Approved

March 2013

Online document sharing and storage tools: Good Practice Guide for NHSScotland

Purpose

This document is aimed at health board employees who provide advice and support (e.g. IT Security, Information Governance and e-communications) as well as business owners who make decisions on information risk at procurement/design stage.

1) Benefits

There are now a vast array of online 'public cloud' document storage and sharing tools such as Dropbox, Google Docs, Apple iCloud, Box.net, Skydrive (to name but a few) that are used by a high proportion of NHS staff in their personal and professional lives (e.g. for storing music, photos, domestic accounts, notes from college modules and training or even personal notes on own healthcare).

Some of these tools, if properly risk assessed and used with the agreement of boards, can bring many corporate benefits to NHSScotland. For example, it can help bridge many of the information sharing gaps that would otherwise necessitate complex and expensive IT systems or which currently require risky workarounds (e.g. sending high volumes of documents to non-official email accounts). There can even be advantages from an information assurance angle (e.g. almost 24/7 availability to any user with an Internet connection, sometimes more robust data-centres than small health organisations such as GP practices can provide and avoidance of removable media or paper files when an employee works on data at different locations). Some of the typical user scenarios are described in Annex A.

2) Purpose

The aim of this guidance, which follows a high level risk assessment, is to show how and when these tools can be used, the measures that need to be in place and the behaviours expected of end-users rather than simply to recommend particular products.

The focus is on the commonly used types of external publicly-hosted document sharing/storage tools (but is not designed to cover use of intranets or every aspect of Cloud Computing security).

Having a policy of simply blocking all usage to these tools will not work as, just like social media, we know that staff already using them in an ad-hoc manner for a variety of personal/health board purposes. We need to haul in this un-official activity from out of the shadows (to risk assess, officially sanction some of it and provide more guidance for use of tools), while at the same time to be clear where information and security policy is transgressed (i.e. ignorance no longer a defence if an employee stores NHS information on patients in non-official places).

3) Information risks

The measures suggested below are designed to mitigate the following very real risks[1] relating to:

- **Security -** Often the technical security offered by these online tools, whether they are branded 'enterprise' or 'consumer' level, are simply not robust enough for the purpose to which they are being used in health or social care. The seventh principle of the Data Protection Act may not be met - in the case of identifiable personal data – and corporate or research non-personal data may not have the controls required for the sensitivity level.
- **Ownership** - Legal issues over 'ownership' of data abound. If an employee for example has signed up as an individual health professional, rather than via an organisational health board agreement with online provider, then it can often be difficult to disentangle ownership and responsibilities for any breaches in security/Data Protection (e.g. are you the Data Controller or is it your health board?).
- **Freedom of Information and other laws –** Access to information legislation (FOISA and Environmental Information Regulations) depend on information being held by the public body and therefore 'discoverable.' And in the case of personal data an organisation needs to be able to satisfy subject access requests for DPA. If data is being uploaded onto an external Internet-based document store in an ad-hoc and un-controlled manner then it may be difficult to be compliant (e.g. a record manager or system administrator cannot search or audit in the same way as on internal systems).

[1] Full Information Risk Assessment for NHSScotland is available on demand for Information Governance and Information Security personnel.

- **Records Management** - There are significant information and records management issues (e.g. users uploading documents onto the online file storage instead of filing them in the official internal records systems and/or lose version control). The storage of unique business documents, and associated knowledge (e.g. 'conversation strings') onto an external web-based site in preference to internal information systems can mean that the board loses key assets that it has paid for or requires for business purposes.

4) First principles: National accredited or locally agreed tools?

A distinction must be made between:

- **Nationally accredited** online tools for agreed purposes (e.g. x knowledge/document sharing tool contracted to be used by several boards).
- **Local tactical** - but still officially sanctioned - online tools (e.g. to allow a small team or even an individual to do a specific time-bound task/project) which cannot be done over the intranet or other internal tool.
- **Employees' own usage** for strictly personal/professional purposes that should not hold any NHSScotland owned information.

Making this distinction is vital as it has a direct bearing on the sensitivity of the information that should be stored on it:

Given what is known about the current cyber threats it is highly recommended that:

Identifiable personal data at 'amber level' (see Annex B for description) can ONLY be held on the nationally accredited tools.

For example, NHSScotland could formally accredit a tool that uses a Public Cloud service model to hold sensitive personal data on patients or staff. There would be a formal contract with the provider and a higher level of assurance than would be the case for the off-the-shelf consumer tools (e.g. as to which country data held in, robustness of data centres etc). See Annex A for examples.

Identifiable personal data or corporate information of the highest sensitivity (i.e. 'red', see Annex B for definition) should NEVER be held on any online public-cloud document storage or sharing tools.

Even with the above accreditation in place, it is recommended that the most sensitive personal or corporate data is still not held in public cloud services until further notice. This is information which is judged to have the highest impact if lost (Annex B lists examples such as child protection, sexual health etc). Instead, private cloud and other service models are recommended (see Annex A for example).

Corporate information at 'amber' level can be held in tactical locally agreed tools

Corporate information, and not just patient information, can have some sensitivity and an impact if it is lost or misused (e.g. draft executive option papers and where FOI exemptions might apply). But with measures, such as those detailed below, they can be held on approved tactical online tools.

Sufficiently Anonymised patient or employee data can be held in tactical locally agreed tools

For example, clinicians may wish to share research data with others outside the board. Provided this is sufficiently anonymised, sanctioned by Caldicott Guardians etc, and has basic measures in place, online document storage tools can be used.

No employee should be filing any corporate or patient data on online tools which are neither nationally accredited nor locally agreed.

For example, if an employee enrols with an online document sharing site for personal/professional purposes (e.g. accreditation documents to satisfy the Royal College of X) and then proceeds to also file health board owned material or patient identifiable information onto it then it would contravene policy and could lead to disciplinary action.

The above is summarised in Fig 1 and scenarios in Annex A show how this policy can be put into action.

Fig 1: Recommended sensitivity levels and use of online tools (Public Cloud)

	AMBER Corporate	AMBER Personal Data	RED Corporate or Personal Data
National accredited online tools			
Local tactical ad-hoc use of online tool officially sanctioned			
Tool an employee uses for personal and professional purposes (i.e. not board sanctioned)			

5) Practical considerations

Check list

Area to consider	Met√
1) Personal identifiable information = nationally accredited tools	
2) Clear on who is 'owner' of each site	
3) Short user information management guide produced	
4) Separate sites for public access	
5) Choose very simple permissions model	
6) Avoid tools that require downloads of software	
7) Consider tools that offer more than password protection	
8) Go for encryption at authentication and when stored	
9) Use 'Favourites' and view links with suspicion	
10) Check if authentication is required to open links	
11) Agree on consistent way of uploading	
12) Check how far data is deleted completely	
13) Follow mobile data encryption standard	
14)Never use online tools as back-up	
15) Never use online tools for mission critical activities	
16) Check in which country data is held	

17) Check suppliers' privacy statements relating to their use of data	
18) Make staff aware risk mixing personal with board material	
19) Do not encrypt files prior to saving onto site	
20) Check web security architecture	
21) Is it knowledge sharing, document sharing or both?	

1) Patient identifiable information = nationally accredited tools

Personal identifiable data on patients and staff can only be held on nationally accredited tools for agreed purposes. The reason for this is that a higher level of assurance is required than that which can be obtained by off-the-shelf tools.

In cases where tools are agreed for local tactical uses (e.g. allowing an employee to share research that derived from the health board) patient data needs to be sufficiently anonymised before it is uploaded.

In the case of corporate information, employee names do not need to be routinely removed from documents unless a Freedom of Information Act exemption would apply (e.g. health and safety, information provided in confidence etc). Boards now publish large volumes of corporate data which include names of attendees at meetings and decision makers.

2) Be clear on who is 'owner' of each site

Where boards agree on usage of a tool there must be a clear owner who will take responsibility for inviting persons to use the site, managing security permissions, to communicate and act upon the board records/information management policy and to ensure that the site is decommissioned when no longer necessary. This might for example be single clinician who has a site to share research or a team leader for a large project with staff scattered all over Scotland.

3) Short user information management guide

Having appointed a site owner it is not acceptable to then just start sending links to colleagues and expect them to understand the functionality and basic rules. There must be a short (could be just one page) guide to what documents can be uploaded and how the site is to be managed for the particular purpose (e.g. "only copies must be uploaded with original

records held by the board; only the site owner can invite others in the space; only use Excel and Word etc.").

4) Separate sites for public access

Online storage tools, and social media sites, can be useful places to store documents that the health board wishes to share with the wider public. Even though it is usually possible to segregate data via permissions (i.e. private and public spaces) it is advisable to keep these sites completely separate from those used for internal/staff purposes (e.g. "we have a Google Docs account used for documents cleared for public view and various Huddle accounts for our staff to use for non-public documents").

This means there is much less risk of sensitive corporate and clinical information being uploaded by mistake onto a public area.

There should also be a formal process by which things are cleared for uploading onto the public areas (e.g. only the board's e-communications team put up the final redacted responses to FOI requests).

5) Choose very simple permissions model

Permissions can be a useful way of ensuring that only a particular individual or team can see information. We also use them outside work in social media sites (e.g. content suitable for "my friends only" and "public"). But in a corporate setting it is very easy for permissions to get out of hand with a multitude of groups, sub-groups and roles. This complexity can often cause mistakes to happen. It is far better to go for a permissions model where the site owner simply maintains a list of approved individuals who can view and edit content. This means that even if the same online product is used for another purpose in another part of the health board the default position is that content will be kept in each discrete 'bubble' with its own Site Owner.

6) Avoid tools that require downloads of software

Consider whether the extra functionality that comes from downloading software onto devices is really essential. Offline working and synchronisation are often pushed by vendors as key selling points but in many cases health board staff just need to be able to upload a completed document onto the site (or replace one document for another in the light of edits).

There are many products which do not require any downloads of software onto devices. This means that malware is far less likely to be picked up and then distributed across the network. Having the 'drop-box-type' virtual folder installed can also mean less care is taken on what documents and emails actually need to be uploaded (i.e. a kind of dumping ground for things which should only ever be stored on internal record systems).

7) Consider tools that offer more than password protection

Having a username and password offers little protection against the determined attacker. So it is recommended that tools are considered that require something in addition to this. In the case of nationally accredited tools with patient data this might be a token or require you to input a code sent to your mobile phone.

Check with the supplier that the pass-code/PIN etc that you insert when logging is encrypted when held on its system (at least to 128 bits but preferably 256 bits). Never use the same passwords or other credentials on these online tools that are also used for internal NHSScotland applications.

Avoid online tools which use a form of Single Sign On for multiple applications (e.g. "I log into my mail and I am also then logged into my document storage, my social media and analytical tool" etc).

Logging into the board approved online tool should be in order to carry out a single purpose relating to information sharing and storage.

8) Go for encryption at authentication and when stored

Given the vast number of tools now on offer it should be expected that encryption is used when the person authenticates (that is when the user is logging in and using the service) and ideally encryption for data at rest (when the data is not in use but simply stored by the provider). This minimises greatly the risk of data being captured while it is on the move (e.g. you are sitting in a wireless hotspot and want to check a document online) and reduce impact if the site is successfully hacked into (i.e. confidentiality and integrity of data maintained).

9) Use 'Favourites' and view links with suspicion

Given the number of bogus web sites out there, and the sophisticated targeted attacks on NHS staff, users should save the URL of the online sharing tool to their favourites and get into the habit of clicking on this each time they wish to use it. In the short user guide it needs to be clear what a legitimate link to a document looks like. If you receive an email from someone you do not recognise or with a title line or content from someone you know that makes no sense (even if it is an official NHSScotland email nhs.net or nhs.uk address with what looks like a link to a popular online tool) do not click on it. This will minimise the risk of downloading malware and also of uploading content onto a spoof site.

10) Check if authentication is required to open links

One of the advantages of online tools is that a colleague not on the board network can be emailed a link to voluminous project documentation rather than receive large attachments. Another is that if the email is sent to the wrong address then the information cannot be read (unless the recipient has logon details to the online site). At planning stage it needs to be checked how far these links can be opened and documents viewed without the user logging in (i.e. the permissions are driven by linking the email address with list of persons registered and authorised to access the information). It is more secure if a user receiving the link also has to authenticate to the service (i.e. their identity is based on their username, password and other credentials per session and not their email address).

11) Agree on consistent way of uploading

Rather than installing software on to devices, users can instead create a temporary folder on their device or network drive which is designed to hold things to be uploaded onto the online site (e.g. Documents for project x on SharePoint). This staging post means the user has to think carefully about what specific documents should be uploaded rather than attempting bulk uploads from folders across the corporate network/EDRM that may contain patient or sensitive corporate data.

12) Check how far data is deleted completely

Good information management on the part of the site manager, which includes regular deletion of redundant versions of documents (and most importantly a process to close down or archive the site when it is no longer required) is the best way to ensure compliance with

legislation such as the Data Protection Act. However, it is highly likely that the provider may still hold vestigial content or metadata for varying periods even after deleted by the user.

The extent of this supplier retention of data needs to be checked prior to signing up to the service. For local tactical solutions, non-patient identifiable and corporate data, the risk may be marginal and acceptable.

In the case of nationally accredited tools the contract would make clear what the supplier can maintain for an agreed period.

13) Follow mobile data encryption standard

Often a great deal of thought has gone into the technical security of the chosen online document storage tool but not of the end-points that are used to connect to it. If the tool does allow offline working for example then does the mobile device that is holding official NHS material have suitable encryption (as laid out in NHSScotland Mobile Data Standard)?[2] And if the health board employee is able to use personally-owned mobile devices and a home desk top computer to connect to the online tool then does this mean that health board data will end up on those devices? Is there a risk that the user may have installed features (e.g. Java on the browser) that means an attack (such as capture of credentials) is far more likely? Such issues need to be determined at the outset between board and site owner.

14) Never use online tools as back-up

In our personal lives it is common to think of these online storage tools as some kind of back up (e.g. “I put all my family photos and university notes up there in case my PC is broken”). But this should never be the justification for using such tools in NHSScotland. Each health board has its own arrangements for back-up of corporate and clinical information. The primary business justification for using online tools in the health board is to make available information to those who would otherwise have difficulties getting it (and NOT as some kind of private convenient back-up).

[2] http://www.ehealth.scot.nhs.uk/wp-content/documents/Revised-mobile-data-standard-May-2012-2.pdf

15) Never use online tools for mission critical activities

Users of such services have no control over the availability of service. For this reason the purposes should not be critical. Outages of hours or days may cause inconvenience ("my co-researcher cannot see my latest academic paper") but not loss of key business functions.

Even where national accredited tools are used (which have formal contracts on level of service) it is likely that they would be used only for corporate (e.g. e-procurement, knowledge management tools, some messaging) but not clinical applications.

16) Check in which country data is held

In the case of 'amber' corporate information and non-identifiable patient data it is advisable to only use tools that hold data in the European Economic Area (EEA) or where a Safe Harbor Agreement is in place.

In the case of nationally accredited tools that hold patient identifiable data there will need to be a formal contract that can demonstrate that the data will be held in the UK (or subject to negotiation the EEA) at all times.

17) Check privacy statements relating to use of data

It is common for online tools to state they would not share client details, or the content saved onto the site, with third parties. But small print does often allow the company (or one of its partners) to run analytical tools over the data. These typically pick out words and characteristics that allow all kinds of profiling (mainly for marketing).

In the case of national accredited tools firm assurances would need to be given at contract stage. But in the case of local tactical tools for non-identifiable patient and corporate data the board will need to decide on how far this activity is acceptable given the wider benefits.

18) Make staff aware of risk mixing personal with board material

Some professionals may wish to set up e-log books and document storage tools online in order to better manage their training and professional affiliation. No patient identifiable information (including identifiers such as CHI) should be used in such cases. If a clinician does upload personal data (e.g. from a private practice and/or health board) then he/she

may become a Data Controller in his own right and subject to compulsory notification with the ICO and other requirements. This would mean that should any breaches occur then he/she could be liable.

19) Do not encrypt files prior to saving onto site

There is no need to manually encrypt individual documents before uploading them onto the online site. In fact doing so can cause problems down the line (i.e. no longer available to staff who need them, encryption key lost etc). Instead, it is better to ensure that the tool's own encryption at authentication (and when the data is stored) is used.

20) Check web security architecture

When an off-the-shelf online tool is selected for local tactical purposes it can be very difficult to get detail from suppliers on their exact web-architecture and security (i.e. there is often no formal contract and you only have their marketing blurb to go on). Firstly, one is looking for the smallest possible surface area from which an attacker can attempt to break into the data store that will hold your NHS board (and other customers') information. Can the supplier state categorically that the *only* way into the data store is via the secure authentication page (i.e. where you insert your name, password or other credentials)? If the online tool also has associated web-pages for guidance/help, blogs, feed-back forms, messaging etc, you will need to check that this content is managed completely separate from the core data store that holds customer documents. Hackers often attempt to circumvent the usual login pages and look for a back-door that allows them in.

21) Is it knowledge sharing, document sharing or both?

The boundaries are now getting blurred between online tools that do document sharing/storage, knowledge management, collaboration and social networking. Most marketing information from companies will suggest they can solve all of the above in one product suite. In reality, some tools are better at some functions (and the security related to them) than others so it needs to be clear at design stage what the exact board business requirements are. If for example the key driver is making available a high volume of sensitive corporate documents to committee members across Scotland, then it would not make sense to simply opt for a big-brand product that is better known for knowledge sharing (i.e. chat, threads, blogs, surveys etc.).

Annex A: Some common scenarios and steps taken to manage risk

1) Request for a national online document storing and sharing tool holding elderly patient personal data
2) Request for survey/questionnaire functionality for members of staff across NHSScotland to use
3) Request to use an online tool to hold sensitive information relating to maternity
4) Clinician employed by health board needed to share data and documents online with other clinicians on a research project
5) Project team and numerous suppliers collaborate
6) Request from the Management Board to share documentation with non-executive members online
7) Community mental nurse asked IT to allow access to an online document sharing site to store notes while on the move
8) Clinician uses an e-logbook to store information required for professional accreditation
9) Query from clinician about whether his patients should use an online tool for hearing tests

Use of national accredited tools

1) Request for a national online document storing and sharing tool holding elderly patient personal data

There was a particular need for hospital clinicians and staff in social services to share certain information, including personal data, on elderly patients. The information typically contained a) CHI number and patient demographics such as name, address and age; b) housing, transport and support needs such as 'meals on wheels'; and c) some mention of the physical and mental state of patients (but not medical records). The staff were on different IT networks and used different applications to hold the data. There was a concern that in order to get around this problem staff might start using off-the-shelf consumer document sharing tools anyway (if they were not all blocked by local IT policy) or insecure email methods. There was no appetite for an expensive data sharing tool.

- The national guidance made clear that these online document sharing tools should **not** be used by staff in an ad-hoc manner for personal identifiable patient data (and only for corporate information up to 'amber' if certain conditions are met). However,

there was one important exception to the rule: this is where tools are formally accredited at a national level for a specific purpose.

- The health boards decided to go down this formal national accreditation route as the online option would be far more effective than trying to put in N3 connections or some other tactical IT workaround.
- Once it was clear that the parties had information sharing protocols in place, the sensitivity impact of the information (individually and in bulk; which was at 'amber') and the business requirement (i.e. whether more document storage and sharing or knowledge functionality etc) was understood, a formal contract was signed with an online document service provider.
- The type of service provided was 'enterprise level' and had more security controls (e.g. encryption, strong authentication) than the free consumer services could offer. The provider could guarantee that the data would be held in the UK at all times and could demonstrate it had acceptable personnel and data centre security. The tool was formally accredited by NSS, who manage national systems, in consultation with the Scottish Government.
- Even with all the above in place, the project team and accreditors made clear that this service had a security ceiling of 'amber' and could only be used for the specific purpose (i.e. not to subsequently be used for data which individually or in aggregate was of a higher sensitivity such as medical records on the elderly patients).
- The sites created had clear owners, who were responsible for ensuring the correct users are enrolled and that the records management policies were adhered to.

2) Request for survey/questionnaire functionality for members of staff across NHSScotland to use

Various departments in more than one health board, including HR and Finance, intend to run more regular surveys of staff on a range of subjects. Up until now they have either been strictly internal (i.e. via board Intranet) or off-the-shelf 'Survey-Monkey-type' survey tools have been used when circulation has been across NHSScotland. The problem with the latter is that in some boards access to them is restricted. After advice the following action was taken:

- A suitable online tool was selected, and then arrangements were made for a single instance of the software to be hosted within NHSScotland, this meant that the actual

data was controlled and accessed only by those who have access to the network (i.e. a private cloud model on N3).

- The result was that the questions, and subsequent responses, could be of a slightly more sensitive nature up to 'amber' (e.g. staff telling management what they think of x and y) than would be the case with ordinary public tools.

3) Request to use an online tool to hold sensitive information relating to maternity

A board wanted to replace its maternity record filing system (currently held on paper) with something that health workers, and some social workers, within the board's geographical area could see and update online. One senior clinician had heard of a public cloud tool called 'MybigcareStore' and suggested purchasing it. The following action was taken:

- Firstly, a review was made of the exact nature of the data itself and what needed to be shared. There was agreement that the type of data captured in paper files could be pared back substantially to what they really needed to provide maternity care and which could be shared digitally (as opposed to what a patient might keep about themselves outside the NHS on social media-type tools).
- The board worked with those agreeing a national template (i.e. every maternity record should have x, y, and z fields) so that there would be consistency across Scotland.
- It was decided that a 'MybigcareStore' type approach was neither needed nor desirable. The type of data (even with the paring down) was of a highly sensitive nature (e.g. past sexual health, miscarriages and social care notes on child protection flags) and given current risks was better held locally within GP practices (or health-board data centres that serve a consortia of GPs) rather than some central cloud-based data centre.
- Although a distributed rather than public cloud option was chosen, the outcome for the staff was the same: i.e. all the health participants in the board area could access the patient information online by logging into either of the existing applications used by GPs.

<u>Local tactical online solutions</u>

4) Clinician employed by health board needed to share data and documents online with other clinicians on a research project

A clinician needed an ad-hoc way to share information and knowledge with practitioners in dermatology who are scattered all over the UK and in Europe. Although this research work was not core to his day-job and not funded by the health board, the management took the view that this kind of collaborative research should be encouraged and assisted by the board. At the same time the board needed to consider how far both the clinician and health board were exposed to information risks and what can be done about them. The following action was taken:

- The Caldicott Guardian and IG panel were consulted about the scope of the data to be shared in this ad-hoc manner (i.e. not part of any formal project).
- After deliberation the board made clear that although it encouraged the research it would not be permissible for any identifiable patient data from the health board to be used and shared in this way. Instead, the clinician would need to take sufficient steps to anonymise the data that originated from the board. Guidance on how to do this was offered.
- It was established that the nature of the sharing was informal and ad-hoc and tended to be in the form of spread-sheets (e.g. showing number of cases each month that would reveal nothing about an identifiable individual) and conversation strings (i.e. observations about symptoms). Many of the participants were outside the NHS and not on N3. Therefore an online collaboration and document sharing tool was recommended in preference to other options (e.g. file sharing protocols and use of email). The clinician was given access to the chosen site while logged on at work (and he could also use the tool from his personally-owned devices). He was given a copy of the board information and records management policy.

5) Project team and numerous suppliers collaborate

A project team wanted a collaborative space, to share large documents as well as conversation strings, with people working for IT suppliers, a charity for older persons' health and the NHS.

- It was ascertained quickly that no patient data was to be shared. But the corporate documentation did have some sensitivity while the project was running (e.g. some company financial data, risk assessments and registers etc that could have a FOI exemption if requested).

- An off-the-shelf tool was selected and a site owner appointed. She was responsible for adhering to the board information and records policies.
- Other controls suggested in the national guidance were put in place (e.g. tool with encryption at authentication and storage; simple permissions etc).

6) Request from the Management Board to share documentation with non-executive members online

The board found that there was no easy way of ensuring non-executive members and other external participants could receive the often voluminous documentation produced by the board. Printing and sending by paper mail or via email were not ideal (not least because much of the information has some corporate sensitivity and cannot be sent to ordinary email accounts). It asked the IT department to come up with an online alternative.

- In line with national guidance, it was agreed that the use of such tools should only be for information no higher than 'amber' [broadly equivalent to PROTECT in HMG]. It needed to be clear that any corporate information above that level needed to be sent via other secure methods. And that no patient data was to be included.
- The online tool selected required a payment for a license to use one 'site'. The data was held at a data centre in EEA and there were some reasonable assurances as to availability etc. The tool also had a simple set of permissions (involving sending a link to someone who then needed to be able to logon to see the document space) and did not require any software to be downloaded.
- The board insisted that there was an 'owner' of the site who would be responsible for inviting persons to join the collaborative space, to ensure that records management policies are adhered to (i.e. that the site will only hold copies).

7) Community mental nurse asked IT to allow access to an online document sharing site to store notes while on the move

An almost qualified community nurse was required to take notes while out visiting and asked the board IT department if it could enable her to download Google Docs (or similar) onto the official tablet device used during the training period. The following action was taken:

- He was shown a guidance document that made clear why this was counter to policy and all the information risks associated with it.

- The contingent worker was reminded that simply by-passing the policy (e.g. downloading the tool onto his personally-owned device and saving documents from there) would be a breach in policy and could lead to disciplinary action.
- At the same time he was asked to give feed-back on how easy (or not) it was to write up notes as the board intended to roll out a mobile version of its community mental health application that would make life easier for all concerned.

Personal/professional use

8) Clinician uses an e-logbook to store information required for professional accreditation

Clinicians started to use various online tools to store information relating to their accreditation/training (e.g. 'e-log book-type' sites). Although not strictly a health board matter, there is the risk of the board being drawn into a breach (e.g. if identifiable patient data from that board was used and wrangles over who is the Data Controller etc). The board takes the following action:

- Issued guidance making clear that patient identifiable information, including identifiers such as CHI, should not be used on such sites.
- Made clear that if a clinician does use any personal data (e.g. from work in private sector for example) then he may be acting as a Data Controller in his own right and would need to seek his own legal advice. If there is a subsequent breach then the individual (not the board) would be liable.
- Issue general guidance on how to reduce information risks when using such sites (e.g. password strength, use of reputable sites based in UK and endorsed by professional bodies).

9) Query from clinician about whether his patients should use an online tool for hearing tests

A hearing specialist employed by the health board found that there were some excellent online tools developed in the USA that his patients could use at home in their own time to carry out hearing exercises. He asked whether using the service to support care (which might also involve taking out licenses) would make the boards liable under DPA if something went wrong.

- After discussing the matter with the Caldicott Guardian and eHealth lead it was felt that formally licensing the tool or just using the service would mean that the board could become liable for many aspects (including as a Data Controller). Or at the very least the patient may perceive that this is a NHS approved service.
- It was decided that the best course of action would be to inform patients that such online tools did exist; and that it was their personal choice if they wished to avail of them (but they were not connected or endorsed in any way by NHSScotland).
- At the same time the patients were given a link to Getsafeonline.org, or similar guidance, so that they could think about how they use non-NHS health-related online tools.

Annex B

What is the sensitivity of the information in NHSScotland?

All NHS information should be handled with care, especially that which contains personal data. But some types of information are more sensitive than others.

Deciding on which online model should be used (i.e. local or nationally accredited solution), depends on the relative sensitivity of the information and the impact that would be caused if the information were lost or misused

Three levels can be used to describe the information which the NHS holds. For simplicity these can be viewed like traffic lights: **'Green', 'Amber'** and **'Red'.**

GREEN: Unclassified information

This is information which is unlikely to cause distress to individuals, breach confidence, or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person's name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person's physical or mental state.

AMBER: Protected information

In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

- Any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost.
- Any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result).
- Any corporate non-patient information if lost that would be likely to negatively affect the efficiency of that service (e.g. cancellation of appointments) and is considered to have some sensitivity (e.g. might reasonably be subject to a FOISA exemption).

RED: Highly sensitive information

Most boards also hold some information which is highly sensitive. Particularly:

- Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way).
- Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health.
- Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file).
- Information relating to vulnerable persons' health (e.g. child protection cases).
- Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment).
- Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

DMB