Southend University Hospital NHS
NHS Foundation Trust

August 2011

It is either regarded by the Department of Health as a Commercial Third Party (CTP) or an NHS Business Partner.

ISO27001/2/BS7799
Under Section 5 of the "NHS supplementary conditions of contract relating to information security" (July 2008) it states that:-

> *5.1 The Contractor shall obtain independent certification of the Security Plan to ISO 27001 as soon as reasonably practicable and will maintain such certification for the duration of the Agreement.*
>
> *5.2 If certain parts of the Security Policy do not conform to good industry practice as described in ISO 27002 and, as a result, the Contractor reasonably believes that its certification to ISO 27001 would fail in regard to these parts, the Contractor shall promptly notify the Authority of this and the Authority in its absolute discretion may waive the requirement for certification in respect of the relevant parts.*

Please find questions below I would like answered regarding the above.

Additionally, I would also appreciate all the correspondence made with other trusts/ 3rd parties/internally made regarding this request.

1. *Is your Trust ISO 27001 Compliant/Certified/Don't Know*

The Trust has not assessed itself against this standard therefore we have no information to disclose. Compliance with ISO 27001 is not a mandatory or statutory requirement for an Acute Trust.

2. *If compliant or certified, how is this measured?*

3. *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.*

4. *if a self declaration, please provide the report and minutes of approval*

5. *The number of Commercial Third Parties (CTPs) and NHS Business partners that your Trust has signed contracts with.*

6. *The names of these companies and when the contract was signed that relate to business in **2011**.*

7. *Which of these companies have access to personal/patient identifiable data? i.e under the Data Protection Act, NHS Number*

8. *Of the companies above, indicate which does your trust feel are required to make an annual Information Governance declaration?*

9. *Of the companies above, which made their **2011** Information Governance Declaration*

10. *How many of these companies has your Trust audited against the Information Governance toolkit over the last 5 years? Please list the year*

11. *Indicate which were regarded as compliant?*

12. *Who conducted the audit? i.e. the trust or an external party. If external, the name of the company.*

13. *Please send the audit findings/reports?*

14. *Which committee were these reports submitted to?*

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

16. *Where the reports approved?*

17. *Please send your official policy/procedure for auditing CTPs*

18. *Which companies were placed on the risk register and when?*

ISO 27001 - *For CTPs/NHS Business Partners that receive person identifiable data from your trust:-*

19. *Which have signed the "NHS supplementary conditions of contract relating to information security" (July 2008)?*

20. *Indicate which are certified, compliant or don't know against the standard*

21. *For those certified, has the scope of the certificate been checked for the data your trust supplies?*

22. *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"*

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

24. *Was this placed on the Trust risk register?*

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

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

27. *Which companies approached the trust for sponsorship of their N3 connection?*

28. *When did they make the request?*

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

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

31. *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.*

32. *Please send the audit findings/reports?*

33. *Which committee were these reports submitted to?*

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

35. *Where the reports approved?*

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

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

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

39. *Kindly supply the correspondence with other Trusts/ SHA/ CfH/DH other parties that relate to this FOI request. If there is a forum that concerns this request, please supply the details and correspondence.*