications Act 2000 (ECA) and the Electronic Signatures Regulations 2002 (SI 2002/318)
- These allow e-signatures to be good *evidence* of authenticity. But they do not make them as binding as wet signatures.

Your reporter Nicky Bray

- Nicky reports from the front line that current negotiations with BMA have indicated that BMA understands that e-signatures are ‘the direction of travel’ the question therefore is how to make them secure.
- NB DPA allows for e-signatures but AMRA does not make provision for them. So the industry will have to come up with something to keep the doctors happy.

Care Data

- Use of NHS data (anonymised or pseudonymised) Currently political as much as legal issue.
- Use of personal ‘named’ data illegal under Data Protection Act, 2007/8 Statistics Acts, Human Rights Act and 2014 Health and Social Care Act!
- Daily Telegraph story “Hospital Records of all NHS patients sold to insurers” 23-2-14 hasn’t helped. Referred to SIAS.

Care.Data

- Partridge Report on disclosures by NHS Information Centre (now superseded by the Health and Social Care Information Centre). Discovered a number of improperly authorised disclosures: “To earn the public’s trust in future, we must be able to show that our controls are meticulous, fool proof and solid as a rock.”
- Document to be settled between ABI and DoH will set out care.data handling matters in greater detail

Genetics – talking point

- Law at present almost totally inadequate to deal with issues of genetics.
- Q: How long will the Moratorium on genetics hold? Who is doing the work on projections of cost and reliability of consumer testing kits?
- Q: are insurers ready to handle genetic data as and when it comes (US examples Huntington's –v- haemochromatosis)

Genetics

- Genetics and all predictive health data currently the subject of a consultation by the Bio-ethics committee of the Council of Europe [NB – NOT EU]. Current recommendation to extend prohibitive guidance to all predictive health data. http://www.coe.int/t/dg3/healthbioethic/Source/Final%20E%20consult%20doc.pdf
- Should we consider the New Zealand system of compulsory quoting (no declines)?

Contact

- steven@stevenmarcrhodes.com