**PCIG Consulting Template**

**PHYSICAL SECURITY AUDIT**

**Version: 4.0**

**Date: 6 April 2021**

**This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.**

**Change Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **To** | **Change** | **Date** |
| **1** | **2** | **Spelling checked - examples given in Column 2.** | **13 August 2019** |
| **2** | **3** | **Reviewed and updated** | **1 May 2020** |
| **3** | **4** | **Reviewed and updated** | **6 April 2021** |

[Practice Name]

**PHYSICAL SECURITY AUDIT**

**Document History**

|  |  |
| --- | --- |
| Document Reference: | … |
| Document Purpose: | Provide an audit tool to ensure that There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed |
| Date Approved: | 1 May 2020 |
| Version Number: | 3.0 |
| Status: | FINAL |
| Next Revision Due: | May 2021 |
| Developed by: | Paul Couldrey – IG Consultant |
| Policy Sponsor: | Practice Manager |
| Target Audience: | This audit applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice. |
| Associated Documents: | All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2020 |

[Practice Name]

Physical Controls Audit DS&P Toolkit Requirement 1.6.3

**Prevention of unauthorised access to the premises, equipment, records and other assets**

The Practice has undertaken a security check of the premises and its contents in order to ensure that there are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed, and to ensure that the organisation has adequate provision to safeguard and protect members of staff, patients, the building and other physical assets including sensitive and personal information

A series of questions outlined in the attached document have resulted in the Practice acknowledging what measures it has in place to support any potential risks/hazards that may arise in the event of any incidents. Each question has had its answer risk assessed using the following criteria:

**High Risk** – Could have a serious impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information **(Action Required)**

**Medium Risk** – Some impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information security **(Action to be considered)**

**Low Risk** – Short term disruption to service with low impact on the delivery of patient care, the security of the building, its contents, staff and confidential/sensitive information security **(No action deemed necessary)**

Action plans have been raised to address any gaps or weaknesses in provision. Staff are aware of the need to report any areas of concern to the IG Lead so that appropriate action can be taken

……………………………………………………………….

[Name of Auditor]

**Date:**

**Completed by:** [Name of Auditor]

**Date:**

**Annual Review Date:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| What security measures are in place to safeguard the outside of the building? (fencing, lockable gates, restricted access) | Building on site – secured by security patrol – non-domestic living area. Alarm to building with rapid call out facility. Open Health Centre – however secure staff areas have restricted access is via card coded door –and manned reception area – OCS Manned Security desk – with patrols. |  |  |  |
| Is there any security to monitor the outside of the building? (CCTV, security company surveillance) | OCS Security Company patrol  CCTV Coverage of building is comprehensive and Practice reception is well covered with tilt and zoom capabilities |  |  |  |
| Does the PRACTICE have an alarm system that is serviced annually and supported by a maintenance contract? | Yes - Via NHS Property Services |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| Does the security system cover all areas of the building (PIR’s) – in particular, rooms that contain IT equipment or records? | Systems covers areas of access and all entry points – call out process is in place. All areas containing records are accessed via third access point verification. |  |  |  |
| Is the security system connected to a Police Station or a Call Response Centre? | Yes – response Centre |  |  |  |
| How often is the security alarm code changed? | Unavailable at time of audit – to be confirmed – maybe NHS property Services issue |  |  |  |
| Are there warnings on windows, visible alarms, etc. that warn potential intruders that there are physical security measures in place? | Yes – on entry and on all outward facing walls of the building – on postings around site of building |  |  |  |
| What types of lighting does the PRACTICE have to the outside of the building and does it adequately protect staff when they enter/leave? (security lighting, flood lighting, street lighting) | Well lit – day and night sensored lighting – street lighting and flood lighting in limited areas. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| How are external doors protected? (e.g. 5 lever locks or equivalent) | 5 level locks on all access points to building – all alarmed – all maintained to a good standard |  |  |  |
| How are fire and external doors secured? (e.g. kept closed when not in use) | Break glass points and bar access facilities |  |  |  |
| Do all windows have locks that are secured when rooms are not in use? | Locks available for use – no evidence of any window being left open on any site visit or at time of audit –staff notices should be posted however |  |  |  |
| How is access restricted to the Reception and Administrative areas of the PRACTICE? | Restricted via access control door - however this is also the regress point – there appeared to be little knowledge of desk staff on emergency procedures, |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| What types of security devices are in place to safeguard internal doors to rooms that hold IT equipment/patient records? (e.g. keypads/swipe cards/locks) | Swipe access and additional keypad access to computer server area |  |  |  |
| What security measures are in place to protect areas where private and confidential information is stored? (e.g. Lloyd George records/letters that have been scanned awaiting shredding, HR information/business finances)  *This may involve restricting access to authorised personnel* | Safe haven Facilities in separate room – confidential waste bin available on each floor – non needing replacing at time of audit |  |  |  |
| What provision does the PRACTICE have for keeping keys safe? | To be confirmed by Practice |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| Is there an agreement in place for members of staff or associates that have keys/keypad codes/swipe cards to access the building? | Yes – Staff having access cards via application and personal details stored with access controls based upon role |  |  |  |
| Does the PRACTICE have a signing in/out policy for attached staff? | Yes – in operation and working well at time of audit |  |  |  |
| How does the PRACTICE establish whether visitors (NHS, third party, etc.) have relevant IG clauses in their contracts of employment? | Yes updated practices visitor guidance and policy in action |  |  |  |
| Are ID badges worn by staff at all times? | ID and visitor badges were [[1]](#endnote-1)seen at time of audit but prominent display not evident |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| How does the PRACTICE keep a record of visitors? | Yes – visitors book at reception – older copies were available upon request |  |  |  |
| How are deliveries to the PRACTICE supervised? (e.g. stationery orders) | Check with PRACTICE |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| Who is responsible for maintaining the PRACTICE’s information asset register? (e.g. hardware, software, manual records, services, portable computing equipment) | IAO Data Mapping to be completed by practices for Assets |  |  |  |
| How frequently is the asset register reviewed and updated? | Yearly – current desktop refresh programme underway with excellent auditing facilities |  |  |  |
| On checking all computer screens and locations, are they angled so that they cannot be viewed by unauthorised personnel from inside and/or outside of the building? | No screen were visible for outside building to be able to read screen display. Limited screen protection inside building, protection based upon staff contracts and training. Systems have emergency call on keyboard shortcut |  |  |  |
| Is all IT equipment asset marked? (HIS number/Smartwater) | Yes |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| Indicate if the PRACTICE has a protocol for transporting confidential information off-site and where it can be found. (e.g. transfer of patient records from a main surgery to the branch/home visits) | Practice has appropriate Policy |  |  |  |
| What provision does the PRACTICE have to ensure that the system server is protected by an uninterrupted power supply? | Referred to NHS Property Services Contract |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| How is the PRACTICE able to check that the clinical system back-up battery is working? | Referred to NHS Property Services Contract |  |  |  |
| Is all electrical equipment PAT checked annually? | Yes­ PAT tested stickers evident on equipment – all were up to date |  |  |  |
| Does the PRACTICE have a fireproof safe where back-up tapes and other sensitive media or documentation can be kept? | Referred to CSU IT Contract |  |  |  |
| How does the PRACTICE manage role-based access to the clinical system for employed and attached staff? | Yes – via username and login - staff training up to date – on audit staff questioned were aware of responsibilities and displayed good security awareness – no screens were found unsecured at time of audit |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| How does the PRACTICE ensure that all computer users aware that passwords should not be divulged/shared? | staff training up to date – on audit staff questioned were aware of responsibilities and displayed good security awareness – no screens were found unsecured at time of audit |  |  |  |
| How frequently are passwords changed? | Dependant on system – all users were aware of their responsibilities on questioning |  |  |  |
| Is it documented that users of computer systems are required to change user/lock down or log out (as appropriate) when leaving their work station? | Yes – via username and login - staff training up to date – on audit staff questioned were aware of responsibilities and displayed good security awareness – no screens were found unsecured at time of audit |  |  |  |
| How long does it take for automatic screen savers to activate? | Timed at 90 seconds |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| Where practicable, does the PRACTICE have a clear screen/clear desk policy? If so, where can it be found? | Clear screen policy was evident in behaviour patterns – clear desks seems less so |  |  |  |
| Does the PRACTICE have a business continuity plan that covers loss of premises, computer systems, utilities, essential supplies, security systems, paper records, clinical/non-clinical cover? | Practice has own BCP |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question** | **State what you have to support your response or why you think it’s not necessary/Action Plan if appropriate** | **Risk Level**  **H/M/L** | **If Action Required**  **Person responsible Action/Target Date for completion** | **Completion Date** |
| How will the business continuity plan be tested for effectiveness? | Tests to be completed 2015 |  |  |  |

|  |
| --- |
| Additional Notes/Comments |

1. [↑](#endnote-ref-1)