

Trust Board

TB2008.13

From: Mr Ian Humphries, Director of Estates & Facilities
Mr Brian Rigby, Non-executive lead for Security

Date: January 2008

Subject: **Security Services update and progress report**

For: **Information**

Synopsis

This paper provides Trust Board with general security information including security incident statistics for 2005, 2006 and for the half year to September 2007, summary details of Security Service initiatives undertaken throughout 2006, and the ongoing ORHT Annual Service Work Plan for 2007/08. In addition, details are provided on IT Security arrangements and assurance.

Commercial Committee has reviewed this report in December 2007 and agreed its progression onto Trust Board.

Trust Board is asked to note the arrangements in place, the statistics with regard to security incidents and the Work Plans ongoing for 2007/08.

Financial, legal and risk impact

Not applicable.

Security Services update and progress report

A: General Security Services Update and Progress Report

Security Incident Statistics

1. The profiles at Appendix A show the average monthly statistics of recorded Security incidents which were experienced across the Trust in four reporting categories through 2005, 2006 and to September 2007.

Incidents of Aggression

Numbers at the JRH continue to show a reduction and this is believed to reflect the improved response of the Security Officer Team brought about by the improved CCTV monitoring arrangements.

The level of incidents at the Churchill and RI remained relatively static.

The increased number of incidents at the HGH is being carefully monitored as this is showing an upward trend; this is believed to reflect the extended security presence and reporting now in place.

The total analysis of aggression incidents throughout 2006 identifies that there were 77 incidents which resulted in full investigation and submission of Physical Assault Reports (PARS) to NHS Security Management Services.

These report forms follow incidents where there was an "Intentional application of force against the person of another, without lawful justification, resulting in personal injury or personal discomfort".

Of the 77 such incidents, 60 arose from the Clinical/Medical condition of patients involving dementia, recovery from anaesthesia, mental incapacity, head injury, infection and confusion.

The remaining 17 physical assaults were not attributable to clinical/medical conditions and involved those under the influence of drink and/or drugs or those who were aggressive by nature. On four occasions the Trust sought to prosecute individuals for incidents viewed as common assault, four convictions were achieved. The average monthly aggression incidents for 2007 are marginally lower than those for 2006.

Removals from Hospital Sites

The removal rate for individuals with no valid reason for being on our sites remained static at the HGH and Churchill. The increase which occurred at the RI reflected the site closure plan and associated protection of Trust assets.

The fall in numbers of removals from the JRH shows an encouraging trend.

The initial statistics for removals in 2007 remains much as in previous years.

Patients Reported as Absent From Their Ward

Numbers remained static across all sites through 2005/06. The level of absent patient reports, averaging 40/month at the JRH, remains under review and is a major demand on Security Team resources.

Of the numbers reported to Security, approximately 73% were very quickly located and returned to wards by the Security Officers.

A further 9% made self returns to wards; 7% were found to have been discharged and have made follow-up visits; a further 4% were recorded as discharged on the Patient Administration System.

The final 7% includes those who have self discharged from the Emergency Department prior to treatment or admission.

Initial statistics for 2007 show that the number of patients reported as absent at the JRH has fallen by approximately 20%.

Thefts

Theft incidents remained relatively low and static at the HGH, Churchill and RI; a fall in numbers was in evidence at the JRH.

For 2007 reported theft numbers remain encouragingly low.

Security Initiatives

2. Throughout 2006 a range of initiatives were undertaken, these included:
 - Site by site security awareness campaign undertaken jointly with TV Police;
 - A joint car crime reduction initiative was undertaken, also with TVP;
 - From March 2006 Police Community Support Officers were introduced at HGH;
 - Headington Hospital sites now included on TVP Area Beat Patrols;
 - Plans to outsource Security Patrol Provision failed after market testing exercise in autumn 2006, but short term external provider service now in place on 24/7 basis at HGH and Churchill. Plan to re-market test in 2007 now under way;
 - Increased CCTV monitoring capacity in place at JRH from December 2006;
 - Regular Security Awareness information and poster campaigns advanced on Vehicle Security, Bike Security, Theft, Credit Card Fraud, Suspect Packages and ID Badges;
 - Trust Security Service Manager now accredited as Local Security Management Specialist following completion of study course.

The ORHT Annual Security Service Work Plan for 2007/08

3. The attached objectives form the basis of the 2007/08 Security Service Work Plan:

- Building a pro-security culture within the Trust
 - Security awareness campaign;
 - Events in partnership with TVP Crime Reduction Unit.

Year to date there have been two sets of bicycle marking and “safe plate” events undertaken on all three hospital sites, and these services are now continuously offered on a request basis. There have also been regular global emails containing security advice and highlighting specific concerns and successes from within the Security Department. A Security Awareness Campaign has successfully been run during November and December to include leaflet, poster and email information, and further Crime Reduction events.

Options to engage a specialist external security services provider are being analysed with a view to strengthening service provisions. Revised arrangements could be in place by April 2008.

- Tackling Violence and Aggression
 - Update and roll-out of the ‘dealing with conflict’ policy (Zero Tolerance);
 - PARS investigations and follow-ups;
 - Investigations and sanctions against offenders.

A proactive approach is being taken on the investigation of PARS incidents, with close liaison with risk management and incident reporting to ensure that no assaults are overlooked. Year to date there have been two successful convictions of violent offenders one Police Caution and a further case currently under investigation.

- Personal safety and transport: Supporting the Transport Strategy with security events and campaigns to encourage ‘greener commute’
 - Bike identity marking and chipping events;
 - Personal attack alarm initiatives.
- Risk assessments of key areas to highlight and put forward recommendations for improved security
 - Paediatrics;
 - Maternity;
 - Areas of high value medical equipment.
- Involvement in the planning and design of new projects in the Trust to ensure that wherever possible security risks have been addressed
 - CH PFI;

- Cardiac Unit;
- Geratology.

There is also close involvement between the Security Manager and the Churchill PFI project in order that the Trust's requirements for the security of the building are maintained. The remodel of level four at the John Radcliffe for the accommodation of the Geratology Outpatients Department is now complete, and advice is ongoing regarding the security of the planned inpatient area.

- CCTV systems are being extended via the Churchill PFI and new monitoring arrangements for these are being planned.
- Access control systems have continued to be extended in areas including Geratology OPD and Discharge Lounge.
- Staff Identify systems continue to be refined and new processes were adopted for the Junior Doctors' intake in August.
- CEAC have completed a Physical Security Audit and the draft report is issued and under review.
- An Annual Security Report will be compiled by Summer 2008.

B. IT Security

Physical Security

OHIS is currently working toward certified compliance to BS7799 standard. This will enable a more cost and work efficient management of Network and IM&T infrastructure security. Timescales are in development for achieving this.

1. All key corporate IT systems operated and hosted by OHIS on behalf of the Trust are housed in secure purpose built environmentally controlled data centres across the three main hospital sites. These areas are alarmed when unattended and have physical access logs in operation.
2. All major corporate systems are password protected. The majority of individual users are issued with a unique username and password for network access.
3. Physical security of the Network from external threats is provided by the Trust's Checkpoint NG (Next Generation) Firewalls. The firewalls provide all perimeter incoming and outgoing defences across a range of information transfer routes.
 - 1 firewall covering Internet/N3 (NHS Network) access (Internal and external traffic).
 - 2 further firewalls will be implemented for N3 connectivity during the upgrade.
 - 1 firewall covering the Virtual Private Network (VPN) solution for home workers, distance workers and third party support companies.
 - 1 firewall covering University access.
 - 2 resilience firewalls for backup.N3 provides a further firewall to protect the NHS Network from external penetration (all Trusts).
4. Controls for incoming and outgoing emails are managed using the Barracuda system. Filtering is conducted against a white list and blacklist of accepted terms. Barracuda provides content filtering, antivirus and spam checking.

Incident reporting

Information Security incidents are recorded as per the Trust Incident reporting procedures.

Copies of the relevant incident report forms are forwarded to the Information Protection Office for investigation, necessary action or filing (as required). Quarterly reports are sent to OHIS management for the quarterly OHIS management group meeting and a report is generated by Non-Clinical Risk and presented to the Information Governance Group.

Information Security Assurance

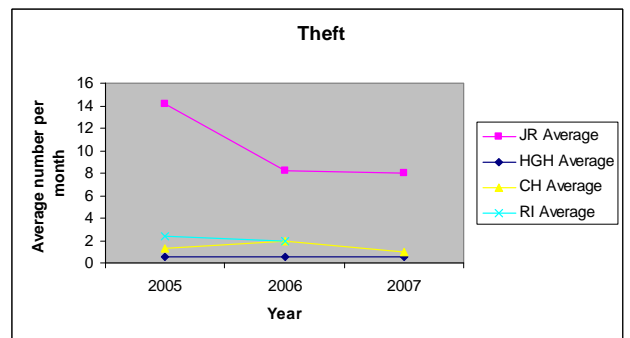
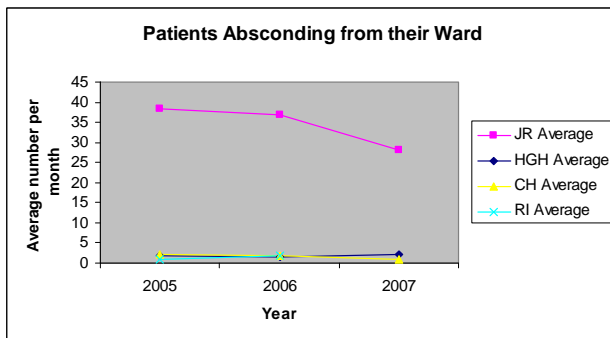
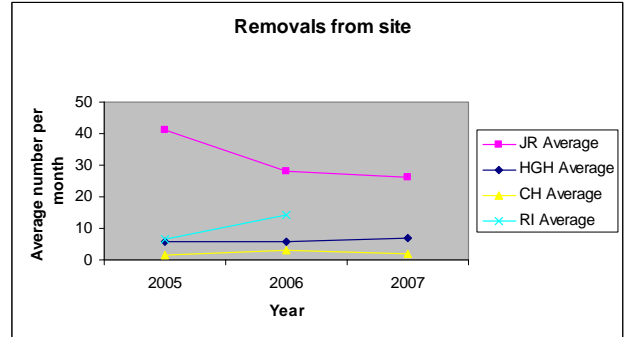
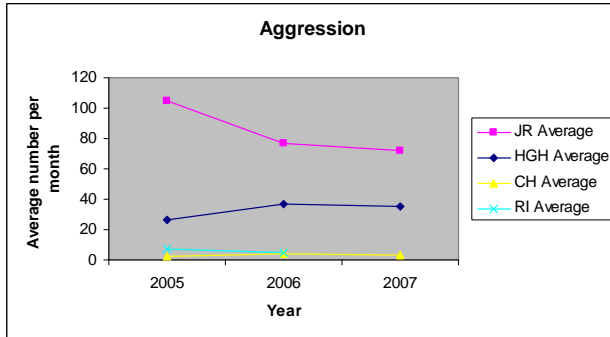
Information security forms part of the annual information governance self assessment. Action plans for areas that require improvement are monitored by the information governance group.

Recommendations

5. Trust Board is asked to:
 - 5.1 Note the statistics and initiatives undertaken in 2006.
 - 5.2 Note the 2007 Security Service Work Plan.
 - 5.3 Note the review of security service provider options.
 - 5.4 Note the arrangements in place for Information Systems security.

Ian R Humphries
Director of Estates & Facilities
December 2007

Oxford Radcliffe Hospitals NHS Trust Security Incident Figures 2005-2007



2007 averages calculated using figures year to date.