The Office *of the* Committee *for* Health & Social Care

Confidential Information

This policy covers security of confidential information and data to ensure that staff, contractors and volunteers are aware of their responsibilities.

Information included:

- Duty of confidence
- Disclosure of information
- Consent
- Confidentiality and children and young people
- Anonymised and aggregated information
- Breaches of confidentiality
- Off-site working
- Classification of documents
- Security including mail, fax, e-mail, telephones

Lead Professional/Reviewer	Claire Mahy, Senior Data Protection Officer – Health & Social Care
Issue date:	23 July 2019
Version no:	5d
Review date:	31 May 2020
Person responsible:	Senior Operating Officer

Ratified by the Corporate Management Team on behalf of the Committee *for* Health & Social Care.	Date: 27 June 2019

Document Control

This is a controlled document. Therefore, it should always be accessed from the intranet and should not be saved onto local or network drives for use.

While this document may be printed, the electronic version displayed on the intranet is the one that staff should refer to if it is available because it is the most up-to-date version. Any printed copies of this document are not controlled and may become obsolete without notice.

Version History

Version Number	Date	Person responsible	Prepared by	Status	Reason for Issue
5d	July 2019	Senior Operating Officer	Senior Data Protection Officer – Health & Social Care	Approved	A review of current policy to extend review date and reflect 2017 Law that came into force in 2018.
5c	Jan 2018	Medical Director	Assistant Director and Chief Pharmacist	Approved	Issued 15 January 2018 to extend the document's review date to the end of May 2018 in light of the forthcoming European General Data Protection Regulation.
5b	Nov 2016	Director of Corporate Services	Corporate Governance Manager	Approved	To extend review date to 2017.
5a	Feb 2011	Director of Corporate Services	Corporate Governance Manager	Approved	Minor amendments to existing document.
5	May 2010	Director of Corporate Services	Corporate Governance Manager	Approved	Current policy reviewed and updated.
4	May 2007	Director of Corporate Services	Corporate Governance Manager	Approved	Current policy reviewed and updated.
3	Nov 2006	Director of Corporate Services	Corporate Governance Manager	Approved	Current policy reviewed and updated.

2	Aug 2003	Deputy Chief Executive	Corporate Governance Manager	Next full review begins	Current policy reviewed and updated.
1	Sept 1999	Administration Director	Corporate Governance Manager	Review deadline	Approved by the Board of Health on 18 May 1999.
	1 Sept 1997	Administration Director	Corporate Governance Manager	Review deadline	Approved by the Board of Health on 22 July 1997, replacing G006 dated 31 August 1993.

Contents

Confidential Information

1. Introduction

This policy covers security of confidential information and data within the Committee *for* Health & Social Care services. It is important that confidential information is respected and not improperly disclosed or misused and that the appropriate people receive confidential information in an accurate, suitable and timely manner. Individuals and organisations must be certain that confidential information about them is treated confidentially and used appropriately. Confidential information may be in written, electronic, audio, video or verbal format.

This policy should be read in conjunction with the following Health and Social Care (HSC) policies:

- G102 Retention and Destruction of Information;
- G105 Dealing with Official Agencies;
- G106 Data Protection;
- G118 Communication and Media Handling;
- G205 Security;
- G212 Management of Contractors;
- G304 Care Records;
- G307 Consent;
- G308 Sharing of Person Identifiable Information;
- G602 Raising of Concerns by Staff (Whistleblowers).

This policy does not alter the rights of staff and volunteers to raise concerns in accordance with the States of Guernsey Whistleblowing Policy on The Bridge, the States of Guernsey intranet (a link to that policy is also available through document G602 on PoliPlus).

For the purposes of this policy, the term 'service user' refers to all those who use HSC services.

2. Policy objectives

This policy seeks to make certain that staff, students, contractors and volunteers are aware of their responsibilities, that confidentiality is maintained wherever appropriate and that guidance is available to assist in deciding whether confidential information is disclosed.

The objectives of this policy are:

a) to ensure that clinical confidentiality is maintained on behalf of the people to whom the Committee provides services;

b) to ensure that commercial confidentiality is maintained, in respect of the activities of the Committee, the Committee's suppliers and those for whom the Committee provides services;

c) to ensure that political confidentiality is maintained so that proposals for HSC policy remain confidential whilst being formulated unless, or until, they are brought into the public arena;

d) to ensure that personal confidentiality is maintained on behalf of the Committee's staff, its volunteers and the people for whom the Committee provides services.

3. Policy statement

It is the HSC's policy that all reasonable action must be taken to maintain confidentiality of person identifiable information and commercial information and that there is timely provision of confidential information to those entitled to receive it. Service users have the right to expect that information about them will be held in confidence.

4. Duty of confidence

A duty of confidence arises when confidential information comes to the knowledge of a person in the course of his/her duties. This requirement applies to all HSC employees, including temporary, fixed term contract, permanent and bank staff, and all those who carry out functions on behalf of the Committee, including contractors and volunteers. Everyone working

for, or in contract with the HSC, who records, handles, stores or otherwise comes into contact with information, has a duty of confidence to service users and also to his/her employer. This obligation to keep information private is covered by:

- Professional requirements, e.g. Code of Conduct, NMC, HPC, GMC;
- Terms and conditions of employment;
- Contracts of employment and the declaration of secrecy;
- The duty of care to service users, who will want confidential information treated appropriately;
- Legal requirements, e.g. the Data Protection (Bailiwick of Guernsey) Law, 2017 (See the HSC's policy on Data Protection (G106), for more information);
- Caldicott guidelines, which cover identifiable data relating to service users.

Health and Social Care professionals have an ethical duty of confidence, which, when considering whether information should be passed on, includes having regard to the health, well-being, needs and wishes of the service user.

Other individuals and agencies to whom information is passed legitimately may use it only as authorised for specific purposes.

Volunteers (including work experience students) may also learn confidential information because of their association with the Committee's services. The HSC acknowledges the valuable service that these individuals provide. Although volunteers are not paid as employees of the Committee, there is still an expectation that they will respect confidentiality. As a result, all volunteers are asked to sign a declaration of secrecy. In addition, all volunteers must follow the principles of this policy.

Contractors must also be made aware of their responsibility to respect confidentiality. Therefore, managers and others who are responsible for contracts should ensure that any contract for services either:

a) contains a clause stating that contractors and their staff have a

responsibility for safeguarding confidentiality (as set out in this policy);

or

b) directly refers to this policy.

Staff must not access any confidential information held in any form when they have no proper reason to do so in the course of their duties.

Staff must not access records for their personal interest. This includes their own records.

5. Balancing the duty of confidentiality against the duty to disclose information

The duty to maintain **clinical confidentiality is not absolute**. This is because an individual's right to confidentiality may conflict with the public interest, i.e. the public may benefit if the confidential information is disclosed. This is of particular relevance in relation to child protection, adults at risk of abuse of abuse or neglect, serious crime and public health risk. Staff and volunteers may receive requests for confidential clinical information from a wide variety of people and organisations such as:

- States members or members of States Committees (including HSC members);
- police;
- the media;
- advocates or legal representatives;
- charities, local companies and other external organisations;
- staff members and volunteers;
- service users, their families and friends and other third parties.

Confidential clinical information should not be supplied unless the request meets one of the criteria listed in Table 1 below. If there is doubt, or if a request is not covered by this policy, then the request must be referred, via line management, to the Senior Manager, Legislation and Administration,

(Tel. 725241 Ext. 4357). Enquiries from the media should be dealt with in line with the HSC's policy 'Dealing with the Media' (G108).

Table 1 lists the 9 circumstances when disclosure of confidential clinical information may occur.

Table 1

	Circumstances when disclosure of confidential clinical information can take place	**Examples and further guidance**
1.	If the service user consents	Service users can only give valid consent if they know exactly what information is to be disclosed and for what purpose. An example would be to inform relatives of a service user's condition.
2.	If it is in the service user's interest	However, the service user's informed consent must be sought unless it is either impossible, medically undesirable or the service user lacks capacity.
3.	If the law requires	The law must require (and not merely permit) disclosure, e.g. the notification of certain diseases under the local public health legislation. In addition, individuals may be required to give evidence in a court of law.
4.	If there is an overriding duty to the public	An example would be when a serious crime has been, or is very likely to be, committed.
5.	If it is necessary to safeguard national security	An example would be when information is obtained about terrorist activity.
6.	If there is a serious risk to public health	An example would be if a person suffering from a serious infectious disease refuses to take precautions to prevent others from being infected and, as a consequence, is likely to cause widespread infection. However, the risk must be serious. It has been held in case law that HIV does not fall

	Circumstances when disclosure of confidential clinical information can take place	**Examples and further guidance**
		into this category. Another example would be if a condition of one staff member indicates that others may be exposed to a serious health hazard in the workplace.
7.	If it is necessary for the purposes of medical or clinical research	Such medical research must have been approved by the local Ethics Committee to use confidential information without service user consent. Wherever possible, the service user's personal details should be omitted, as should any other information that would enable their identification. If service user anonymity cannot be kept, then service user consent must be obtained.
8.	If it is needed for the care and treatment of another service user whose health may be affected by the condition of the original service user	An example would be if a blood or organ donation were likely to take place.
9.	There may be occasions when release of confidential information may be justified to ensure efficient and effective operation of Committee services	To be dealt with on a case by case basis, seeking advice from the Senior Manager, Legislation and Administration and/or Caldicott Guardian. For example, local data protection legislation exempts disclosures for legal purposes (i.e. in connection with defending or pursuing litigation) - meaning that it will often be acceptable to release information to the organisation's insurers and Advocates in such circumstances.

6. Disclosure of confidential clinical information

Confidentiality is the service user's right and may usually only be waived by the service user or by someone legally entitled to do so on his / her behalf.

If a service user wants information withheld from someone who might otherwise have received it in connection with his / her care or treatment, the service user should be informed of any health or social care implications or of other relevant factors (e.g. the importance for the service user of the long-term record held by the GP). The service user's wishes should be respected unless there are overriding considerations to the contrary (See Table 1). The reasons for passing on information must be recorded in the health or social care record.

Generally, the duty of confidentiality means that there must be no disclosure of confidential clinical information without service user consent for any purpose other than the clinical care of the service user to whom it relates. However, Table 1 describes the circumstances when disclosure of confidential clinical information can take place without such consent.

In deciding whether a duty of confidentiality exists, the following two scenarios apply:

- the **information was gained in the course of professional work**. This is a key factor, because there is a significant public benefit in making sure that confidential clinical and personal information remains confidential. The duty of confidentiality encourages service users to be open with health and social care professionals, which then helps in their care and treatment and this benefits the public's health generally;

- the **information is in the public domain**. If the information is in the public domain, it is so widely known that it is no longer confidential. The duty of confidentiality is, therefore, unlikely to apply. However, if a known breach of confidentiality led to the information becoming public, no more breaches of confidentiality should be allowed and the information must be treated as if a duty of confidentiality still applied.

7. Consent to disclosure of confidential clinical and social care information

The public expects the Committee's services to provide professional standards of care and treatment. In the health and social care services, staff, volunteers and outside agencies work together to provide care. This requires confidential clinical and personal information being made known to those who are involved with the care and treatment of service users.

A main principle of keeping clinical and personal information confidential is that it can only be disclosed if the person it concerns consents. Consent should not be automatically assumed. Consent also needs to be informed in order to be valid, i.e. the individual it concerns must know and understand what information is to be disclosed and why. Nevertheless, it is not always practical, or desirable, to seek consent every time information is legitimately needed, e.g. for care planning or to inform relatives of a service user's condition.

However, wherever possible, people should be informed about how information relating to them will be used. The HSC leaflet 'Consent – What You Need to Know' provides information for service users so that they are aware of the position relating to information and consent. The leaflet also includes information regarding people who are unable to give their consent.

8. Confidentiality and children

Young people aged 16 or 17 are regarded as adults for purposes of consent to treatment and are entitled to the same duty of confidentiality as adults. Minors who undergo treatment having given their consent are entitled to expect their confidentiality to be respected. In such cases, confidential information cannot be shared with the parents without the minor's consent.

Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal or clinical information may be passed on and generally to have their confidence respected (e.g. they may be receiving treatment or counselling, about which they do not want their parents to know). In other

instances, decisions to pass on personal or clinical information may be taken by a person with parental responsibility, in consultation with the health and social care professionals involved.

In Gillick v West Norfolk and Wisbech Health Authority (1986) AC 112, it was decided that a child's confidentiality must be respected if the child:

> *reaches a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision." (Lord Scarman)*

The Gillick ruling is that children and young people should, if possible, be persuaded to allow their parents to be consulted; but that, ultimately, where they are *of sufficient understanding*, there is no obligation to do so.

In child protection cases, the overriding principle is to secure **the best interests of the child**. If a health or social care professional (or other person) has knowledge of abuse or neglect, it may be necessary to share this with others. Information should be shared on a strictly controlled basis so that decisions relating to the child's welfare can be taken in the light of all the relevant information.

9. Confidentiality relating to personnel information

All personnel files should be stored in lockable cabinets. Only authorised personnel will have access to employee files.

The Human Resources Department is obliged to provide certain information to the Police, States of Guernsey Income Tax, Committee *for* Employment & Social Security and Customs and Excise. No other information will be provided to a third party without the prior permission of the employee.

10. Anonymised information

Anonymised information refers to information from which a person's identity and other identifying details have been removed. Where anonymised information would be sufficient for a particular purpose, identifiable information should be omitted. All reasonable steps must be taken to ensure that the recipient is unable to trace the person's identity.

The fact that information has been anonymised does not remove the duty of confidence.

11. Aggregated information

Aggregated information, usually statistics, is compiled from personal information relating to a number of people. Aggregated information about performance and activity is an important aspect of accountability and is also vital for research and development. However, aggregating selective information about a small number of people may not always safeguard confidence adequately. Decisions will need to be made as to the point at which aggregated material cannot be regarded as personal and identifiable.

Statistics based on a count of fewer than 5 people are regarded as potentially person identifiable or disclosive particularly in small geographical areas. Depending on the sensitivity of the statistics it may be necessary to increase the minimum number to 10. It is recommended that information relating to small numbers are not published in the public domain.

12. Breaches of confidentiality

A person who discloses confidential information without consent, or against the wishes of the service user must be prepared to justify doing so to the HSC and, if necessary, to a court of law. Very careful consideration must be given before any disclosure is made. The person who discloses the information must be prepared to demonstrate that the above principles have been considered and a reasoned, deliberate decision was taken to release the information. It is also advisable for the person to document the reasoning behind the decision, the sources of advice that were used, to whom the information was released and the purpose of releasing the information.

The unauthorised passing of service user information by any member of staff or person in contract with the Committee is a very serious matter and will result in disciplinary action or action determined by the terms of the contract. Health and social care professionals may also be subject to action by their regulatory bodies. Staff must be aware of the possibly severe consequences of breaching service user confidence and this information

must be included in induction programmes.

It can be difficult to be sure when there is sufficient cause to break confidentiality. In some circumstances, a court may need to make the decision. Advice is available from the Senior Data Protection Officer and Caldicott Guardian. Medical practitioners and other health and social care professionals may wish to seek advice from their defence union or from their statutory bodies. Individuals may also seek advice from their professional staff association or trade union. However, the final decision rests with the individual, who must be able to justify his / her actions.

Service users who think their confidence has been breached may use the HSC complaints procedure.

13. Off-site working

Staff working off site are responsible for ensuring the security, proper care and use of confidential material. Equipment or paper documents containing confidential information must not be left unattended or visible when being carried in a car.

14. Classifying the confidentiality of Health and Social Care documents

The Committee has adopted the following classification to be used on all documents originating from the HSC's services. This will help to safeguard confidentiality and will mean that, within the organisation, both the addresser and the addressee will understand what a term means and the degree of confidentiality that applies.

The system set out in Table 2 must be used by all the HSC's services for all internal or outgoing mail and e-mail. Classifications not in the table are not acceptable and must not be used.

Externally generated mail received by the organisation will be treated according to the following table.

Table 2

	Classifications to be used	Who can open or read the item?	When should the classification be used?	When can the item be copied to others?
1.	**'Personal'** or **'To be opened by the addressee only'** Address must include the addressee's name	Addressee only	When the information is for **a named individual only** and not a post-holder	Only with the addressee and the addresser's agreement.
2.	***'Private'*** Address must include a post title	Addressee or addressee's deputy / secretary or a person covering in the addressee's absence.	When the addresser wants a **specific potholder** to see the document	Can be passed or copied to others if those people may be required to action the subject matter.
3.	***'Confidential'*** Address must include the potholders title or a class of reader, e.g. ward staff	Addressee (s) or addressee's deputy / secretary or a person covering in the addressee's absence.	When the addresser wants a **restricted circulation within the HSC.**	Can be passed or copied to the class of people or post-holder mentioned in the address.
4.	***'Not restricted'***	Anyone considered appropriate.	When the addresser considers that the item is not confidential	Unrestricted.
5.	**No classification is used.**	Anyone (unless the addressee (s) decides to assign one of the above classifications to it).	When the addresser considers that the item is not confidential	Unrestricted (but the addressee can change the classification).

Staff must be aware that private correspondence (i.e. non-work) addressed to the place of work may be opened in error if the envelope does not indicate that correspondence is personal. Private, non-work, correspondence should not ordinarily be sent to a place of work.

Business letters, even though they may have the name of the employee on the envelope, can be opened by any properly designated and authorised person at the place of work, as the letter relates to the activities of the employer and not the employee. Managers / department heads must ensure that procedures are in place within the department/service so that all staff are fully aware of persons who have authorisation to open mail, including their deputies. Arrangements must also be in place to ensure mail is opened by authorised persons when staff are on annual or sickness leave.

Mail addressed to service users should not be opened by anyone other than the addressee. However, service users who are infirm or incapacitated may allow their post to be opened.

15. Maintaining the Security of Confidential Information

Physical security of information:

- Information not in use should be kept in looked rooms and/or filing cabinets, folders, envelopes or other containers to prevent others from being able to access or read the information;

- It should be ensured that confidential information in use cannot be deliberately or accidentally read by unauthorised individuals;

- Confidential information should be locked away when not in use;

- A ‘Clear Desk Policy’ should operate;

- Confidential information should not be requested or given where this can be overheard by unauthorised third parties;

- It should be ensured that unauthorised personnel cannot see computer

screens, e.g. by using security screens, logging out when the computer is not in active use, using password protected screensavers;

- It should be ensured that confidential waste is destroyed by shredding or incineration. All confidential waste should be kept securely until it is destroyed. Please refer to the HSC's policy 'Retention and Destruction of Information' (G102).

Archiving:

- Confidential archived documents must be kept in a locked area with restricted access.

Electronic information systems (Trak Care, CID, PACS, etc.):

Access to electronic information systems is for the authorised purpose only. These systems must not be used to access information for unauthorised use, for example:

- accessing personal information such as blood test results;

- checking a colleague's date of birth or the reasons for an acquaintance's stay in hospital.

Unauthorised use of electronic information systems may result in disciplinary proceedings.

Mail: (See also Section 14, Table 2)

- Recycled envelopes must not be used to send person identifiable information in the internal post;

- Confidential information must be correctly and fully addressed to a named individual, including their post title and department;

- HSC reply paid envelopes issued to service users to return information, must be addressed to a named person;

- Outgoing posted items containing confidential information should have

a return address on the envelope;

- Health or social care records sent by post must be addressed to a named person and sent by special delivery or courier;

- Where possible, window envelopes should be used as they ensure the mail goes to the right person. However, care must be taken to ensure that only the name and address is visible through the window.

Fax machines:

- Fax machines should be used only where absolutely necessary. Encrypted email should be used instead;

- Fax machines and printers should be located away from public areas. Faxes that receive person identifiable or confidential information must be sited in a secure location (safe haven). Access should be limited to authorised staff within the department(s) served by the fax;

- When transmitting a fax message, a cover sheet must be prepared, clearly indicating who the message is for and contact details of the sender. It will be marked 'confidential' and indicate the total number of pages to be sent. The cover sheet will include a further statement, as follows, relating to the confidential nature of the message:

  Confidentiality: This fax and any documents transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this fax in error, please notify the sender immediately at the address shown above and destroy it without further action. Any dissemination, distribution or copying of this message or any files transmitted with it by an unauthorised recipient is strictly prohibited.

- If a fax is sent to an incorrect destination, a personal data breach form must be completed.

- If confidential information has to be transmitted by fax machine, the sender should contact the recipient to ensure they are available to receive the fax within an agreed timescale, unless faxing to an

unmanned, but secure, fax machine e.g. out-of-hours;

- In exceptional cases, where health or social care records are urgently needed and have to be faxed, the name and address of the service user and any third party mentioned must be obscured;

- Information containing sensitive patient details, e.g. HIV status, sexually transmitted disease or drug abuse, should not be transmitted using fax machines. However, in exceptional circumstances, where a delay would cause harm or potential risk to a patient, a fax can be used to transmit or receive sensitive information;

- Before transmitting, the user must ensure that the correct number has been dialled. The 'memory dial' facility on fax machines should be utilised for frequently used numbers to prevent the risk of misdialling. The responsibility for the correct dispatch of a fax is with the sender.

E-mail:

Although e-mail may be considered 'safer' than postal mail, no system can be considered fool proof. The following guidance should be observed:

- When sending service user identifiable information, the e-mail address of the recipient should be selected from the standard or personal address books to avoid mistyped addresses;

- The email should be encrypted using Egress;

- Do not include service user/staff names in the email subject line

- Service user identifiable information should not be stored within e-mail. Messages should be printed out and filed in the appropriate paper record or stored electronically within the service user's electronic health and social care record. E-mails must then be deleted from the system;

- Service user identifiable e-mails should not be directed or forwarded to home addresses;

- Before forwarding an e-mail containing confidential information to someone else, the sender's permission should be sought. The use of Egress will automate this process through email notification, sent to the originator;

- When replying to a message, the difference between 'reply to sender' and 'reply to all' should be noted, and the appropriate one used;

- External e-mail messages incorporate a warning in case they reach other than the intended recipient as follows:

  This e-mail (including attachments) may contain confidential and/or privileged information. If received in error, its use by you is not authorised and may be unlawful. Please notify the sender and delete all copies immediately. E-mails may be subject to error, interference and virus and no liability is accepted for loss or damage however it arises and whether direct or indirect. E-mails may be monitored for compliance purposes. All documents are subject to copyright.

Printing documents:

The title of any document being printed should not contain the name of a service user. If an e-mail is received from an external source, and contains the name of a service user in the title, the e-mail should be saved with an alternate title prior to being printed.

Telephones:

- When using telephones, confidential information must only be passed on, after verification of the recipient's identity, using call back if necessary;

- Messages including confidential details must not be given to third parties, who would not be authorised to receive the information.

Answer phones / voice mail:

- No confidential information should be left on answer phones or voice mail messages.

Monitoring the security of confidential information:

- Members of the Caldicott Committee, chaired by the Director of Public Health, audit the security of confidential information in line with Caldicott principles.

16. Accountability

The Chief Secretary is accountable to the Committee *for* Health & Social Care for ensuring that this policy is implemented throughout the Committee *for* Health & Social Care's services.

All directors are responsible for ensuring that this policy is brought to the attention of all staff and volunteers within their directorates.

All staff and volunteers are required familiarise themselves with the requirements of this policy and to take all reasonable steps to act in accordance with these requirements. Contravention of this policy by any member of staff will be regarded as an offence for which disciplinary action may be taken.

17. Compliance Monitoring

It is the responsibility of the Chief Secretary to ensure that compliance monitoring of this policy is undertaken. All directors are required to ensure compliance monitoring within their directorates.

Managers of contracts are required to ensure compliance monitoring of contractors.

18. Distribution

This policy will be placed on PoliPlus by the Senior Operating Officer. Directors will make copies available as needed to staff who do not have access to the intranet.

19. Review period

This policy will be reviewed by the Senior Operating Officer as required but

at a frequency of not less than every 3 years.

20. Policy removal

This policy replaces policy numbered G122, approved by the Board of the Health and Social Services Department on 28 May 2010, and should be retained on PoliPlus until such time as its replacement has been approved by the Committee *for* Health & Social Care. A single copy of the superseded policy will be held on the archived files of the HSC. Upon removal of the policy from the policy folder, no further copies need be kept.

21. Effective date

This version of the policy was approved by the Corporate Management Team on behalf of the Committee for Health & Social Care on 27 June 2019 and will come into effect on the date of issue shown on the title page.

The initial substantive version of this policy was approved by the Board of Health on 22 July 1997. Version 5c was issued 15 January 2018 with the approval of the Medical Director, to extend the document's review date to the end of May 2018 in light of the forthcoming European General Data Protection Regulation. Some amendments were made to the text to update the list of associated documents in section 1.