United States

Gaela Bailey, Benjamin Butler, Christopher Calsyn, Robin Campbell, Charles Hwang, Kris Meade and John Stewart, Crowell & Moring

www.practicallaw.com/3-241-6982

REGULATION

1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The US has not enacted a comprehensive national or federal law governing the collection and use of personal information. Instead, the US has dealt with the protection of personal information in a piecemeal way, primarily through industry-specific or data-specific laws at both the federal and state levels. In addition, even where a federal law covers similar conduct as corresponding state laws, it may not necessarily pre-empt or override such state law requirements.

Federal laws on privacy

There are numerous statutes, regulations and agency guidelines that govern privacy, but the following are the most broadly-applicable federal laws:

- The Health Insurance Portability and Accountability Act (*Public Law 104-191*) (specifically, the administrative simplification provisions of Title II of Subtitle F) (HIPAA).
- The Fair Credit Reporting Act (*15 U.S.C. § 1681 a-x*) (FCRA).
- The Fair and Accurate Credit Transactions Act (FACTA) (which operated mainly to amend the FCRA, and is rarely discussed independently).
- The Gramm-Leach-Bliley Act (*15 U.S.C. §§ 6801-6827*) (GLB).
- The Children's Online Privacy Protection Act (*15 U.S.C. §§ 6501-6506*) (COPPA).
- The Privacy Act of 1974 (*5 U.S.C. § 552a*) (Privacy Act).
- Under the HIPAA, the US government has promulgated several categories of regulations, three of which are:
  - The Standards for Privacy of Individually Identifiable Health Information (*45 C.F.R. parts 160 and 164 (subparts A and E)*) (HIPAA Privacy Rule). (The HIPAA Privacy Rule generally does not pre-empt state laws to the extent that the state laws provide greater privacy protection or privacy rights.);
  - The Security Standards for the Protection of Electronic Protected Health Information (*45 C.F.R. parts 160 and 164 (subparts A and C)*) (HIPAA Security Rule);
  - The Standards for Electronic Transactions and Code Sets (*45 C.F.R. parts 160 and 162*) (HIPAA Transactions Rule).

In addition to the above statutes, there are numerous less broadly-applicable federal statutes dealing with everything from the treatment of educational records held by federally-funded institutions, to videotape rental and motor vehicle records.

State laws on privacy

At the state level, there are many privacy-related statutes, ranging from those dealing with mundane details such as publishing social security numbers in divorce records, to sweeping privacy statutes such as those found in California. (In particular, the California Online Privacy Protection Act (which came into effect on 1 July 2004) virtually acts as a national law because it established rules for the treatment of personal information collected online which must be followed by any company whose website is accessible to a Californian citizen).

The most significant state laws dealing with privacy are the recently-enacted "security breach notification" laws. Given the large number of security breaches in 2005 (and the enhanced awareness of such breaches), many states enacted legislation paralleling California's Security Breach Bill, passed in 2003, which provides for notification to be given to individuals whose personal information is compromised.

As of March 2007, 36 states had enacted their own version of security breach notification laws, and more were under consideration. Some states have adhered to the specific purpose of protecting against identity theft and financial loss, and have therefore established a materiality requirement or threshold of harm before notification is required. Some states have limited the application of this type of law to entities that were most likely to process large amounts of personal information, including data brokers and government entities. Other states have included every type of person or entity, without excluding those already under the jurisdiction of federal or state privacy regulations such as the GLB or the HIPAA. The existence of at least 36 different state statutes with inconsistent scope and detailed requirements obliges data controllers to look carefully at each to determine the best route to compliance in the US. At the time of writing, several federal bills intended to pre-empt this patchwork quilt of state laws were pending. No clear forerunner had emerged, but it is predicted that a federal data breach law with pre-emption will likely follow in due course.

Generally, the US state security breach notification laws define "personal information" much more narrowly than European privacy laws. Many limit this term to information that enables a person to commit identity theft. At a minimum, the state laws require notice to be given to the individuals residing in the state if their personal information has been, or is reasonably believed to have been, compromised. Other states have added pre-breach measures, similar to EU requirements, such as:

- Mandatory security procedures and practices;
- Contractual safeguards for transfers;
- Document destruction policies appropriate for personal information; and
- Encryption for transfers.

California also paved the way in 2005 (with Civil Code Section 1798.85) for the recent state interest in introducing legislative restrictions on the collection, use and display of an individual's social security number (SSN) by companies and individuals. At present 25 states have laws containing restrictions on the use of SSNs and over 30 state legislatures have seen the introduction of one or more SSN restriction bills in their current legislation sessions. Existing and pending laws vary, but tend to prohibit:

- Selling SSNs.
- Publicly posting an individual's SSN.
- Transmitting SSNs over the internet.
- Requiring the use of SSNs for access to websites.
- Printing an individual's SSN on any materials that are mailed to the individual (including faxed documents or pay stubs).
- Using SSNs as an employee ID or customer account number.

The following answers in this chapter address the federal statutes above only. In addition, the answers for the FACTA and the FCRA are the same, unless otherwise stated.

2. To whom do the rules apply (EU: data controller)?

HIPAA. The HIPAA governs the following "covered entities":

- Health plans (that is, an individual or group plan that provides, or pays the cost of, medical care).
- Healthcare clearinghouses.
- Healthcare providers that engage in certain electronic transactions.
- Medicare prescription drug card sponsors.

FACTA/FCRA. These statutes regulate:

- "Consumer reporting agencies", which includes any entity that, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information for the purpose of providing "consumer reports" (*see Question 3*) to third parties.
- Users of consumer reports, by limiting the permissible purposes for which credit reports can be obtained (*see Question 7*) and regulating the activities of users who take an "adverse action" (such as a denial of credit) against a consumer (*15 U.S.C. §§ 1681b, 1681m*).
- Entities that provide consumer credit information to consumer reporting agencies (*15 U.S.C. § 1681s-2*).
- Persons who unlawfully obtain a consumer's credit report (*15 U.S.C. § 1681q-r*).

GLB. The GLB governs financial institutions that engage in "financial activities", which includes (*12 U.S.C. §1843(k)*):

- Lending.
- Insuring.
- Exchanging.
- Investing for others.
- Providing financial, economic or investment advisory services.
- Dealing in securities.

COPPA. The COPPA regulates "operators", defined as any person who:

- Operates, for commercial purposes, a website on the internet or an online service.
- Collects or maintains personal information from or about the users of, or visitors to, that website or online service, or who does so on another's behalf, both domestically and between any US state or territory and one or more foreign nations.

It does not include certain non-profit entities.

Privacy Act. The Privacy Act applies to US federal agencies and government contractors that operate any system of records on behalf of such agencies.

3. What data is regulated (EU: personal data)?

HIPAA. The HIPAA regulates protected health information (PHI), that is, in general, individually identifiable health information held or transmitted by a covered entity or its "business associate". It can include demographic information about an individual.

FACTA/FCRA. These statutes regulate consumer reports, defined as any written, oral or other communication of any information by a consumer reporting agency (*see Question 2*) bearing on a consumer's creditworthiness, character, reputation, personal characteristics, or mode of living, which is used for the purpose of establishing the consumer's eligibility for credit, insurance or

employment. FACTA also imposes restrictions on the extent to which credit card information, including account numbers and expiration dates, may be reflected on any credit card receipts that are generated.

GLB. The GLB governs non-public personal information of a customer of a financial institution, which generally means personally identifiable financial information that:

- Is provided by a consumer to a financial institution.
- Results from a transaction between the consumer and the financial institution.
- Is otherwise obtained by a financial institution.

COPPA. The COPPA regulates "personal information" collected from a child (an individual under the age of 13), defined as individually identifiable information about an individual collected online, including:

- A first and last name.
- A home or other physical address including a street name and a name of a city or town.
- An e-mail address.
- A telephone number.
- A social security number.
- Any other identifier that the Federal Trade Commission (FTC) (*see box, The regulatory authorities*) determines permits the physical or online contacting of a specific individual.
- Any other information concerning the child or the parents of that child that the website collects online from the child (for example, hobbies, interests or information collected through tracking mechanisms such as cookies) when that information is combined with any other identifier set out above.

Privacy Act. The Privacy Act regulates any record contained in "a system of records", defined as a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to the individual.

4. What acts are regulated (EU: processing)?

HIPAA. The HIPAA regulates the use and disclosure of PHI, and the collection, maintenance, use or transmission of electronic PHI.

FACTA/FCRA. These statutes govern preparing, disseminating, obtaining, contributing information to and using consumer reports. These statutes also govern the printing of credit card receipts and disclosure of information on such receipts.

GLB. The GLB regulates the disclosure of non-public personal information of consumers by financial institutions to non-affiliated third parties. The financial institution must:

- Provide the consumer with written notice of the privacy procedures of the financial institution.
- Allow the consumer the opportunity to opt out of the privacy policies so that his non-public personal information is not disclosed.

The financial institution must also provide an explanation as to how the consumer can exercise the non-disclosure option.

There are several exceptions to this general rule, including when the non-affiliated third party is performing services on behalf of the financial institution, such as marketing the financial institution's own products. (*See also Question 15.*)

COPPA. The COPPA regulates the collection, use and disclosure of the personal information of children online.

Privacy Act. The Privacy Act governs the disclosure of private information by an agency or contractor unless an individual consents in writing. The statute does not specifically define what constitutes disclosure, but some judicial precedents offer a few guiding principles.

5. What is the jurisdictional scope of the rules?

HIPAA. Jurisdictional scope is limited to covered entities over which the US government has enforcement authority (*see Question 2*); however, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of the US jurisdiction.

FACTA/FCRA. The FCRA applies to:

- Consumer reporting agencies.
- Information providers.
- All persons who obtain or use a consumer report within the US.

All federal and state courts have jurisdiction to hear claims for violations of the FCRA.

GLB. The GLB applies to:

- All financial institutions in relation to their handling of their customers' non-public personal information.
- Non-affiliated third parties that receive non-public personal information from a financial institution.
- Persons who obtain or attempt to obtain, or cause or attempt to cause disclosure of, that non-public personal information from financial institutions through false or fraudulent means.

COPPA. The COPPA applies to websites or online services involving commerce among the US states or territories, with foreign nations or in any territory of the US.

Privacy Act. The Privacy Act applies only to federal agencies and certain contractors of such agencies, and only to information about "individuals" who are US citizens or foreign persons lawfully admitted for permanent residence.

6. What are the main exemptions (if any)?

HIPAA. The main exemptions are:

- Health information that is not individually identifiable (for example, aggregate data).
- Use and disclosure by individuals or organisations that are not covered entities (or business associates of covered entities) (for example, most employers that are not involved in providing or financing healthcare).

FACTA/FCRA. The FCRA permits a consumer report to be provided or obtained only for specified purposes and subject to certain disclosure and consent requirements. Employment background checks consented to by the prospective employee and employee misconduct investigation reports are excluded from the definition of "consumer report". Reports may be provided, according to the written instructions of the consumer or to a court order or grand jury subpoena, without regard to the list of permissible purposes. Reports obtained in investigations related to employee misconduct, to government employee security clearances, or to the loss or disclosure of classified government information are exempt from consumer disclosure and consent requirements while the investigation is ongoing.

GLB. Financial institutions can share customers' non-public personal information:

- With non-affiliated third parties who are providing services to the financial institution.
- When necessary to effect, administer or enforce a transaction.
- In connection with a financial service, requested or authorised by the consumer.

In addition, this information can be disclosed without notice to entities such as:

- Insurance rate advisory organisations.
- Guaranty funds or agencies.
- Applicable rating agencies of the financial institution.
- Persons assessing the institution's compliance with industry standards.

The GLB also does not apply to publicly-available information.

COPPA. The parental consent generally required by the COPPA is not required when:

- An operator collects an e-mail address to respond to a one-time request from a child and then deletes it.
- The information is being used to obtain parental consent.
- The contact information is used only to respond more than once to a specific request and is not used to contact the child beyond the scope of that request (for example, subscription to a newsletter).
- An operator collects the information to protect the child's safety.
- An operator collects information to protect the security or liability of the website, or to respond to law enforcement.

Privacy Act. There are 12 express exceptions to the general rule requiring an individual's prior consent to the disclosure of records. The most relevant of these exceptions are law enforcement activities and "routine use", which is a broad exception defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" (*5 U.S.C. § 552a(a)(7)*).

7. Is notification or registration required before processing data? If so, please provide brief details.

HIPAA. Notification or registration is not required with a government authority. However, when required under the HIPAA Privacy Rule, a covered entity may be obliged to obtain an authorisation from the individual who is the subject of the PHI before using or disclosing the PHI. In addition, covered entities must keep an accounting of certain disclosures of the PHI.

FACTA/FCRA. These statutes deal with the dissemination of a consumer's credit report rather than "processing" data. To receive a consumer report, the user of the report must have a "permissible purpose" (*see below*), and a consumer reporting agency can only provide a consumer report to a person who it has reason to believe has such a purpose. For certain employment purposes, and for certain credit and insurance transactions not initiated by the consumer, notification must be given to the subject consumer, and his consent must be obtained, before the report is provided.

A permissible purpose exists where the person receiving the consumer's report intends to use it:

- In connection with a credit transaction involving the consumer, including an account review.
- For employment purposes.
- In connection with the underwriting of insurance.
- In connection with the consumer's eligibility for a government licence.
- In connection with a transaction initiated by the consumer.

- In relation to a child support obligation.
- To offer the consumer a "firm offer of credit".

A consumer can elect to have his name and address excluded from any list provided by a consumer reporting agency to its subscribers in connection with firm offers of credit.

GLB. The GLB requires that, at the time of establishing a customer relationship with an individual, the financial institution must disclose its privacy policy in writing to the individual and allow him to opt out and prevent the disclosure of his non-public personal information. The financial institution must also provide an explanation as to how the consumer can exercise the non-disclosure option.

Each agency or authority with jurisdiction under the GLB over financial institutions is required to:

- Establish standards to ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of these records.
- Protect against unauthorised access to, or use of, these records or information, which would result in substantial harm or inconvenience to any customer.

COPPA. The website or online service must provide notice about:

- What information is collected from children.
- How such information is used.
- The operator's disclosure practices.

Parental consent is required for the collection, use or disclosure of personal information from children.

No notification to authorities is required.

Privacy Act. No notification or registration is required, only the consent of the individuals involved before disclosure, but each agency must keep an accurate accounting of each disclosure it makes.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

HIPAA. The HIPAA Transactions Rule sets out uniform standards for certain electronic transactions commonly used in the healthcare industry. Covered entities engaged in one or more of these transactions generally must comply with the relevant standard for that transaction. The HIPAA Privacy Rule requires, with some exceptions, covered entities to use, request or disclose only the minimum amount of PHI necessary to establish the purpose of the use, request or disclosure. The HIPAA Security Rule requires covered entities to implement a variety of administrative, physical, technical and organisational safeguards. (*See also Question 14.*)

FACTA/FCRA. The FCRA is a comprehensive statutory scheme that requires, in part, consumer reporting agencies to maintain reasonable procedures to ensure the maximum possible accuracy of the information in consumer files. The FCRA also states that those entities that provide information to consumer reporting agencies have a duty to:

- Correct information and update information that they discover is inaccurate.
- Notify consumer reporting agencies promptly of any errors concerning a consumer's credit.

FACTA imposes obligations on issuers of credit card receipts to refrain from disclosing full credit card account numbers and expiration dates.

GLB. The federal and state agencies responsible for enforcing the GLB have created standards applicable to the financial institutions within the agencies' jurisdiction (*see Question 7*).

Some of the common standards that have been promulgated are requirements restricting access to authorised individuals through:

- Authentication mechanisms.
- Background checks of employees.
- Data encryption.
- Regular monitoring and testing of the information security systems.

COPPA. In addition to the requirements in *Question 7*, an operator:

- Must provide certain information to a parent on request.
- Cannot condition a child's participation in a game or other activity on the child disclosing more personal information than is reasonably necessary.
- Must maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

Privacy Act. In addition to a general prohibition against disclosure of personal information without consent, the Privacy Act requires the agency to:

- Make an accurate accounting of each disclosure of a record.
- Permit access by an individual to his record or to any information about him which is contained in the system, and permit a request to amend such record.
- Maintain in its records only such information about an individual as is relevant and necessary.

- Collect information, to the extent possible, directly from the subject individual.
- Inform each individual whom it asks to supply information of:
  - the authority that authorises solicitation of the information;
  - the principal purpose(s);
  - the routine uses which may be made of the information; and
  - the consequences of not providing the information.
- Publish in the Federal Register notice of the existence and character of the system of records.
- Maintain all records with such accuracy, relevance, timeliness and completeness as is reasonably necessary.
- Before disseminating any record, make reasonable efforts to assure that such records are accurate, complete, timely and relevant.
- Maintain no record describing how an individual exercises his First Amendment rights.
- Make reasonable efforts to notify an individual when any record is disclosed by compulsory legal process.
- Establish rules of conduct for persons involved with systems of records.
- Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records.
- Before publication, provide notice of a new use of the information.

9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there regarding the form and content of consent? Would online consent suffice?**
- **Are there any special rules regarding the giving of consent by minors?**

HIPAA. The HIPAA Privacy Rule generally requires a covered entity to obtain an individual's authorisation before using or disclosing the individual's PHI, unless otherwise permitted by the HIPAA. Several exceptions apply, most notably the use or disclosure of PHI for "treatment", "payment" or "healthcare operations" (as those terms are defined in the Privacy Rule), as well as uses or disclosures of information that are required by law. The HIPAA Privacy Rule establishes core elements and required statements that must be included in a valid authorisation. An authorisation must generally be in writing and include the signature of the individual (or representative) and date.

The HIPAA generally defers to state or other applicable law in relation to the right of a minor to authorise use or disclosure of PHI.

FACTA/FCRA. The consent of data subjects is not required before processing personal data. Consumer reporting agencies do not need consent from consumers to disseminate consumer reports. Similarly, information providers do not need consent from consumers to report a consumer's account activity to consumer reporting agencies. Generally, if a person has a permissible purpose to receive the consumer report (*see Question 7*), the consumer reporting agency can provide the consumer's report. but if the report is to be used for employment purposes, the agency must obtain a certification from the recipient that it has complied with a number of requirements, including having received the subject consumer's consent to the procurement of the report. Further, a consumer can notify a consumer reporting agency that he does not consent to any use of a report in connection with any credit or insurance transaction not initiated by the consumer.

There are no special rules regarding the giving of consent by minors.

GLB. At the time of establishing a customer relationship, and at least annually after that, the financial institutions subject to the GLB must notify the customer of the institution's privacy policy and allow the individual to restrict the financial institution from sharing the individual's non-public personal information with non-affiliated third parties.

This disclosure can be in writing or in electronic form but must provide a clear description of the institution's policies and practices with respect to, among other things, the following:

- Disclosing non-public personal information to affiliates and non-affiliated third parties including the categories of information that can be disclosed.
- Disclosing the non-public personal information of former customers.
- Protecting the non-public personal information of consumers.
- The categories of non-public personal information that are collected by the institution.

There are no specific clauses in the GLB's provisions on privacy that mention minors. However, the GLB provides that financial institutions can disclose an individual's non-public personal information to persons acting in a fiduciary or representative capacity with respect to a customer without violating the GLB.

COPPA. The "verifiable parental consent" required by the COPPA is defined as "any reasonable effort (taking into consideration available technology), including a request for authorisation for future collection, use and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use and disclosure practices, and authorises the collection, use and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child" (*15 U.S.C. § 6501(9)*).

Privacy Act. The consent of the individuals involved is required before a record containing personal information can be disclosed.

There are no special rules regarding the giving of consent by minors.

10. If there is no consent, on what other grounds (if any) can processing be justified?

HIPAA. The HIPAA Privacy Rule generally permits a covered entity to use or disclose PHI, without an individual's authorisation, for purposes of "treatment", "payment" or "healthcare operations". In addition, the HIPAA Privacy Rule includes other exceptions where authorisation is not required, such as where a disclosure is otherwise required by law.

FACTA/FCRA. No other grounds are necessary, merely a permissible purpose for dissemination (*see Question 7*).

GLB. See *Question 9*.

COPPA. Consent is required, unless an exemption applies.

Privacy Act. See *Question 9*.

11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

HIPAA. The HIPAA Privacy Rule provides special rules for "psychotherapy notes", generally defined as notes that are:

- Recorded (in any medium) by a healthcare provider who is a mental health professional, documenting or analysing the contents of conversation during a private counselling session or a group, joint or family counselling session.
- Separated from the rest of the individual's medical record.

The definition excludes certain categories of treatment-related information such as:

- Medication prescription and monitoring.
- Counselling session start and stop times.
- The modalities and frequencies of treatment provided.
- Results of clinical tests.
- Any summary of the following items:
  - diagnosis;
  - functional status;
  - the treatment plan;
  - symptoms;
  - prognosis; and
  - progress to date.

With some exceptions, most uses and disclosures of psychotherapy notes require individual authorisation, even if for purposes of treatment, payment or healthcare operations.

FACTA/FCRA. The FCRA prohibits the provision of consumer reports containing medical information without the specific consent of the consumer. Credit card account numbers are given special treatment under FACTA.

GLB. There are no special provisions regarding certain types of data. However, under the GLB's general principles, some sensitive information may require greater safeguards in handling and storage. Financial institutions are prohibited from disclosing, other than to a consumer reporting agency, an account number or similar access code for a credit card, deposit account or transaction account to a non-affiliated third party for use in telemarketing, direct mail marketing or other marketing through e-mail.

COPPA. No special rules apply, except to the personal information of children described in *Question 3*.

Privacy Act. No special rules apply.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

HIPAA. A covered entity is required to develop and make available a Notice of Privacy Practices, a document that generally describes the covered entity's privacy practices and satisfies the criteria required by the HIPAA Privacy Rule. A covered healthcare provider with a direct treatment relationship with an individual must provide the Notice of Privacy Practices at the time of the first treatment encounter.

FACTA/FCRA. The FCRA does not require that any information be provided to the consumer at the point of collection. The FCRA does require consumer reporting agencies to notify consumers of the entities that received the consumer's report. There are also special notification requirements if a consumer report is used for employment purposes.

GLB. At the time of establishing a consumer relationship, the GLB requires financial institutions to:

- Notify the consumer either in writing or electronically of the privacy policies and practices of the financial institution for non-public personal information.
- Provide the consumer with the opportunity to opt out of these policies and require the financial institution to refrain from disclosing any of this information.

The financial institution must also provide an explanation as to how the consumer can exercise the non-disclosure option. In addition, the GLB obliges the financial institutions to provide an updated notification of their privacy policies and practices at least

once annually to all of their customers, and provide them with the choice of opting out of the policies at that time.

COPPA. Operators must provide notice on the website as to:

- The information that is collected from children by the operator.
- How the operator uses such information.
- The operator's disclosure practices for such information.

Privacy Act. The individual must be provided with:

- Notice of the authority for collecting the information.
- The principal purpose(s).
- The routine uses to be made of the information.
- The consequences of not providing the information requested.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

HIPAA. An individual has a right to request:

- Access to his own PHI.
- An amendment of his own PHI.
- An account describing the circumstances of previous disclosures of his PHI (exceptions apply).

An individual can also request a covered entity to restrict the use or disclosure of the individual's PHI, or request confidential communications with respect to the use and disclosure of his PHI (such as use of an alternative mailing address).

FACTA/FCRA. On a consumer's request, the agency must disclose to the consumer:

- All the information in the consumer's file.
- The sources of the information.
- The identification of each person who procured the consumer's report.

The consumer can dispute the accuracy of the specific items appearing in his file.

GLB. The only right afforded to individuals under the GLB is the right to notice of the privacy policies of the financial institutions with which they do business and the ability to opt out of those policies to prevent the disclosure of their non-public personal information.

COPPA. A parent is entitled to:

- A description of the specific types of personal information collected from the child by the operator.
- The opportunity to refuse to permit further use or maintenance or future online collection of personal information from that child.
- A means to obtain any personal information collected from that child.

Privacy Act. An individual has the right to:

- Access his personal information.
- Request an amendment to it.
- Dispute any refusal to amend it.
- Have such a dispute noted on the record.

SECURITY REQUIREMENTS

14. What security requirements are imposed in relation to personal data?

HIPAA. The HIPAA Security Rule requires covered entities to implement a variety of administrative, physical, technical and organisational safeguards. For example, a covered entity must analyse potential risks to the confidentiality and integrity of electronic PHI, and take steps to manage those risks, such as limiting access to facilities and workstations. The technical safeguards are designed to protect a covered entity's information systems from unauthorised access through the use of access controls and authentication requirements, including, if appropriate, the use of an automatic logoff function and/or encryption of electronic PHI.

FACTA/FCRA. A consumer reporting agency cannot disclose a consumer's report following a consumer request without proper identification. Also, an agency cannot release a consumer report unless the user of the report has a permissible purpose (*see Question 7*).

GLB. Each agency or authority with jurisdiction under the GLB over financial institutions must satisfy certain requirements (*see Question 7*).

COPPA. An operator is required to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of the personal information of children.

Privacy Act. Agencies are required to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records.

PROCESSING BY THIRD PARTIES

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

HIPAA. A third party who processes PHI on behalf of a covered entity is generally considered a "business associate" of the covered entity and must agree to certain contractual obligations set

out in the HIPAA Privacy Rule and the HIPAA Security Rule. These obligations are generally intended to ensure that the business associate properly safeguards the PHI.

FACTA/FCRA. To provide consumer reports to a third party, consumer reporting agencies must have written agreements in place with the users of the reports. The written agreements must contain certifications, which promise that the user has a permissible purpose to receive the consumer's report (*see Question 7*). The certification guarantees that the user of the report will comply with all of the provisions of the FCRA.

GLB. Financial institutions can disclose non-public personal information to a non-affiliated third party that performs services for the financial institution, provided that:

- The consumer receives full disclosure that such information can be so disclosed.
- The financial institution's contract with the service provider contains a "flow-down" clause that requires the service provider to maintain the confidentiality of such information.

The financial institution's data protection plan should appropriately address any additional risks created by the disclosure of such information to the service provider.

COPPA. The definition of operator does not distinguish between parties and includes any person who operates a website or online service "or on whose behalf such information is collected or maintained" (*see Question 2*).

Privacy Act. Government contractors that operate a system of records on behalf of federal agencies are subject to the requirements of the Privacy Act.

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

No distinction is made for data disclosed outside of the US in any of the six federal statutes.

17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

HIPAA. The HIPAA Privacy Rule and the HIPAA Security Rule include required provisions for "business associate" agreements between covered entities and their business associates (*see Question 15*). In addition, the HIPAA Transactions Rule addresses "trading partner agreements", which are agreements related to the exchange of information in electronic transactions (specifying, for example, the duties and responsibilities of each party to the agreement in conducting a standard transaction). The HIPAA Transactions Rule does not specify the contents of such agreements, but provides certain terms that cannot be included. For example, if the Transactions Rule requires that a certain category of data must be included in a transaction, the agreement cannot require a trading partner to delete such data from a transaction.

The US Department of Health and Human Services (HHS) (*see box, The regulatory authorities*) has issued sample business associate agreement terms, but covered entities generally have flexibility as to the specific form used for a business associate agreement or trading partner agreement.

FACTA/FCRA. No.

GLB. No standard forms have been produced, but each of the enforcing agencies have created exemplary language that can be used by financial institutions falling under the agency's specific jurisdiction in drafting the notices of their privacy polices that the institutions are required to send to their customers.

COPPA. No.

Privacy Act. No.

18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

HIPAA. Where a third party has signed a business associate agreement with a covered entity, and a disclosure of PHI would otherwise be permitted under the HIPAA without the authorisation of the person who is the subject of the PHI, the covered entity can generally disclose the PHI to the third party without the individual's authorisation. Trading partner agreements are generally used to establish the technology-related responsibilities of the parties to a transaction; where an authorisation would otherwise be required, the existence of a trading partner agreement would generally not change that requirement.

FACTA/FCRA. No.

GLB. Before transferring any non-public personal information, the financial institution must disclose to the customer the institution's privacy policies and provide the individual a chance to opt out of those provisions. Because it is an opt-out provision as opposed to an opt-in, an individual would have to take affirmative action to stop the transfer.

COPPA. No.

Privacy Act. No.

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

HIPAA. No, although covered entities may be subject to a government compliance review, including a review of business associate agreements with third parties.

FACTA/FCRA. No.

GLB. No; the disclosure requirements in the GLB and the regulations issued by the enforcing agencies under it provide guidance

THE REGULATORY AUTHORITIES

Office for Civil Rights (OCR), US Department of Health and Human Services

Head. Winston A Wilkinson (Director)

Contact details. 200 Independence Avenue, SW
Room 515F, HHH Building
Washington, DC 20201
United States
T +1 202 619 0403
F +1 202 619 3437
E *OCRPrivacy@hhs.gov, winston.wilkinson@hhs.gov*
W *www.hhs.gov/ocr/hipaa*

Main area of responsibility. The OCR regulates, among other things, the Health Insurance Portability and Accountability Act's (*Public Law 104-191*) (HIPAA) Standards for Privacy of Individually Identifiable Health Information (*45 C.F.R. parts 160 and 164 (subparts A and E)*).

Contact for queries. See above, *contact details*.

Obtaining information. See above, *contact details*.

Centers for Medicare & Medicaid Services (CMS), US Department of Health and Human Services

Head. Leslie V Norwalk (Acting Administrator)

Contact details. 200 Independence Avenue, SW
Room 314G, HHH Building
Washington, DC 20201
United States
T +1 202 690 6726
F +1 202 690 6262
E *leslie.norwalk@cms.hhs.gov*
W *www.cms.hhs.gov/HIPAAGenInfo/*

Main area of responsibility. The CMS regulates, among other things:

- The Security Standards for the Protection of Electronic PHI (*45 C.F.R. parts 160 and 164 (subparts A and C)*).
- The Standards for Electronic Transactions and Code Sets (*45 C.F.R. parts 160 and 162*).

Contact for queries. See above, *contact details*.

Obtaining information. See above, *contact details*.

Federal Trade Commission (FTC)

Head. Deborah Platt Majoras (Chair)

Contact details. 600 Pennsylvania Avenue, NW
Room 442
Washington, DC 20580
United States
T +1 202 326 2100
F +1 202 326 2396
E *chairman@ftc.gov*
W *www.ftc.gov/privacy/index*

Main area of responsibility. The FTC can commence a civil action in a US district court to recover a civil penalty or bring an injunction against any person violating the Fair Credit Reporting Act (*15 U.S.C. § 1681 a-x*).

The FTC can also bring enforcement actions and impose civil penalties for violations of the Children's Online Privacy Protection Act (*15 U.S.C. §§ 6501-6506*).

In addition, in relation to the Gramm-Leach-Bliley Act (*15 U.S.C. §§ 6801-6827*) (GLB), the FTC enjoys residual enforcement

on what must be included in the notices provided by financial institutions to their customers, but no further approval is necessary for the financial institution.

COPPA. No.

Privacy Act. No.

ENFORCEMENT AND SANCTIONS

20. What are the enforcement powers of the national regulator?

HIPAA. The HHS can conduct compliance reviews to determine whether covered entities are complying with the HIPAA Privacy Rule. The HHS has also established a complaint mechanism for individuals to raise concerns about a covered entity's compliance and may investigate a covered entity who is the subject of a complaint.

FACTA/FCRA. The FTC may commence a civil action in a US district court to recover a civil penalty or obtain an injunction against any person violating the FCRA. The FTC can recover US$2,500 (about EUR2,000) for each violation of the FCRA. The FCRA also provides for a private right of action for consumers harmed by a person's negligent or wilful non-compliance. A consumer can recover actual damages and statutory penalties of US$1,000 (about EUR770) for each wilful violation. A consumer can also recover punitive damages for wilful violations of the FCRA.

GLB. Each of the various agencies with jurisdiction under the GLB has established regulations consistent with the GLB for the part of the financial industry it regulates, and can implement those regulations pursuant to its grant of authority under other laws.

COPPA. A violation of COPPA is considered an unfair or deceptive act or practice. Both the FTC and the Attorney Generals for the 50 states are given authority to enforce the COPPA by:

- Enjoining a practice.
- Enforcing compliance.
- Seeking damages.
- Obtaining other relief deemed appropriate by the courts.

jurisdiction over any other financial institution that is not subject to the jurisdiction of any agency or authority listed below (*see below, Other regulatory authorities*).

Contact for queries. Joel C Winston (Associate Director)
601 New Jersey Avenue, NW
Room 3119
Washington, DC 20001
T +1 202 326 3153
F +1 202 326 3768
E *jwinston@ftc.gov*

Obtaining information. More information can be obtained at *www.ftc.gov/privacy* and *www.ftc.gov/kidzprivacy*.

Other regulatory authorities

The GLB is enforced by seven federal regulatory agencies and by the various state insurance regulatory authorities. These entities and the groups of financial institutions over which they have enforcement powers are:

- The Office of the Comptroller of the Currency (national banks and certain other banking entities or subsidiaries of them, except brokers, dealers, persons providing insurance, investment companies and investment advisers): *www.occ.treas.gov/.*
- The Board of Governors of the Federal Reserve System (member banks of the Federal Reserve System (other than national banks) and certain other banking entities or subsidiaries of them, except brokers, dealers, persons providing insurance, investment companies and investment advisers): *www.federalreserve.gov/*.
- The Board of Directors of the Federal Deposit Insurance Corporation (FDIC) (banks insured by the FDIC (other than members of the Federal Reserve System) and certain other banking entities and subsidiaries of them, except brokers, dealers, persons providing insurance, investment companies and investment advisers):
  - *www.fdic.gov/* (FDIC);
  - *www.fdic.gov/consumers/index.html* (Consumer Protection);
  - *www.fdic.gov/about/learn/board/index.html* (Board of Directors).
- The Director of the Office of Thrift Supervision (savings associations insured by the FDIC, and subsidiaries of them, except brokers, dealers, persons providing insurance, investment companies and investment advisers): *www.ots.treas.gov/* (Office of Thrift Supervision).
- The Board of the National Credit Union Administration (federally insured credit unions, and any subsidiaries of them):
  - *www.ncua.gov/* (National Credit Union Association);
  - *www.ncua.gov/NCUABoard/index.htm* (NCUA Board).
- The Securities and Exchange Commission (SEC) (brokers, dealers, investment companies and investment advisers registered with the SEC): *www.sec.gov*.
- The state insurance authorities (insurance companies and any other persons engaged in providing insurance): *www.naic.org/state_web_map.htm* (links to state insurance agencies).
- The FTC (*see above*): *www.ftc.gov*.

Privacy Act. There is no centralised governing body that oversees the Privacy Act. The responsibility for compliance is dispersed among the federal agencies, often the agency's Chief Information Officer.

Officers or employees who contravene the Privacy Act can be prosecuted for criminal violations.

21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?

HIPAA. The HHS can impose on a covered entity a civil monetary penalty of US$100 (about EUR77) for each HIPAA violation, not to exceed US$25,000 (about EUR20,000) for multiple violations of an identical requirement or prohibition in a calendar year. The HHS cannot impose a civil monetary penalty in some circumstances such as where non-compliance was not discovered or where the failure was due to reasonable cause and is corrected within 30 days. The HHS has not, to date, issued a civil monetary penalty for a HIPAA violation.

The US Department of Justice has the authority to enforce criminal sanctions under the HIPAA. A person who knowingly, and in violation of the administrative simplification-related provisions of the HIPAA, uses or causes to be used a unique health identifier, or obtains or discloses individually identifiable health information to another person, can be fined up to US$50,000 (about EUR39,000) or be imprisoned up to one year, or both.

If the offence is committed under false pretences, the criminal penalties increase to a maximum fine of up to US$100,000 (about EUR78,000) or up to five years imprisonment, or both.

If the offence is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm, the criminal penalties increase to a maximum fine of US$250,000 (about EUR193,000) or up to ten years imprisonment, or both.

There are less than 10 reported cases to date in which individuals have been prosecuted for HIPAA criminal violations.

FACTA/FCRA. See *Question 20*. In addition to the possibility of criminal prosecution resulting in fines and imprisonment up to

two years for knowingly providing consumer reports in violation of the law or for obtaining a consumer report under false pretences, the FTC actively enforces against FCRA violations, and has brought numerous cases resulting in fines of hundreds of thousands of dollars and consumer redress recoveries of millions of dollars.

GLB. Each of the regulating agencies has the ability to enforce the GLB under the same enforcement mechanisms granted to the agencies under their otherwise applicable authorising statutes. In addition, individuals who obtain, attempt to obtain, cause to be disclosed or attempt to cause to be disclosed customer information of a financial institution relating to another person through a false, fictitious or fraudulent statement or representation, can be subject to fines and/or imprisoned for up to five years. If this crime or attempted crime is committed while violating another US law or as part of a pattern of illegal activity involving more than US$100,000 in a 12-month period, the perpetrator can be fined up to US$500,000 (about EUR385,000) (if an individual) or US$1 million (about EUR771,000) (if a company), and/or a prison term of up to ten years.

COPPA. The FTC or state Attorney Generals can bring enforcement actions and impose civil penalties up to US$10,000 (about EUR7,700) for each violation of the COPPA. The FTC has brought a number of cases against websites collecting children's personal information, which have generally been settled in exchange for the modification of the charged operators' policies and payment of fines of tens of thousands of dollars.

Privacy Act. Individuals affected by an agency's failure to comply with the Privacy Act can bring a civil action against the agency to recover actual damages sustained (in no case less than US$1,000 (about EUR771)) and the costs of the action including lawyers' fees. In addition, there are criminal penalties (misdemeanour and a fine of no more than US$5,000 (about EUR3,900)) for any employee or officer of an agency who:

- Wilfully discloses personal information.
- Maintains a system of records without meeting the notice requirements.
- Requests or obtains any record under false pretences.