

# Service Level Agreement – March 2008

between

Bromley PCT ICT Team

&

General Practice

for the provision of Technical Support Services

## **Service Hours and Standard Service Availability**

Standard hours of service

- Between the hours 09:00 – 17.00 Monday – Friday excluding Bank Holidays;

Extended support hours may be provided, however this is at the discretion of the PCT and may be subject to a reasonable charge.

## **Support Desk**

It is expected that the first point of contact for practices in notifying incidents will be with the agreed Help Desk facility. The core functions of a Support Desk service include:

- receive user reports against the service;
- agree with the reporter what the Incident Priority Level is; (High, Medium, Low)
- allocate a unique incident identification number;
- initiate and manage the support process;
- agree incident closure.

Whilst in some cases the Support Desk operator may assist in the solution of incident reports it should not be assumed that provision of detailed technical support is a core function of the Support Desk. Where the Support Desk cannot offer detailed technical support its role is to facilitate access to such support under the terms of the relevant agreement.

The Service will be available 100% of the time within the Service Hours and the Help Desk aims to answer 90% of initial Incident calls within 60 seconds.

Outside the standard hours of service and during normal service hours peak times an automated facility exists to log and record incident reports. The methods in place include

- answer machine;
- email; or
- online via intranet

### **Service Provision method**

The support service may be provided to practices by a number of methods, dependent upon the type of Incident identified, local agreements and existing infrastructures. Methods that may be employed are as follows:

<b>Types of support</b>	<b>Example Instances</b>
Telephone support	Upon notification of Incident or a call back from the support organisation
Remote Software Support (where available)	By remote connection, agreed with the practice. This may be at notification of Incident stage or after a call back from the support organisation. This method may also be used by third party suppliers to connect to practices systems to support Incidents or where suppliers are required to check if practices have activated patches or system upgrades.
Practice Site Visit (PCT or relevant contractor)	Where an Incident requires on site support by PCT staff (or contractors).
Practice Site Visit (GP Clinical system supplier)	Where an Incident requires on site support from the Clinical System Supplier.
Repair /Replacement	Where hardware or network equipment requires repair or replacement. Where equipment needs to be repaired off site, loan equipment should normally be provided and the installation signed off by the practice to ensure business continuity.

### **Incident Closure**

Ownership and management of all Incidents should be the responsibility of the Technical Support Team. If an Incident requires a Third Party to be involved this

need not normally lead to the registering of a new Incident. In such cases the original Incident number (and obligations in respect of Priority Levels and Standard Response Times) will apply.

Priority Levels may be varied (upon agreement with the Help Desk and the practice) during the period of an Incident, dependent on user impact.

Where it is agreed (between the practice and the Help Desk) that an Incident has been resolved (by whatever Service Provision method) the incident needs to be closed in the Help Desk system. This may be by direct contact between the Help Desk and the practice, or by “signing off” an Incident by the practice to a support person, using prevailing local custom and practice.

Closure of an incident should not generally take place without agreement from the user affected.

### **Service Areas Covered**

- accredited General Practice clinical system hardware, software and networking equipment required to operate the system at existing versions and/ or to prevailing manufacturers standards in current use within the practice and any branches, including document management systems or handheld computers;
  - supporting business software and/or hardware (e.g. Microsoft Office, Antivirus utilities) at existing versions in current use within the practice and any branches, including electronic mail systems;
  - software and/ or hardware at existing versions in current use within the practice and any branches for connection to services provided by the PCT (i.e. NHSnet or internet services) or to national systems (i.e. electronic access to referrals, discharges, diagnostic tests etc);
  - the implementation and operation of current security and access policies e.g. role based access control;
  - other software and/or hardware at existing versions in current use within the practice and any branches for clinical/administrative support purposes. It is likely that this category will encompass “non standard” software and/ or hardware discovered as part of any baseline audit/ due diligence exercise undertaken by the PCT as part of the transfer of assets/responsibilities from the practice;
- 
- such software and/ or hardware will be supported on a reasonable endeavours only basis by the PCT;
  - where the practice requires a defined service level the PCT may consider this to be an additional service and make a reasonable charge for the support service;

- where this software/hardware requires to be upgraded, a case for the investment to be made will need to be made by the practice to the PCT, with the PCT not being obliged to meet these costs.
- PCT to agree an approved list of software that may be loaded onto PCT equipment.

## **Security and Confidentiality**

It is the responsibility of all parties to adhere to prevailing Security and Confidentiality policies at all times. Further details of current Security and Confidentiality policies can be found on the following web site:

<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationsecurity/index.htm>

## **Data Protection and Related Legislation**

It is the individual responsibility of all parties to ensure that they conform to current legislation relating to the use of IT systems within general practice, including the Data Protection Act 1998, Computer Misuse Act 1990, Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000.

The GMS contract includes a clause that obliges practices to adhere to all relevant legislation and to have regard to relevant guidance (Schedule 6, paragraph 125), a similar clause (applying to both parties) in this part of support contract would be good practice.

Relevant documents can be accessed via the Data Protection website:

<http://www.dataprotection.gov.uk/>

## **Recommended Processes and Procedures**

To operate successfully the support service in a manner that is efficient and fair to all parties there needs to be a set of procedures and processes that everyone agrees to adhere to. Some basic ground rules are suggested below.

## **Preparing to Call the Help Desk**

In order that a call can be dealt with quickly and efficiently it is good practice for the caller, as far as possible, gather the following information prior to making the call:

- the practice name and location of the equipment;

- the support tag number, where it exists, being provided for all Incidents;
- the GP clinical system and version of the software used e.g. EMIS LV, InPS Vision
- Consider the impact of the Incident in relation to the Priority Levels described in their support agreement;
- Check if anyone else in the practice is experiencing similar Incidents. This is important as it may be symptomatic of a larger Incident (i.e. access to an application) and provision of this information will aid a speedy resolution.

It is always good practice for the calls to be made by the person experiencing the fault in order that full details are available to the Help Desk. The practice may find it useful for one or two individuals to act as the owner of the practice fault log monitoring that each of the faults recorded are resolved to the practice's satisfaction.

### **Logging the Incident**

When the call is answered the Help Desk operator needs to lead the caller through a series of questions. The first set of questions should aim to establish caller identity and verify the caller location and contact telephone number are correct.

Having established caller identity the operator needs then take details of the Incident. The operator may ask the caller to carry out some diagnostic checks but this will only happen if the caller is comfortable with the checks they are being asked to carry out.

Finally, the operator needs to agree the Priority Level of the Incident and issue the caller with a unique call reference number, which should be noted, by the caller together with the time that the call was logged. The call reference number should be quoted in any further contact with the Help Desk relating to the Incident.

### **Service Management**

#### **Service Standards**

The following industry standards are applicable and it is recommended that they are, where relevant, carefully incorporated when developing the support service:

- BSI PD0005, - code of practice for IT service management
- BS15000
- ISO 9000 series, EN29000 and BS5750 - Quality Management and Quality Assurance Standard
- British Standard 7799 for Information Security Management

Information to aid in the development of services is also available through IT Infrastructure Library (ITIL).

## **Health and Safety**

In order to ensure safe usage of the systems, equipment and delivery of the Service, practices need to ensure that all practice staff using systems are adequately trained in Health and Safety issues and that systems and equipment are sited and used by practice and support staff in accordance with appropriate Health and Safety legislation.

## **Access to premises and systems**

Practices need to ensure that support persons have reasonable access (including via agreed remote support) to premises and equipment during Service hours. Where access is not made available, it is recommended that the consequent delays should not be taken account of in calculating response times.

Where equipment is sited in clinical areas and as a consequence this affects the delivery of the Service, it is recommended that consequent delays should not be taken account of in calculating service provision.

## **Disposal of equipment**

When equipment has been replaced, it is important that when it is taken off the practice premises that any patient-based or business confidential data has been removed. Additionally if any software is to be reinstalled onto new equipment (to comply with end user license agreements) then that software must be removed, or if to be retained by the practice, appropriately licensed by the practice taking into account the need to preserve initial licenses for any version upgrades.

When practice-owned equipment is replaced then the responsibility for disposal lies with the practice. Responsibility for the disposal of PCT-owned equipment lies with the PCT. PCT disposal ought to be completed within an agreed timeframe.

The PCT should have in place arrangements/contracts for secure disposal of equipment, which can also be accessed by practices, at their own cost, for equipment that they are responsible for.

## **Business Continuity (Contingency) Arrangements**

It is good practice for practices to be required to develop "Business Continuity Arrangements" (BCAs) to cover situations where the service or elements of the service are not available. Practices need to develop these arrangements against their need to maintain appropriate standards of support for patient care during periods where access to their GP Clinical system is denied to them.

## **Software Not Supplied by NHS**

It is recommended that the support service agreement require practices to seek permission from the PCT prior to loading any software not supplied by the NHS. It would not be desirable for the PCT to withhold permission for software that a practice reasonably needs to perform NHS and non-NHS services unless it has reasonable grounds for suspecting that installation will materially affect system performance/availability. It is good practice for the PCT to advise the practice of their decision within a reasonable time, for example within one month. Such software may include payroll, accountancy, or reference software etc.

It would be sensible for the PCT in conjunction with its LMC (if any) to reach local agreements regarding which software is normally acceptable.

Practices would normally be required to load the non-NHS supplied software, and to rectify any problems caused by the software. It is not reasonable to expect the PCT to accept financial or other responsibility for such software and all costs of maintenance, upgrades and support are to be considered as falling to the practice unless, exceptionally the PCT agrees otherwise.