What counts in the UK? HIPAA, ISO or ICO?

Confidentiality and Security for Working Online as a Counsellor or Psychotherapist

HIPAA The US Federal Health Insurance & Accountability Act 1996	ISO27001:2013 International Organisation for Standardization	ICO –Information Commissioner's Office
USA	International	UK (linked with EU)
HIPAA is a set of regulations that governs how "covered entities" manage the security, privacy and exchange of protected health information (PHI) data. A "covered entity" is an organisation or corporation that directly handles PHI or Personal Health Records (PHR) and is therefore required to be compliant with HIPAA. http://health.state.tn.us/hipaa/	This International Standard provides requirements for establishing, implementing, maintaining and continually improving an information security management system [ISMS] that preserves the confidentiality, integrity and availability of information by applying a risk management process & gives confidence to interested parties that risks are adequately managed." (Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 27, IT Security Techniques. 2013). There are other ISOs to consider including ISO13385 and ISO17491.	Your need to "….. encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen …." http://ico.org.uk/for_organisations/data_protection/security_measures Accessed 19/06/14 A provider of a public electronic communications service must take appropriate technological and organisational measures to safeguard the security of its services. **An appropriate measure is one that is proportionate to the risks it would safeguard against, taking account of the state of technological development & the cost of implementing the measure**. These measures must **at least**: **(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;** **(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and** **(c) ensure the implementation of a security policy with respect to the processing of personal data.** http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services Accessed 19/06/14

Available at http://www.pwtraining.com/resources -for-working-online/