BSO Pharmaceutical Secure Web Portal User Agreement Additional Explanatory Notes

The following text provides explanatory notes in relation to the User Agreement. The section heading and numbering below relates to the relevant paragraphs in the User Agreement.

Section A – Obligations

2 – BSO requires adequate notice to implement changes on the system and to mitigate risk to the Contractor in instances of staff movement etc. Five days is the standard timescale across all Secure Web Portals. However, we understand that there may be circumstances where this isn't possible. In these cases where reasonably practical will suffice.

3 – All Active Directory accounts are set at an individual level, details of which must not be shared with anyone. These should be changed immediately upon suspicion of any compromise. This will protect both your account and the BSO Secure Web Portal.

7 – Appropriate access to the BSO Secure Web Portal should be for business use only. Any activity should be for business purposes and any information obtained from the BSO Secure Web Portal should only be shared with authorised users.

8 – Each pharmacy will have a nominated Sponsor. The Sponsor will be a nominated senior member of staff within that organisation who is responsible for authorising users and their access levels, within their relevant pharmacy and informing the BSO of any changes.

9 – For example, in situations where a contract ends, or a Pharmacy changes ownership, or you believe your account has been compromised, you must inform BSO as soon as reasonably practical to disable your account.

11 – The BSO servers are set to protect against any malicious attack on its systems, especially in today's environment of cyber-attacks, which would have a devastating effect on the Health Service. Therefore, if the systems detect malware from a contractors PC trying to illegally access or infect the BSO network, whether it's intentional or unintentional, the account could be suspended as an automatic safeguard. This would be carried out by the eBusiness team who would then immediately inform the contractor in order to assist in addressing this issue. A detection of high volume activity beyond reasonable human actions would be perceived as excessive account activity as some malware designed to disrupt or overload systems does so by performing sustained high volume of actions in quick succession.

13 – For example, access to the Portal will be temporarily suspended during payment runs or in unforeseen circumstances where the system may require urgent critical ITS intervention e.g., patches, updates or server outages etc. Other than on these occasions, the system will be routinely available. Contractors will be notified in advance of any planned downtime.

Section B – Cryptocard Key fob

For Example – The BSO has the right to request the return of the Cryptocard key fob if it's damaged and requires replacement or 3 months maximum after a contract has ended.

Section C – Remote Technical Support

1 – In order for the BSO eBusiness team to support connectivity issues they may require remote access into the Contractors PC. In order to facilitate this they avail of the Bomgar software which provides an industry standard secure encrypted connection. This will only be used with the permission of the Contractor, is fully auditable and can be terminated at any time by the Contractor. In instances where BSO detect an application requires updating the Contractor will be advised and BSO will only act upon instruction. They will never auto update any application on a contractors PC.

3 (d & e) – Any remote assistance from BSO will only be provided by staff who have been fully trained and reached the required competency level to offer safe and efficient remote support services. Staff are fully accountable, comply with internal Governance standards and are bound by BSO confidentiality agreement as part of their employment terms & conditions.

Section D – Access to the FPS Payments Portal and Future HSC Services

2 – FPPS is one of a number of services that could be deployed via the BSO Portal Landing Page. Any future services deployed on the BSO Portal Landing Page will require separate user logins and passwords for each individual service.

Section G – Confidentiality

All employees of BSO, including temporary and agency are bound by confidentiality compliance agreements as part of their contract of employment. BSO is fully compliant with statutory requirements in line with the Data Protection Act 1998 and its subsequent replacement, The General Data Protection Regulation, which takes effect in May 2018.

Section F – NIECR

All system access and usage is audited. The information below is typical of, but not limited to, the proactive auditing which will be performed by the NIECR team based in BSO:

- Possible abuse of passwords (e.g. where log-ins show an account has been used consecutively over a long period of time – longer than an average shift – e.g. 15hrs)
- No valid reason for demographic search is given (user name, name, location, date, time)
- Users with large number of searches over defined periods (>100 searches within a reporting month)
- Consent override alerts
- No valid reason given for 'other' category for absent patient access
- Results of ad hoc audit queries.

Section H – Personal Data

Personal data is required by the BSO in order to create an Active Directory Account for the user. The National Insurance number is a guaranteed unique identifier for each individual. This enables BSO to ensure there isn't duplication of accounts i.e., details of the same individual do not appear on multiple occasions in the directory. In compliance with good Governance and Audit practice the National Insurance Number is encrypted and stored by BSO ITS in a secure locality.

Section I – FPPS Pharmaceutical User Agreement (Sponsor Section)

Each organisation is required to select a Sponsor for that organisation. The Sponsor will be a nominated senior member of staff within that organisation who is responsible for authorising users, and their access levels, within their relevant pharmacy and informing the BSO of any changes etc.