BDA

British Dental Association

BDA advice

Protecting personal information
Data protection, including GDPR

Date: June 2019

Protecting personal information
Data protection, including GDPR

Contents

Overview

The Data Protection Act 1998 established a framework of rights and duties to safeguard personal information and balance the legitimate needs of organisations to collect and use personal information again the right of individuals to have the privacy of their personal details respected.

Much has changed since 1998. We now give a lot of information about ourselves to a lot of organisations, usually willingly but frequently unknowingly. Quite often we don't know what happens to this information, how it is used and how decisions about us are made. The General Data Protection Regulation 2018 (GDPR) makes organisations more accountable in the way that they collect, use, store and dispose of personal information and gives individuals more control over information about them that they pass onto others.

Many of the general data protection requirements are unchanged and the need to comply continues. However, now if you hold personal information, you must be able to explain what information you have, why you have it, what you do with it and who you share it with, in addition to the general need to protect it by

- Only collecting information that you need for a specific purpose
- Keeping it secure
- Ensuring that it is relevant and up to date
- Only holding as much as you need and only for as long as you need it, and
- Allowing the subject of the information to see it on request.

Personal information

As a dentist in general practice, you will handle and store personal information about your patients and existing and prospective members of your team. Personal information is any information that allows an individual to be identified and can include anonymous data if it can be easily linked to an individual. It can also include opinions about and proposal for an individual – for example, patient treatment proposals and employee appraisals and performance records.

Controllers and processors

A controller determines the purposes and means of processing personal information. The role is usually undertaken by the practice owner who can be an individual dentist, a partnership or a corporate body. If you work in an expense-sharing arrangement that is not a legal partnership, each expense-sharing dentist will be a data controller. Self-employed associates, using the practice computer or the practice filing system for storing patient records, are not controllers.

A processor is responsible for processing personal information on behalf of the controller; self-employed associates are processors. Processing simply means doing something with the information – for example, collecting or recording it, organising, storing, retrieving, disclosing or destroying it. Employers remain responsible for how their employees process information obtained in the course of their work; the need to follow practice data protection policies should be included in employment contracts.

Data protection fees

A controller must pay the Information Commissioner's Office (ICO) a data protection fee, unless they are exempt. This replaces the previous requirement to 'notify' or register with the ICO if information was processed electronically.

Data protection fees are set annually by the ICO and are based on staff numbers and annual turnover:

- Tier 1: maximum annual turnover of £632,000 or no more than 10 staff members (£40 fee)
- Tier 2: maximum annual turnover of £36m or no more than 250 staff members (£60 fee)
- Tier 3: if you do not meet the criteria for Tier 1 or Tier 2 (£2,900).

'Staff members' is defined broadly to include employees, workers and partners; each part-time staff member is counted as one member of staff. Although associates engaged under a BDA template associate contract do not fit the ICO's definition of staff members, for the purposes of calculating the right tier and data protection fee, they should be included (as should self-employed hygienists and therapists). This may result in a tier 2 fee rather than a tier 1 fee, but it avoids a potential penalty fine of £4,350 should the ICO take a different view on the status of associates.
The ICO will assume that you fall into Tier 3, unless you tell them otherwise (by email or phone) quoting your security number and reference number.

If you have a current registration (or notification) with the ICO, you will not need to pay the new data protection fee until your registration expires.

Exemptions
You do not need to pay a fee if you are processing personal information only for one or more of the following purposes:

- Staff administration (pay, superannuation and personnel matters)
- Advertising, marketing and public relations
- Accounts and records relating to the practice
- Or you are processing personal information without using a computer.

Data protection principles

The data protection principles require personal information to be

1. Processed fairly and lawfully
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and not excessive
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than necessary
6. Kept secure.

You must be able to show compliance with these principles through your practice policies and procedures.

1. Fair and lawful

You must process personal information fairly and lawfully. Fairness requires you to be transparent – be clear and open with individuals about how you will use their information.

There are six lawful bases and at least one must apply and be cited in your practice policies and protocols, impact assessments, and patient and staff notices.

a) **Consent**: the individual has given clear consent for you to process their personal information for a specific purpose – for example, if you collect information for research. It is not appropriate for the provision of patient care or managing staff, where records are integral to the provision of treatment or employment.

b) **Contract**: this is a lawful basis if you need to process someone's personal data to fulfil your contractual obligations to them or they have asked you to do something before entering into a contract. This is an appropriate reason for keeping patient and employee records.

c) **Legal obligations**: this is a lawful basis if you need to process personal information to comply with a statutory obligation (not a contractual one) – for example, GDC standards, NHS regulations, tax law.

d) **Vital interest**: the processing is necessary to protect someone's life. This is unlikely to be a relevant reason in dental practice.

e) **Public interest**: the processing is necessary to perform a task in the public interest or an official duty, and the task or duty is a legal requirement. This could apply with processing NHS information and your policies or impact assessments must show this to be a more appropriate reason than contract or legal obligations bases.

f) **Legitimate interests**: the processing is necessary for your legitimate interests (or the legitimate interests of a third party) but you must consider and protect the individual's rights and interests. This cannot be used for processing NHS information in relation to NHS care, but you can use it for processing information about private care. You must identify a legitimate interest, show that the processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms. You should keep a record of your legitimate interests' assessment to demonstrate compliance (if required). This would be an appropriate basis for sending out patient recalls to NHS and private patients.

You must be able to show that you have properly considered which lawful basis applies to each type of processing and can justify your decision. You should keep a record of each type of processing that you undertake, the lawful basis for it and how you have decided this.

Special category information

Special category information includes information about race, ethnic origin, political opinions, religion, trade union membership, genetics, biometrics, health, sex and sexual orientation. It includes patient records and, depending on the information you record, can include staff records.

In addition to identifying a lawful basis, you must identify a separate condition for processing special category information. For processing patient records, the condition is likely to be 'health care'. Where you are involved in passing information to an indemnity or insurance provider, the condition is likely to be 'for the establishment, exercise or defence of legal claims'. The legal basis and condition should be stated in your practice policies and protocols and any associated documents or paperwork.

To be processed fairly, you must give the individual (a patient, employee or self-employed contractor, for example) a Privacy notices explaining why you are collecting the information and what you intend to use it for.

2. Purposes

You must only collect personal information for a legitimate purpose and process it in line with the reasonable expectations of the individual. You should be open about your reasons and give a privacy notice when collecting the information to explain what personal information is held by the practice and why, and how it will be used.

3. Adequacy

You must only collect personal information for the purpose stated in the privacy notice and ensure that the information you collect is sufficient for this purpose; you should not hold more information than you need or on the off-chance that it might be useful sometime in the future.

If the information insufficient for its intended purpose, you should not hold it. For example, if the quality of CCTV images is so poor that identification is difficult.

4. Accuracy

The information you hold must be accurate and up to date. You should take reasonable steps to ensure that any personal information you obtain is not incorrect or misleading. Where personal information has been provided by someone else, you should take all reasonable steps to ensure its accuracy. If, for example, you receive information from a referring dentist, confirm with the patient that the information is accurate. Inaccuracies must be corrected without delay.

Opinions are frequently recorded in patient records as part of an initial diagnosis and form part of the individual's personal information. The record should clearly indicate that it is an opinion. If the diagnosis is later found to be incorrect, both records should be retained; the original record reflects your true opinion at the time.

Records of events that happened in error should not be misleading about the facts. For example, if you dismiss an employee for alleged misconduct but an employment tribunal finds the dismissal unfair and reinstates the employee, you should keep your record of the dismissal but amend it to reflect the tribunal's decision.

The need to keep personal information up to date depends on its purpose. Information for employee payroll purposes or patients' medical histories, for example, must be updated regularly.

5. Retention

Personal information should not be kept for longer than is necessary for the purpose you obtained it. You must dispose of any information that is no longer needed, reducing the risk that it will become inaccurate, out of date or irrelevant.

You should review the length of time that you keep personal information, consider your reason for collecting it and its current and future use. Information that is no longer needed, should be securely deleted. If you use a commercial company, you must have a written agreement that describes their obligations to comply with data protection rules and ensure secure disposal arrangements.

6. Rights

Right to be informed

You must tell people what information you hold about them and their rights, typically through a privacy notice given when you first collection information.

Right of access

Individuals have a right to access their personal (and supplementary) information and to get copies.

- You must provide a copy of the information without delay, and within one month of receiving the request. If the requests are complex or numerous, you can extend the deadline by two months, but you must explain this to the individual within the original one-month limit.
- You must provide the information free of charge. However, if the requests are unfounded or excessive (because they are repetitive), you can charge a reasonable fee or refuse to respond. You can also charge a reasonable fee for further copies of the same information. The fee must be based on the administrative cost of providing the information. If you refuse a request, you must do so within one month, give a reason and inform the individual of their right to complaint to the ICO or to seek another legal remedy.
- You must provide the information in a way that is useful to the individual. If the request is made electronically, you should provide the information in a commonly used electronic format. You may need to provide a password-protected file, if the individual does not want to receive a standard email. If requested, you should provide a physical copy of the information. You may need to include an explanation to the clinical notes.
- You must only provide personal information to the individual it concerns so check their identify (confirmation of name, address and date of birth). For electronic requests, you will need to satisfy yourself that the request has been made by the individual concerned.

The right of access applies to individuals aged 16 years and older. If you receive a request from someone who is younger, you must assess their mental capacity and understanding to determine if they have a right of access. Where a parent or guardian makes the request and the child is capable of making the request, you should seek the child's consent. If the child is sufficiently mature to understand their rights, you should respond to the child rather than the parent. Do not give access to a parent or guardian where the child has expressly indicated otherwise or has provided the information on the basis that it would not be disclosed.

Right to rectification

Individuals have the right for information to be corrected if it is inaccurate or incomplete. You must respond to a request to correct information within one month; this can be extended by two months if the request is complex. If you do not agree with the requested corrections, you must explain why and inform the individual of their right to complaint to the ICO or to seek another legal remedy.

Right to erasure

An individual can ask you to delete their personal information. You should comply unless you still need the information for the purpose it was collected – for example, the need to keep patient records for 10 years would allow you to reasonably reject a request from the patient to delete the records two years after the last treatment, but you could comply with a request to delete an email address.

Right to restrict processing

An individual can ask you stop processing personal information – for example, if they are contesting its accuracy or they want to prevent you from using or destroying it. You should continue to store it without further processing until you know whether you need to comply with the request.

Right to data portability

This allows individuals to move, copy of transfer their personal information to another practice. You should comply with the request within one month and, where possible, ensure that the information is transferred safely and securely and in a way that can be used by the new dentist (software providers may have systems that will facilitate this transfer). You should keep copies of the transferred information to comply with recommended retention periods.

Right to object

Individuals can object to their personal information being used for direct marketing, profiling and research. They cannot object to its use for a legitimate purpose such as keeping clinical records.

Rights related to automated decision making including profiling

Automated decisions are those made without any human involvement, which can include profiling. Examples include using software systems to analyse identifiable information – for example, recruitment aptitude tests that use pre-programmed algorithms. The individuals involved must be informed and be given the opportunity to request human intervention or challenge a decision.

7. Security

You must have appropriate security to protect personal information against unlawful or unauthorised processing and accidental disclosure or loss. All members of the team must understand the need to keep information secure and be well-trained in your policies and procedures. You should keep a list of staff who have access to the various types of information held at the practice (and why) and keep the list updated.

Personal information should never be left unattended. Personal health information calls for a high level of security because of the potential damage that could result by unauthorised disclosure.

- Manual records should be stored in lockable, fireproof cabinets and the premises should be protected to prevent entry by intruders.
- Computerised records should be protected by passwords known only to essential staff.
- CCTV recordings must be stored securely and in a way that maintains the integrity of the image. You should restrict access to the images and delete those that are no longer needed.

Your practice risk assessment should consider the risk of access to personal information by unauthorised individuals and resulting from unauthorised entry.

8. International

Personal information must not be transferred to a country outside the EEA unless the country can process the personal information in a way that protects the individual concerned. Service companies may transfer personal information to another country for processing – for example, employee pay-roll activities or internet service providers. Check the company's arrangements for processing information and, if this involves transfer outside the EEA you should confirm with the ICO that the location has adequate and recognised data protection laws.

Demonstrating compliance

You must be able to show that you comply with the data protection principles for the types of information that you hold and manage. For example, patient contact details, clinical records, study models, radiographs, correspondence, staff contact details, employment contracts, pay and absences.

- Establish your lawful basis for processing the types of information that you deal with – for example, contract, legal obligations or, for private dentistry, legitimate interests. For special category information, you will also need to establish a separate condition – for example, the provision of health care (for patients), obligations under employment law (for employees), or the defence of legal claims (patients and employees).
- Keep a record of the information you collect, record, organise, store, retrieve, disclose or destroy.
- Maintain a list of those involved with processing information and how.
- Have written contracts with those involved with processing information (employees, associates and third-party providers) to ensure that they understand their responsibilities and liabilities.
- Record only the information that you need and, where circumstances permit, anonymise it.
- Provide privacy notices to patients, staff and associates.
- Appoint a data protection officer (where NHS care is provided).
- Carry out an impact assessment if you are introducing new technology.

Privacy notices

Under an individual's right to be informed, you must provide a privacy notice describing your lawful basis for processing their personal information (collecting it, using it, storing it and disposing of it, for example). When processing special category information, you must identify both a lawful basis for general processing and an additional condition for processing this type of information.

You must provide privacy notices to your patients, your employees (including prospective employees) and self-employed contractors. They must be easy to understand and be given free of charge. A privacy notice should include:

- A statement that the practice processes personal information
- The type of information that you process and why
- How you use the information, how you store it and your security arrangements
- How long you keep it
- Your criteria for disclosing information
- The identity and contact details of the controller and, if relevant, the data protection officer
- How the individual can access their information
- How the individual can complain about the use, storage or disclosure of their information.

Expert template privacy notices are available.

Written contracts with processors

Where the processor works at the practice (an employee, associate, or partner), the written contract requirement can be fulfilled by amending existing contracts.

For third-party processors (for example, companies providing pay-roll services or IT support and storage), your written contract must include the following details and terms:

- The information being processed and for how long
- How the data is being processed and why
- The type of personal information and individuals
- Your obligations and rights (as the controller)
- The processor must:
  - only act on your written instructions
  - take appropriate measures to ensure secure processing
  - only engage sub-contractors with your prior consent
  - assist you with subject access requests
  - assist you to comply with your data protection obligations
  - delete or return personal information when requested
  - allow audits and inspections.

Data protection officer (DPO)

If you provide NHS care, you are defined as a public authority and must appoint a DPO. If you do not provide NHS care, appointment of a DPO is discretionary.

The role of a DPO is to:

- Inform and advise you about your obligation to comply with data protection requirements
- Monitor compliance and manage internal data protection activities, advise on impact assessments, train staff and conduct internal audits
- Act as the first point of contact for individuals whose data is processed (employees, associates, patients).

A DPO must be sufficiently independent of the information processed at the practice to be able to undertake their duties responsibly. A practice manager, for example, with the right training should be able to fulfil the DPO function. You can also decide to outsource the function.

Impact assessments

A data protection impact assessment can help you to identify the most effective way to comply with your data protection obligations and meet privacy expectations. Generally, you are unlikely to meet the criteria that make an impact assessment mandatory unless you introduce new technologies that involve processing personal information – for example, a new software package for processing the personal information of patients or employees or introducing CCTV throughout the practice.

An impact assessment involves:

- Describing the processing activities and the reasons for them
- Assessing the necessity and proportionality of the processing in relation to the purpose
- Assessing the risks to individuals and how you intend to address these.

Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. You must report a breach to the ICO within 72 hours of becoming aware of it, unless you are satisfied that the breach is unlikely to result in a risk to people's rights and freedoms. If you do report a breach, you must and explain how it happened, the number of people affected the likely consequences and how you are dealing with it.

In assessing the risk, you must consider the potential negative consequences to the individual: loss of control over the information; discrimination; identity theft or fraud; financial loss; reputation damage; or loss of confidentiality.

If you decide that you do not need to report the breach, you must be able to justify this decision and have documented it.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, you must inform them as soon as possible to allow them to take steps to protect themselves from the effect of the breach.

Practice policies

Practice policies and protocols will help you demonstrate compliance with data protection requirements and introduce effective systems in your practice. Policies and protocols provide a useful training resource and can help those working at the practice to understand their responsibilities. Relevant policies include your confidentiality policy, your records management policy and your data security policy. Expert templates are available.

Employing staff

Data protection requirements apply to information you hold about your past, current and prospective employees and self-employed contractors. You must provide all members of your team (and prospective members) with a privacy notice describing how you will process their personal information.

Recruitment and selection

When recruiting staff, you need to balance your need for information against an individual's right to privacy. Applicants should know what information you are collecting and how it will be used. You must not gather information covertly.

- Recruitment adverts must identify your practice.
- The information provided by applicants must be used only for selection and recruitment; do not ask for more information than you need.
- The applicant should be told of any checks that you need to make. Although you do not need consent for employment checks, the applicant must be able to withdraw their application if they do not want you to carry out the checks.
- Information necessary for employment (bank details, for example) should only be requested when an offer of employment has been made and accepted.
- Keep recruitment information for only as long as you need to, say 12 months from when the new employee starts. A claim through an employment tribunal should be raised within three months but, in exceptional circumstance, this limit may be extended.
- For successful candidates, the information you obtain at recruitment (about their skills, qualifications and experience) forms the basis of their employee record.

Employment records

You must only hold information that is necessary for employment – for example, name and address, pay-roll information, leave and sickness records, appraisals and any disciplinary or grievance procedures. You can disclose information that is required legally – for example, by HMRC – but you should not disclose more than is needed. Only provide confidential references if you are confident that the ex-employee has proposed you down as a referee. If in doubt, speak to the ex-employee first.

All personal information must be kept secure (locked away or password protected). Sickness records and information about medical conditions is sensitive personal information and, where practicable, should be kept separate.

Periodically review the information that you hold about your employees and self-employed contractors to ensure that it is accurate and up-to-date and is no more than you need. Information that is no longer needed must be disposed of securely. Be aware that contractual claims can be submitted up to six years after the event, providing a useful guide to retention. Personal injury claims should be made within three years but can be submitted beyond this time if the individual only becomes aware of it a later date.

Employees have a legal right of access to any personal information that you hold about them, including information about grievance and disciplinary issues, and information obtained through monitoring.

Monitoring employees

Monitoring employees is not prohibited but any potential adverse effect on the individual must be justified by the benefit that will result. You should use the least intrusive method and consider target monitoring.

If you use monitoring, everyone should be aware of the nature, extent and reasons for it, and know what is expected of them; there are few occasions when covert monitoring is permissible. You can only use information obtained from monitoring for the purpose it was carried out, unless it reveals activity that puts others at risk. Monitoring is rarely justified and must not be used in private areas, unless the police are involved and advise it.

Patients

All information obtained in the course of caring for patients is confidential, including that an individual is a patient at the practice. Confidentiality must be maintained even when a patient dies.

Personal health information is classified special category information and includes: clinical notes and medical histories; radiographs and study models; information held in appointment booking systems; financial records, NHS forms, exemption status; and video and audio tapes, photographs and medical illustrations.

You must ensure that all members of the team understand the need to protect personal health information and what this means in their day-to-day work at the practice – for example, not talking about patients in places where they might be overheard by those who should not have access to this information. Those working at the practice reception area must take care to avoid disclosing a patient's identity alongside other personal information. The need to maintain confidentiality should be included in your contracts of employment and agreements with self-employed contractors. Expert template contracts and agreements are available.

If you provide NHS care in England, you must also comply with the requirements of the NHS Digital Data Security and Protection Toolkit.

Sharing information

Your privacy notice should also explain that you may share a patient's personal health information with other team members and other healthcare professionals if, for example, you need to refer them for specialist advice and treatment. Issuing prescriptions, laboratory work and NHS or private dental plan paperwork also need information to be shared.

Identifiable information should only be shared on a need-to-know basis and, where possible, anonymised (by using reference numbers and codes). For example, when sending work to a laboratory, you do not need to identify the individual. Removing obvious identifying information does not alter the need to observe confidentiality; health information or circumstances may be sufficient to reveal a patient's identity.

Teaching and research

If you share information for research and teaching purposes that identifies the individuals, your lawful basis for processing information must reflect this.

So, for example, your legal basis for processing personal information might be 'consent' and your specific conditions for processing special category (sensitive) information might be 'provision of health care', 'public health interests' or 'scientific or research' purposes. Your patient privacy notice should reflect this.

Health research involving access to patient records must be approved by a local Research Ethics Committee. Applications must be made through the online gateway. Further information on ethical approval for research within the NHS is available from the National Research Ethics Committees

Photographic images

If you take and use photographs of your patients, say for academic or marketing purposes, you must obtain the patient's explicit consent in writing, which should be freely given and unambiguous. The patient must be told why you want the photograph, how it will be used and who will use the image.

If you have more than one use for the photograph, you must obtain the patient's consent for each use. Over time and as circumstances change, consent loses its validity, so it must be renewed. The patient must know that they can withdraw consent at any time.

Mobile devices such as phones, tablets and iPads are not secure and should not be used for taking images of patients.

Patient records

Practice systems should allow you to identify patients who have not returned to the practice or have died. Bearing in mind that you should not hold more information than is reasonably required, you should dispose of any records that you no longer need to hold.

The law does not stipulate a period for retaining records. The NHS recommends that records should be retained for 10 years or until the age of 25, whichever is the longer. These timescales are consistent with those for bringing claims against the practice. You should review your records annually and delete those that exceed these time limits.

IT security

Keeping your IT systems safe and secure can be a complex task that requires time, resource and specialist knowledge. Personal information may be at risk and you need to protect it. The Government's National Cyber Security Centre's (NCSC) guidance for small businesses describes how you can significantly reduce the likelihood of your practice becoming a victim of cyber-crime.

No specific product will guarantee complete security and you will need complementary security controls with ongoing support to maintain an appropriate level of security. The NCSC cyber essentials scheme describes the following five technical controls for keeping information safe.

1. Use a firewall to secure your internet connection

A firewall creates a 'buffer zone' between your practice computers (your network) and the internet. Incoming traffic is analysed within this buffer zone to determine if it should be allowed onto your network.

There are two types of firewalls:

- A personal firewall on your internet-connected laptop, which is normally included as part of your operating system at no extra charge
- If you have several types of computer devices you might wish to set up a dedicated boundary firewall to create a protective buffer around your entire network. Some routers have a firewall that could be used to provide boundary protection. You should ask your internet provider about your specific router model.

2. Choose the most secure settings for your devices and software

Manufacturers often set the default configurations of new software and devices to be as open and multifunctional as possible to make them easy to connect and use. Default settings can make it easier for cyber attackers to gain unauthorised access to your information. Do:

- Check the settings of new software and devices and, where possible, make changes to raise your level of security – for example, by disabling and removing any functions, accounts or services that you do not need
- Use passwords on your laptops, desktop computers, tablets and smartphones and on any online accounts that you access. Devices store details of the online accounts that you access. Passwords – when used correctly – are an easy and effective way to prevent unauthorised users accessing your devices. Passwords should be easy to remember and hard for somebody else to guess. Default passwords that come with new devices (such as 'admin' and 'password') are easy for attackers to guess so change all default passwords before devices are distributed and used. The use of PINs or touch-ID can also help secure your device. More information on choosing passwords can be found in the NCSC password guidance
- Use extra security for important accounts, such as banking and IT administration. You should use two-factor authentication, also known as 2FA, which often involves a code being sent to your smartphone for you to enter in addition to your password.

3. Control who has access to your data and services

To minimise the potential damage that could result from an account being misused or stolen, you should restrict staff access to software, settings, and online services to the minimum required for them to perform their role. Extra permissions should only be given to those who need them.

Check the privileges of your accounts. Accounts with administrative privileges should only be given to those who need to adjust computer settings; standard accounts should be used for general work. By ensuring that your staff don't browse the web or check emails from an account with administrative privileges you reduce the likelihood that an administrative account will be compromised. An attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account.

4. Protect yourself from viruses and other malware

Malware is software or web content that has been designed to cause harm. For example, the recent WannaCry attack used a form of malware that makes information or systems unusable until the victim makes a payment. Viruses are the most well-known form of malware. These programs infect legitimate software, make copies of themselves and send these duplicates to any computers which connect to their victim.

Malware can find its way onto a computer by, for example, clicking on a link in an infected email, browsing a compromised website or opening an unknown file from removable storage media, such as a USB memory stick.

Protect against malware by

- Using antivirus software on all computers and laptops. It is often included within popular operating systems and only requires you to click 'enable'. Smartphones and tablets might require a different approach but, if configured in accordance with the NCSC's guidance, you may not need separate antivirus software
- Only downloading apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple Store). These apps are checked to ensure a certain level of protection from malware. Prevent staff from downloading apps from unknown vendors/sources, as these will not have been checked
- If you are unable to install antivirus or limit users to approved stores, a more technical solution is to run your apps and programs in a 'sandbox' to prevent them from interacting with, and harming, other parts of your devices or network.

More information on protecting against malware is available in the NCSC guidance 10 steps to Malware Prevention.

5. Keep your devices and software up to date

Phones, tablets, laptops and computers must have up-to-date operating systems, software and apps.

Manufacturers and developers release regular updates that add new features and fix any security vulnerabilities that have been discovered. Applying these updates (a process known as patching) is one of the most important things you can do to improve security. If available, set your operating systems, software, devices and apps to 'automatically update' to ensure that you are protected as soon as the update is released.

However, all IT has a limited lifespan. When you no longer receive new updates for your hardware or software, you should consider a modern replacement.

Other precautions

- You should make regular backups of the essential information that you need to keep the practice functioning, store them away from the computer and restrict access. Cloud storage separates your information from your location and can allow you to make backups automatically.

- In-house training to ensure that those using your IT systems are appropriately trained in the software used, your systems for security and best practice, and are aware of the risks and how to avoid them. Security breaches are most likely to occur because of lapses, errors or lack of knowledge by users.
- Encourage users to only visit reputable websites and to always check the web address – consider restricting access to a whitelist of acceptable websites.
- Only open emails from recognised senders and never click on links or open attachments that are not explained or look dodgy.
- Do not mix work and personal devices and email accounts.
- Monitor your IT and website logs and check that any changes are legitimate to help you identify attempts to hack into your systems.
- Periodically undertake penetration tests to assess the security of your computer networks and website.

Phishing

Phishing describes a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. It works because it exploits people's social instincts to be helpful and efficient (and hackers can make messages look trustworthy or familiar).

Email is an ideal delivery method for phishing attacks as it can reach users directly and hide amongst the vast number of benign emails that busy users receive. Phishing emails allow attackers to steal information, install malware (such as ransomware), sabotage your systems or steal money through fraud.

NCSC's guidance Phishing attacks: defending your organisation can help you to protect against malicious emails that use social engineering techniques.

Cloud storage

The NCSC's cloud security guidance will help you to evaluate the security of any cloud service and identify cloud services that are suitably secure for your intended use.

Cloud storage can bring many advantages in terms of affordability, support, processing power, storage capacity and backups. The information is managed by a third party and transmitted via the internet, but you continue to have data protection responsibilities. Use your privacy notices to inform individuals that their information is stored on a cloud and the measures in place to protect it

- Consider the information that you plan to move to the cloud and the impact on your business if it was lost, corrupted or stolen. Consider whether some information should not be cloud-based.
- Check the security measures of your cloud provider; ask for an independent security audit of their physical, technical and organisational security (reputable cloud providers should have this).
- Check that the provider encrypts information that is transferred to or from the cloud and stored within or moved around their system.
- Check whether the provider uses the information in any way – for example, to create statistics relating to your use of the systems – and whether you can object if the use is unsuitable. You may need permission from the individuals, depending on how their information is used.
- Monitor, audit and assess the cloud provider's service and security measures; audit trails should show who is accessing and changing the information.
- Access to the information should require a secure authentication process. You must be able to create or delete user accounts. If your provider requires access, you should understand their reasons and be confident that they will respect the need for confidentiality.
- Check how your provider deletes out-of-date or unwanted information.
- You must have a written legally-binding contract with the provider. You retain responsibility for how the information is processed and its integrity; it should only be processed following your instructions.

Emails

Email accounts require the same precautions as other IT services, but you should also consider the following when sending or receiving emails:

- Avoid sending sensitive personal information
- Obtain the recipient's permission to contact them by email
- Consider encryption – if the both the sender and the recipient subscribe to the same encryption service. This must be considered if you exchange clinical information with another dentist
- Use password protected files for personal information (this is insufficient for sensitive personal information)
- Use a web template for patients to contact the practice; it is more secure than an email inbox
- Label your email messages as private and confidential; it may act as a deterrent if someone receives a message accidentally. Your email footer should state that, although you take precautions to ensure email and internet security, messages could be targeted by hackers and that recipients must also take precautions to ensure that their use of email and the internet is secure.

If the message that you wish to send is extremely sensitive or confidential, email is the wrong method to use.

Recovery

If you suffer an attack you will need expert help to restore your system fully by: detecting the cause; investigating what has been affected; dealing with the incident to prevent further damage; and restoring your system and reviewing your security procedures.

An attack may not be obvious. A specialist data loss and intrusion detection programme alongside regular in-house checks may help. Your provider will advise you on a suitable programme.

Video and audio recordings

Your data protection responsibilities extend to information captured in audio or video recordings, including CCTV. The ICO's publication CCTV code of practice provides good practice advice on how to meet your legal requirements.

The code requires you to consider whether CCTV is appropriate and proportionate and whether less intrusive systems might deliver the desired outcome. An impact assessment will help you to assess the benefits of monitoring against the adverse effect on privacy. You must record your reasons for using CCTV and whether its use is justified in your practice.

As the practice owner, you should oversee the use, storage and disclosure of captured images. Your practice CCTV policy should include your reasons for using CCTV, the area covered, the CCTV operators, access to the images, disclosure, secure storage and retention.

The quality of your CCTV images must be sufficient for the purpose it was installed and have accurate time and date stamps. In-built audio recording facilities must be capable of being disabled; an essential feature for general overt recording.

Overt recording

Overt recording (where a camera is obvious) can take place in public or private areas. When used in a public area, you should have clear, prominent signage that CCTV is being used and why and identify the operator (usually the practice owner), giving contact details.

The cameras should be positioned to monitor only the intended areas. If monitoring involves private property, you will need the consent of the property owner. CCTV must not be used in private areas nor to record private conversations or discussions with patients about their treatment; any audio facility must be switched off.

If you use CCTV with audio recording to augment a patient's medical records, you must seek the patient's explicit permission with written consent. If the patient objects, the equipment must be turned off.

Covert recording

Covert audio or video recording of patients is illegal. Covert monitoring of staff can be used in exceptional circumstances – for example, where you suspect criminal activity or serious equivalent malpractice. You must be satisfied that:

- Covert cameras will be used for a specific purpose and then removed
- Informing staff about the recording would prejudice the investigation
- Intrusion on the privacy of innocent employees is justified
- Your position within the practice entitles you to make the decision to use covert recording.

Covert surveillance must not be used in private areas unless serious crime is suspected, and the police are already involved.

Where the recording reveals activity that is not relevant to the investigation, it should not be used, unless the activity constitutes gross-misconduct or is a criminal matter.

Releasing information

If you release personal information to a third party, the individual concerned should be informed (this can be via your privacy notice). Only the necessary information should be disclosed and be used only for the purpose it was disclosed.

In limited circumstances, disclosures to protect the individual or the public at large may be made to the appropriate authorities, without informing the patient – for example, in cases of suspected abuse of children or vulnerable adults, to protect against future risks to the health and safety of the individual or of others, and certain infectious diseases.

Where a record includes details of a third party (where they have provided information, for example), you must obtain their consent before disclosing the information, unless the third party is a health professional involved in the individual's care. It may be reasonable to disclose information without consent from a third party if disclosure would not infringe their rights or cause them embarrassment or distress. In other circumstances, details of a third party should be redacted.

Police enquiries

You can disclose information to the police to assist in the prevention and detection of crime, but you should ask for clear authority (a court order, for example) before disclosing. Where the police demand that the situation is urgent and require information without a court order, you must consider the seriousness of the crime, the potential danger to the public, and the likelihood that the suspect will cause serious injury to another person. If you receive a disclosure request from the police, seek advice on your obligations.

Certain circumstances require you to disclose information to the police:

- Where a driver has been injured or has committed an offence, you can disclose their name and address but not clinical information (Road Traffic Act 1988)
- If you have information about a planned or actual terrorist act (Terrorism Act 2005).

Legal advice and legal proceedings

You can disclose personal information in connection with legal proceedings, to obtain legal advice and to establish, exercise or defend legal rights. This allows you to pursue patients for non-payment or defend a claim by a member of staff in an Employment Tribunal.

You can report to the police a crime that you have witnessed or a crime against the practice, (such as robbery or assault). If, for example, a theft took place at the premises and you disclose a list of those present at the time, you may also need to inform patients that they may be subject to a police investigation.

Where a solicitor or other person makes a request for access on behalf of the individual, before providing the information you should satisfy yourself that the individual has consented to the disclosure. A solicitor would normally provide a signed statement from the individual.

CCTV images

Individuals caught on CCTV have a right to view the images and receive a copy. The request should include enough information to allow you to find the image (date and time, for example). Where a third party is identifiable, you may need to obscure their features to avoid unfair intrusion.

Any disclosure of images to a third party must be consistent with the purposes for which they were captured; you must not disclose CCTV images for any other reason.

However, you can disclose images to the police to assist in the prevention and detection of crime, but you should ask for clear authority before disclosing (a court order, for example). A court can ask (or order) you to disclose images as evidence in a civil legal case. You must assure yourself that the information is relevant to the case and notify the individuals concerned that their information is being used in this way.

Missing or deceased persons

You may be asked to release a patient's records to help with the identification of a body; the police or the coroner should make a formal request. You should comply promptly, but you should reassure yourself that there are reasonable grounds to believe that the body is the patient in question. If the request is in relation to a missing person, you should be more cautious and seek advice before disclosing the requested information.

Records of deceased people can be accessed by their personal representatives (the executor or administrator of their estate) or by anyone with a claim arising from the death. You must provide the information within 40 days of receiving the request and can only pass on copying costs and postage.

Tax enquiries

During routine inspections, tax inspectors may ask to see and take away appointment books, day books and patient records. Patient details should be anonymised if possible.

If a tax inspector has reasonable grounds to suspect that an offence involving serious fraud has been or will be committed and that evidence will be found on your premises, they can obtain an order requiring you to produce the information or a warrant for inspectors to enter your premises, search and seize it.