The Dudley Group NHS
NHS Foundation Trust

Trust Headquarters
Russells Hall Hospital
Dudley
West Midlands
DY1 2HQ

FREEDOM OF INFORMATION ACT 2000 - Ref: FOI/010942

With reference to your FOI request that was received on 04/08/2011 in connection with 'Information Security'.

Your request for information has now been considered and the information requested is attached.

Further information about your rights is also available from the Information Commissioner at:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113
Fax: 01625 524510
www.ico.gov.uk

Yours sincerely

Information Governance Manager
Room 34a, First Floor, Esk House, Russells Hall Hospital, Dudley, DY1 2HQ
Email: FOI@dgh.nhs.uk

Aug-11	Trust FoI	**Kindly refer to the attached document for clarity on the requests being made**	
			Indicate Below
	Is your Trust ISO 27001 Compliant/Certified/Don't Know	Don't know	
	If compliant or certified, how is this measured?	IT services are outsourced to a private company via our PFI project agreement and local PCT for community.	
	If complaint, was this declared by a third party or by the board? If by a third party, kindly send the report declaring the Trust as compliant. If the Board, the minutes of declaration.	n/a	
	if a self declaration, please provide the report and minutes of approval	n/a	
	The number of Commercial Third Parties (CTPs) and NHS Business partners that your Trust has signed contracts with.	2	
			List names of CTPs across each cell
	The names of these companies and when the contract was signed that relate to business in **2011**.	Summit He NHS Dudley (Community staff IT requirements)	
	Which of these companies have access to personal/patient identifiable data? i.e under the Data Protection Act, NHS Number	Both	
	Of the companies above, indicate which does your trust feel are required to make an annual Information Governance declaration?	NHS Dudley Summit Healthcares repsosibilies are covered by our PFI PA. Also the Trust makes IG declarations.	
	Of the companies above, which made their **2011** Information Governance Declaration	NHS Dudley	
	How many of these companies has your Trust audited against the Information Governance toolkit over the last 5 years? Please list the year	Both (2010, 2011)	
	Indicate which were regarded as compliant?	Both	

Who conducted the audit? i.e the trust or an external party. If external, the name of the company.	RSM Tennon
Please send the audit findings/reports?	
Which committee were these reports submitted to?	Audit Committee
Please provide the minutes of the committee meeting that the reports were submitted at.	
Where the reports approved?	Yes. Mitigating actions have action plans and these are being monitored.
Please send your official policy/procedure for auditing CTPs	Covered by main audit policy.
Which companies were placed on the risk register and when?	Neither

ISO 27001

For CTPs/NHS Business Partners that receive person identifable data from your trust:-	
Which have signed the "NHS supplementary conditions of contract relating to information security" (July 2008)?	PFI PA superseeds this requirement.
Indicate which are certificed, compliant or don't know against the standard	
For those certified, has the scope of the certificate been checked for the data your trust suplies?	
With regards to section 5.2, how many of the CTPs/NHS Business Partners have notified you that they "reasonably believe(s) that its certification to ISO 27001 would fail"	

For which CTPs/NHS Business Partners did the Trust “waive the requirement for certification in respect of the relevant parts”.

Was this placed on the Trust risk register?

If an alternative contract was signed, for companies that are supplied personal/patient data please send the details

Are these companies required to be compliant or certified in ISO 27001? Please state

List names of CTPs across each cell

Which companies approached the trust for sponsorhip of their N3 connection?

When did they make the request?

If turned down, **when** and **for what reason.**

Kindly supply the names of the companies that the trust sponsored for a N3 Connection

Who conducted the audit to ensure their request was accurate? i.e the trust or an external party. If external, the name of the company.

Please send the audit findings/reports?

Which committee were these reports submitted to?

Please provide the minutes of the committee meeting that the reports were submitted at.

Where the reports approved?

if non-compliance was identified but approval given, on what grounds, and who was notified?

Was this non-conformance placed on the risk register give date and indicate if still on register and the level?

Please send your official policy/procedure for auditing CTPs on information governance, security and ISO 27001?

Kinldy supply the correspondence with other Trusts/ SHA/ CfH/DH other parties that relate to this FoI request. If there is an forum that concerns this request, please supply the details and correspondence.