

GLASTONBURY SURGERY

NHS Information Governance:

Information Security Policy

1. Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of Glastonbury Surgery. It is based on the expectations set out within the Information Security Management: Code of Practice for NHS organisations:

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/policy/code-of-practice>).

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by Glastonbury Surgery. This shall be achieved by:

- Ensuring that all members of Glastonbury Surgery staff are aware of and shall comply with relevant legislation, including the Data Protection Act (1998) and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Describing the principles of information security management and describing how they shall be implemented within Glastonbury Surgery.
- Introducing an approach to information security that is consistent with other NHS organisations.
- Assisting staff to identify and implement information security as an integral part of their day to day role within the practice.
- Safeguarding information relating to staff and patients under the control of the practice.

2. Objectives

Key objectives of this Glastonbury Surgery Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those GPs and staff of Glastonbury Surgery and relevant others with agreed authority to view it.
- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised GP or medical professional, when it is needed.

3. Responsibilities for Information Security

- Responsibility for information security shall rest with Dr Alastair Corfield. However, on a day-to-day basis the practice manager shall be responsible for

organising, implementing and managing this policy and its related good working practices.

- The practice manager shall be responsible for ensuring that both permanent and temporary staff including any contractors and locums are aware of:-
 - The information security policies applicable to their work areas
 - Their personal responsibilities for information security
 - Who to ask or approach for further advice on information security matters.
- All staff shall abide by security procedures of Glastonbury Surgery. This shall include the maintenance of Practice records whilst ensuring that their confidentiality and integrity are not breached [this applies to patient, staff and practice information]. Failure to do so may result in disciplinary action.
- This Information Security Policy document shall be owned, maintained, reviewed and updated by the practice manager. This review shall take place every two years. The results of which shall be made known to Dr Corfield with overall responsibility for security.
- Staff of Glastonbury Surgery shall be responsible for both the security of their immediate working environments and for security of information systems they use [eg workstations, laptops, PDAs, cardex etc].
- Any contracts with third party organisations that allow access to the information systems of Glastonbury Surgery, shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by the practice.

The Practice shall undertake to ensure:

1. **Contracts of Employment** – address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.
2. **Access Controls** - to areas containing information systems are restricted and controlled to ensure that only GPs and those authorised can access information of the Practice.
3. **Equipment Security** – is effective in order to minimise losses, or damage to the Practice. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fire proof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).
4. **Information Risk Assessment** – a regular assessment of the working environment, shall be conducted to identify potential risks to the security of Practice information. Where risks are identified, these should be noted and where possible mitigating action taken.
5. **Security Incidents and weaknesses** - are to be recorded and reported to Dr Alastair Corfield or the practice manager so that they can be investigated to establish their cause, impact and the effect on the Practice and its patients.

(NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).

6. **Protection from Malicious Software** – should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Practice without the explicit permission of the practice manager. Breach of this requirement may be subject to disciplinary action.
7. **Secure Communications** – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of patient records are conducted in a secure and confidential manner. The communication of NHS Confidential or NHS restricted information by email must be appropriately protected, using cryptographic controls (AES 256 bit or equivalent). NB: When using NHSmail this technical security protection is automatic. Somerset PCT promotes the use of SECURESEND as their preferred secure document sender.
www.securesend.somersetpct.nhs.uk
8. **Business Continuity and Disaster Recovery Plans** – are in place so that in the event of a disruption to the information services of the Practice, it is possible to activate relevant business contingency plans until affected services are restored.

Policy approved by:

Signature

Dr Alastair Corfield

Date October 2009

Glastonbury Surgery

COMPUTER AND DATA SECURITY PROCEDURES

Staff Responsibilities:

Lead responsibility for Information Governance:	Dr Alastair Corfield
Information Security :	Dr Alastair Corfield Andrea Ball (Practice manager)
Data Input Clerk: Housekeeping, data accuracy. Checking memory status and contacting EMIS via support line in event of fault/problems.	Hayley Browning
Back up tapes:	Justine Harris

Practice Computer System

The practice operates EMIS LV 5 and is working towards Paperlight Accreditation. The system is incorporated into a network of PCs through out the building incorporating Millfield School Surgery and Millfield Prep School.

Password Access

Practice Employed Staff:

- Maximum password age; expires in 120 days
- Minimum password age: allows changes immediately (with authorisation from Hayley)
- Minimum password length: at least 6 alpha or numeric characters can be used.
- Password uniqueness: password can be reused after 5 different passwords have been used.
- Account lock out after 3 bad logon attempts. 2 minute lockout.

Third party staff – login passwords: e.g. Midwives, Dieticians, Locum GP's:

EMIS –

All third party staff with frequent turnover of personnel have generic logins. This is to prevent the event of messages from other practice staff going unread, and to ensure access to the EMIS system so that they may record consultations etc.

The login details are unique to each group, (meaning the midwifery team has it's own login details, as do the dieticians, and the locum GP's).

NETWORK –

Midwives: There is normally a practice-based midwife, who has their own personal network login. In the event another midwife comes in to cover a clinic or likewise, they will log in using the generic practice account.

Dieticians: Dietician clinics are often held by different members of staff, therefore there is a generic dietician profile for them to use.

Locum GP's: There is a generic network profile for locum GP's meaning the practice can ensure they have access to everything they might need, for example, access to the practice intranet for referral documents.

Back up Schedule

Daily server back up is performed using a rotation of 10 tapes. It is performed automatically via a timed backup in the early hours of the morning. Tapes are removed in the morning and are stored in the adjacent Pharmacy locked safe.

Somerset PCT have purchased Egton's Tape Validation Service (TVS) on behalf of the practice. The primary objective of TVS is to ensure that the system backup is not corrupt and can be restored onto an alternative server if necessary. All tapes are processed by staff who have CRB security clearance and who comply with BSI registered ISO27001 (data security standard) and ISO20000 (service delivery) qualified management systems.

The tape that is validated by Egton on a quarterly basis is also stored in the Pharmacy safe.

Daily backup of the appointment system to a dedicated PC is carried out by Justine in the event of a server failure situation.

System Restrictions

EMIS has user categories, which dictate the level of access for each user, within the surgery.

Hayley is responsible for adding new members of staff onto the system and with the practice manager determining the levels of access to medical information.

Data Protection

The practice is registered under the Data Protection Act.

Smart Cards

Where access to the clinical or other systems is to be controlled via the issue of a Smart Card the following will apply:

- Smart cards are issued to an individual on a named basis and are for the use of that person only. RA01 forms to be understood & signed by staff upon issue of smart card
- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff

- The Smart Card is to be kept under the personal control of the individual to whom it has been issued at all times and must not be left inserted into a smart card reader when the individual is not present
- The Smart Card will normally be held on a neck cord or other similar device to ensure that it remains with the owner
- On leaving a terminal the Smart Card is to be removed ***on every occasion***
- Staff members are responsible for the security of their own smart cards and may only leave it on the premises if securely locked away.
- Staff members leaving their cards at home will be required to go and collect it
- Staff members sharing Smart Cards on more than one occasion will be considered for disciplinary action in accordance with the Practice's normal procedures. This would normally be after an informal warning
- Staff members must report the loss of a card to the practice manager as soon as it is known that the card is missing
- Smart Cards will not normally be handed over between individuals. In the event of a staff member needing to relinquish a card (e.g. over a holiday period) then this will be passed back to the Practice Manager or nominated person who will log the transfer and retain the card securely

Policy Review Date : Oct 2010