



Table of Contents

McKesson Safe Harbor Privacy Policy	1
Employee Safe Harbor Privacy Notice	4
Notice Procedures	6
Choice Procedures	8
Data Integrity Procedures.....	11
Onward Transfer Procedures	12
Access Procedures	14
Security Procedures	17
Dispute Resolution Procedures	21
Enforcement Procedures.....	23



McKesson Safe Harbor Privacy Policy

McKesson recognizes that privacy is very important to our customers and employees, and therefore strives to protect the personal information it collects and handles. This Safe Harbor Privacy Policy (the "Policy") sets forth the privacy principles that McKesson follows with respect to transfers of personal information from the European Union (EU) to the United States (US).

Scope

This Safe Harbor Privacy Policy (the "Policy") applies to all personal information received by McKesson in the US from the EU. For the most part, that personal information pertains to McKesson employees. Nonetheless, McKesson US operations also provide third tier technical support for our UK operations, and may have access to personal information. However, McKesson US operations personnel do not have direct contact with those individuals about whom the information pertains.

Definitions

The following definitions shall apply throughout this Policy:

"Agent" means any third party that uses personal information provided to McKesson to perform tasks on behalf of and under the instructions of McKesson.

"McKesson" means McKesson Corporation., its subsidiaries, divisions, and business units in the US.

"Personal information" means any information or set of information that identifies an individual, or could be used by or on behalf of McKesson to identify an individual.

"Sensitive personal information" means personal information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that concerns health or sex life. In addition, McKesson will treat as sensitive personal information any information received from a third party where that third party treats and identifies the information as sensitive.

Privacy Principles

The privacy principles in this Policy are based on the Safe Harbor Privacy Principles.

Notice

When McKesson collects personal information directly from individuals in the EU, it will inform them about the purposes for which it collects and uses their personal information, the types of non-agent third parties, if any, to which McKesson discloses that information, and the choices and means, if any, that McKesson offers individuals for limiting the use and disclosure of their personal information. Notice will be provided in clear and



conspicuous language when individuals are first asked to provide personal information to McKesson, or as soon as practicable thereafter, and in any event before McKesson uses the information for a purpose other than that for which it was originally collected.

If McKesson receives personal information from its subsidiaries, affiliates or other entities in the EU, it will use such information in accordance with the notices such entities provided and the consents or choices made by the individuals about whom such personal information relates.

Choice
McKesson will offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a non-agent third party (unless allowed or required by contract), or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

For sensitive personal information, McKesson will give individuals the opportunity to affirmatively and explicitly consent (e.g., through an opt-in) to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

McKesson will provide individuals with reasonable methods to exercise their choices.

Data Integrity
McKesson will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. McKesson will take reasonable steps to ensure that personal information is relevant to its intended use, accurate, complete, and current.

Onward Transfer
McKesson will obtain assurances from its agents that they will safeguard personal information consistently with this Policy. If McKesson has knowledge that an agent is using or disclosing personal information in a manner contrary to this Policy, McKesson will take reasonable steps to prevent or stop the use or disclosure.

Access
Upon request, McKesson will grant individuals reasonable access to personal information that it holds about them, and McKesson will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete.

Security
McKesson will take reasonable precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Enforcement
McKesson will conduct compliance reviews of its relevant privacy practices to verify adherence to this Policy. Any employee that McKesson determines is in violation of this policy will be subject to disciplinary action up to and including termination of employment.



Dispute Resolution	<p>Any questions or concerns regarding the use or disclosure of personal information should be directed to the McKesson Privacy Office at the address given below. McKesson will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this Policy. For complaints that cannot be resolved between McKesson and the complainant, McKesson has agreed to participate in the dispute resolution procedures of the panel established by the European data protection authorities to resolve disputes pursuant to the Safe Harbor Principles.</p>
Contact Information	<p>Questions or comments regarding this policy should be submitted to:</p> <p>Leonard M. Patterson Associate General Counsel Law Department McKesson Corporation One Post Street, 33rd Floor San Francisco, CA 94104 (415) 983-8330 Leonard.Patterson@mckesson.com</p>
Changes to this Policy	<p>This Policy may be amended from time to time, consistent with the requirements of the Safe Harbor Principles. McKesson will provide appropriate notice about such amendments.</p>
Effective Date	<p>February 1, 2006</p>



Employee Safe Harbor Privacy Notice

This notice follows and is based on the principles set in the McKesson Safe Harbor Privacy Policy. The McKesson Safe Harbor Privacy Policy can be found at www.mckesson.com or can be requested directly by contacting one of the representatives listed below in the Contact Us section of this notice.

Scope

This notice sets forth the data privacy policy of McKesson (“we,” “us,” or “our”) concerning the transfer of personal information relating to its employees (“you” or “your”, or “individuals”) from the European Union to McKesson operations and corporate headquarter in the United States (US). In this statement, “personal information” means information that pertains to a present or former employee of McKesson and can be linked to that individual.

We collect and use personal information about you only for job-related purposes. By “job-related purposes,” we mean legitimate purposes reasonably related to your employment by McKesson, your performance of your job responsibilities for McKesson, or our ability to make services and benefits available to you as an employee.

Notice

We only transfer to McKesson US personal information about you for the purposes of payroll management, headcount, incentive and merit decisions, promotion, and your participation in benefits programs such as the Stock Option Program and the Employee Stock Purchase Program (ESPP).

The information that we transfer to the US includes your contact information such as name, address, McKesson identification numbers, existing compensation, performance ratings, proposed incentive and merit increase, and your eligibility for participation in McKesson benefits programs. This information is gathered for the purpose of human resource administration, and it is not further disseminated or used for any other purpose (e.g., marketing).

No sensitive information, as defined in our policy, is sent to the US. We therefore do not transfer to the US personal information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or that concerns health or sex life.

You are allowed access to the personal information we transfer to the US and can correct, amend, or delete information where it is inaccurate and as reasonably possible. We provide a list of local contacts below who can assist you in accessing your personal information.

Some European employees are eligible to participate in the Stock Option and Stock Purchase programs. If you are eligible to participate in either or both programs, you should be aware that for facilitating your participation in these programs, McKesson must share a subset of the information we transfer to the US with the third parties that assist us in administering these programs. Those third parties, Merrill Lynch and eTrade, receive basic payroll data such as name, address, base salary and your level of tax withholding.



Our agreements with Merrill Lynch and eTrade require them to treat your personal information in line with our Safe Harbor Privacy Policy with regard to the protection and handling of your personal information. In addition, we use a variety of security mechanisms when communicating with them to protect your personal information. However, if for any reason you are uncomfortable with the sharing of your personal information with these third parties you can prevent it by not enrolling in the Stock Option or Stock Purchase programs, or cancel your participation in those programs by contacting the McKesson representatives listed below.

Contact Us

To limit your information from transfer to Merrill Lynch and eTrade, and for any inquiries, complaints or concerns regarding the protection and privacy of your personal information

UK - Fiona Connor, UK Data Privacy Manager, Fiona.Connor@mckesson.co.uk

France, the Netherlands, and Ireland - Paul Nielsen, International Legal Director, Paul.Nielsen@mckesson.co.uk

To access your personal information and request to correct, amend, or delete inaccurate information

UK - Fiona Connor, UK Data Privacy Manager, Fiona.Connor@mckesson.co.uk

France - Stephanie Plangol, HR Director, Stephanie.Plangol@mckesson.fr

Netherlands – Monique van Elst, HR Director, mve@mckesson.nl

Ireland - Angela Glanton, HR Director, Angela.Glanton@mckesson.ie



Notice Procedures

Policy

When McKesson collects personal information directly from individuals in the EU, it will inform them about the purposes for which it collects and uses their personal information, the types of non-agent third parties, if any, to which McKesson discloses that information, and the choices and means, if any, that McKesson offers individuals for limiting the use and disclosure of their personal information. Notice will be provided in clear and conspicuous language when individuals are first asked to provide personal information to McKesson, or as soon as practicable thereafter, and in any event before McKesson uses the information for a purpose other than that for which it was originally collected.

If McKesson receives personal information from its subsidiaries, affiliates or other entities in the EU, it will use such information in accordance with the notices such entities provided and the consents or choices made by the individuals about whom such personal information relates.

Procedures

Providing Notice to Consumers

At this point, McKesson access to consumer data is limited to the third tier technical support it provides for its UK subsidiary as an agent. In this capacity, McKesson is not required to provide notice to consumers.

Review and Update

Implementation: Associate General Counsel, International Legal Director

- The content of the McKesson Safe Harbor Privacy Policy (Policy) and the Employee Safe Harbor Privacy Notice (Notice) will be reviewed on an annual basis to determine whether any changes or updates are required. The review will consider:
 - Changes in McKesson business practices
 - Changes in the requirements of the Safe Harbor program
- Upon making a changes to the Policy and/or Notice, the Associate General Counsel will inform the McKesson representatives who are directly involved with providing the notice to individuals or enforcing its privacy principles with the updated language.
- Upon making a change to the Policy and/or Notice, the Associate General Counsel will determine whether the change is substantial enough to merit the Policy and/or Notice re-issuance to the individuals that are subject to the updated practices.
- Changes and updates to the Notice and Policy will not deviate from the requirements of the Safe Harbor privacy principles.

Making the McKesson Safe Harbor Privacy Policy Available for Inspection

Implementation: Associate General Counsel

- The McKesson Safe Harbor Privacy Policy represents is the one and only statement that McKesson is required to make public. The Notice as well as the



accompanying procedures are internal and should be made available only to the relevant McKesson representatives for which the Notice pertains or who are required to follow the practices.

- McKesson will indicate in its communication with the Department of Commerce that it will make available its Policy upon request to the Associate General Counsel (current contact is Leonard Patterson).
- Upon receipt of a request for a copy of the Policy, will provide a copy of the Policy by either:
 - Sending the Policy in a PDF file format to the noted email address, or
 - Faxing or mailing a copy of the Policy to the noted contact information.
- Requests for a copy of the Policy will be answered within two business days if sent to the Associate General Counsel.

Providing Notice to Employees

New Hires

Implementation: European HR Directors

- The New Hires procedure refers to employees, temporary employees, contractor, agents, and interns.
- Before (or soon following the) commencement of an employment relationship with McKesson that will require the transfer of personal information to the US, the individual will be presented with McKesson Safe Harbor Privacy Policy (Policy) and the Employee Safe Harbor Notice (Notice).
- The HR Director will include copies of the Policy and Notice when presenting the individual with an offer letter.
 - In countries where local practices require a probationary period prior to presenting an individual with an offer letter, the Policy and Notice will be presented upon commencement of the probationary period.
- The Policy and Notice will be listed in any list or table of contents of materials that are provided to new McKesson employees.

Existing Employees

Employees will be provided with a copy of the Notice and Policy when invited to participate or renew their existing participation in the Employee Stock Purchase and Stock Option programs.

Written Confirmation

Although a written confirmation of receipt and acknowledgement are not required for the Policy and Notice, HR Directors, based on common local practices, may choose to collect such acknowledgements in the form of a signature for consistency purposes.



Choice Procedures

Policy

McKesson will offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a non-agent third party (unless allowed or required by contract), or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

For sensitive personal information, McKesson will give individuals the opportunity to affirmatively and explicitly consent (e.g., through an opt-in) to the disclosure of the information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

McKesson will provide individuals with reasonable methods to exercise their choices.

Procedures

At this point McKesson access to consumer data is limited to the third tier technical support it provides for its UK subsidiary as an agent. In this capacity, McKesson is not required to provide choice to consumers, but rather to limit the processing of the data as directed by McKesson UK.

Implementation: International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK)

- The International Legal Director and the UK Data Privacy Manager are the contacts for employees who wish to opt out of sharing of their personal information with Merrill Lynch and/or eTrade. The contact information for the International Legal Director and the UK Data Privacy Manager is as follows:

Fiona Connor
UK Data Privacy Manager
Fiona.Connor@mckesson.co.uk

Paul Nielsen
International Legal Director
Paul.Nielsen@mckesson.co.uk

- Once an employee requests to opt out of the third party sharing, the International Legal Director / UK Data Privacy Manager will send an email to the employee's McKesson address with an attachment of the Employee Opt Out Form. The form is to be faxed back to the the UK Data Privacy Manager or the International Legal Director with all the requested information completed and the form signed.
- Faxed with the Employee Opt Out Form should be a photo copy of the employee ID.
- The Employee Opt Out Form will include the following categories:
 - Employee name
 - Employee ID number
 - Employee home address

Providing Choice to
Consumers

The Opt Out Process



- McKesson affiliate company name
 - Description of the opt out request
 - Employee signature
 - A statement regarding the need to fax a copy of the employee's photo identification.
- The International Legal Director / UK Data Privacy Manager will verify the employee identity with the information provided with the Opt Out Form and will document the employee preference as described in the Employee Preference Log.
 - The International Legal Director / UK Data Privacy Manager will follow the relevant Choice procedures within five business days of receiving the opt out request.

Opting Out Prior to Program Participation

Implementation: International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK), EU HR Directors

Employee Stock Purchase Program

- No particular process is identified for opting employees out of the Employee Stock Purchase Program (ESPP) if they did not participate in the program previously. Employees who wish to opt out of having their information shared with eTrade (the third party administering the program) will not sign up for the program. Since registration to the program for European employees is based on the submission of the enrollment kit to Georgeson in New York, employees who do not submit those forms would in fact prevent their information from being forwarded to eTrade.
- The enrollment packet for the ESPP should include the Notice and McKesson Policy.

Stock Options

- McKesson will include a copy of the Notice in the Grant Notice employees receive.
- Employees wishing to opt out of having their information shared with Merrill Lynch are instructed in the Notice to contact the International Legal Director / UK Data Privacy Manager.
- The International Legal Director / UK Data Privacy Manager will document the employee preference in a log (Employee Preference Log) and will inform the HR Director in the employee country of operation within five business days of receiving the opt out request.

Opting Out After the Employee Has Begun to Participate in the Programs

Implementation: International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK), EU HR Directors, ESPP Administrator, Corporate Secretary

- Employees wishing to opt out of having their information shared with eTrade and/or Merrill Lynch are instructed in the Notice to contact the International Legal Director / UK Data Privacy Manager. The International Legal Director / UK Data Privacy Manager will document the employee preference as delineated in the



“Receiving and Documenting Employees Choice Preferences” procedure and will inform the HR Director in the employee country of operation.

- The International Legal Director / UK Data Privacy Manager will contact in the ESPP administrator or the Corporate Secretary (Stock Options) to inform of the employee preference within five business days of receiving the opt out request.
- The ESPP Administrator / Corporate Secretary will remove the employee information from the data feeds provided to eTrade / Merrill Lynch.
- The ESPP Administrator / Corporate Secretary will provide the International Legal Director / UK Data Privacy Manager with an email message confirming the removal of the employee information from the communication to the third party.
- The International Legal Director / UK Data Privacy Manager will document the confirmation in the Employee Preference Log.

Communicating Employees Preferences to HR

Implementation: International Legal Director, UK Data Privacy Manager

- The International Legal Director / UK Data Privacy Manager will send a message to the HR Director via email with the subject line reading “FOR ACTION – <EMPLOYEE NAME> OPT OUT OF < PROGRAM NAME>”.
- If the Privacy Officer receives any return message suggesting that the email was not delivered or will not be received by the HR Director prior to the bi-annual process of updating employees benefits in the US, the International Legal Director / UK Data Privacy Manager will proceed to contact other HR representatives in the respective country of operation.

Choice Verification Prior to Transfer to the US

Implementation: International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK), EU HR Directors

- Twice a year, one week prior to the transmission of the benefits offered to European employees to the US, the International Legal Director / UK Data Privacy Manager will transfer the names and employee ID numbers from the Employee Preference Log to the HR Directors in the countries of operations (each HR Director will receive only the information pertaining to employees in their care).
- HR Directors will ensure that no benefits updates are sent to the US without a review of the updated list from the Employee Preference Log.

The Employee Preference Log

Implementation: International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK)

The Employee Preference Log will include the information obtained in the Employee Opt Out Form, and the confirmation dates from the ESPP Administrator / Corporate Secretary, if applicable.



Data Integrity Procedures

Policy

McKesson will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. McKesson will take reasonable steps to ensure that personal information is relevant to its intended use, accurate, complete, and current.

Procedures

Date Integrity and Consumer Information

At this point, McKesson access to consumer data is limited to the third tier technical support it provides for its UK subsidiary as an agent. For this activity, there is no direct impact of the data integrity process.

Date Integrity

Implementation: McKesson Provider Technologies HR, Corporate HR, Corporate Secretary

- McKesson will take steps to ensure the European personal information it process is accurate, complete, reliable, and current by reviewing the data:
 - When updating existing data (e.g., extracting the information of terminated and retired employees from McKesson benefits)
 - When receiving new data (e.g., when receiving the proposed benefits and compensation for European employees)
 - When specific actions must be taken with the information, such as the creation of reports, reviews that are about to take place for specific decision making processes (e.g., reporting the updated list of employees who are eligible for Stock Options to the Corporate Secretary)
- The data integrity steps to be taken in those circumstances include review for:
 - Duplicate information
 - Missing data elements
 - Use of incorrect data elements
 - Including more identifiable information than necessary
 - Inaccurate use of identifiers (e.g., employee ID numbers)
 - Inappropriate inclusion or exclusion of individuals for the intended process or purpose.
- McKesson representatives handling European personal information may adopt an automated process for data integrity purposes, or, when an automated process is deemed unreliable, conduct the data integrity process manually.



Onward Transfer Procedures

Policy

McKesson will obtain assurances from its agents that they will safeguard personal information consistently with this Policy. If McKesson has knowledge that an agent is using or disclosing personal information in a manner contrary to this Policy, McKesson will take reasonable steps to prevent or stop the use or disclosure.

Procedures

Onward Transfer and Consumer Information

At this point, McKesson access to consumer data is limited to the third tier technical support it provides for its UK subsidiary as an agent. This activity does not include onward transfer activity.

Contracting

Implementation: Associate General Counsel

- McKesson will not provide a third party with the personal information of Europeans without contractually committing that entity to appropriate protection of that data as described by these procedures.
- All contracting with third parties outside of the EU that involves the processing of European personal information on behalf of McKesson in the US will be reviewed by McKesson's Associate General Counsel to ensure appropriate level of compliance with the Safe Harbor Program requirements and the Policy.
- The Enterprise Security Group (ESG) will review the electronic transmission of European data to a third party when first contracting with a new third party, and when changing the method of electronic communication with a third party or agent as described in McKesson's Safe Harbor security procedures.

Maintaining an Updated List of Third Parties

Implementation: Associate General Counsel

- McKesson Associate General Counsel will maintain a list of third parties with which contracts requiring compliance with McKesson's Safe Harbor requirements were implemented.
- The list of McKesson's third parties will include the name of the company, the effective dates of the contracts, and the contract number.

Limiting the Personal Information Shared with Third Parties

Implementation: Corporate Secretary, ESPP Administrator

- McKesson representatives will not provide a third party with more personal information than it deems as required to fulfill the task.

Inappropriate Disclosure, Use, and Protection of Personal Information

Implementation: All McKesson representatives handling European personal information.

- If a McKesson representative is notified or becomes aware of an inappropriate disclosure or protection of personal information or a practice of inappropriately



disclosing personal information by a third party, the McKesson representative will:

- Notify McKesson's Associate General Counsel
- Stop the practice or disclosure
- Document the event and the circumstances surrounding the event
- Forward the report to McKesson's Associate General Counsel and the International Legal Director. Where UK data or operations are involved, the UK Data Privacy Manager will receive a copy of the report as well
- In consultation and cooperation with the Associate General Counsel and the International Legal Director / UK Data Privacy Manager, take steps to mitigate any negative impact that may result from the inappropriate disclosure, if practical.



Access Procedures

Policy

Upon request, McKesson will grant individuals reasonable access to personal information that it holds about them, and McKesson will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete.

Procedures

Access and Consumer Information

At this point, McKesson access to consumer data is limited to the third tier technical support it provides for its UK subsidiary as an agent and is not impacted by the Access principle.

Existing Practices

European privacy and data protection regulations require McKesson to provide its employees with access to their personal information. In countries of operation where policies and procedures already exist for providing employees access, the existing practices should be followed.

Scope of the Access Procedures

- The following procedures should be followed where no documented processes exist in a particular McKesson European operation
- The delineated procedures are:
 - Based on the Safe Harbor requirement
 - Applies only to the non-sensitive payroll, merit, incentives, and benefits data elements that are transferred to the US.
- These procedures are not intended to replace or elevates the need for each European McKesson entity to create a local access process for its employees.

Implementation for the following Access procedures: European HR Directors, International Legal Director (for Ireland, the Netherlands and France), UK Data Privacy Manager (for the UK).

Access Requests

- McKesson European employees are instructed to contact their HR Directors with requests to access the personal information that pertains to them and that McKesson transfers to the US.
- When contacted by an employee with an access request, the HR Director will request the employee to submit their request in writing and specifically indicate the extent of the requested access (i.e., what is it that they want to review).
- Note that when the access request is vague or broad in scope, McKesson should engage in dialogue with the employee to better understand the motivation for the



Denying or Limiting Access Requests

request and therefore locate responsive information. Nonetheless, McKesson should understand that individuals are not required to justify their access request!

- Upon receipt of a written access request, the HR Director will have to first determine whether any reasons exist for denying or limiting the access request.

- Upon receipt of a written access request, the HR Director will review the requested records prior to sharing them with the employee to identify whether one of the following reasons apply and therefore require McKesson to deny the request, or limit the level of the employee access:
 - Interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial
 - Interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial
 - Disclosure of personal information pertaining to other individual(s) where such references cannot be redacted
 - Breaching a legal or other professional privilege or obligation
 - Breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies
 - Prejudicing employee security investigations or grievance proceedings
 - Prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations
 - Prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management
 - Other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

- If any of the exceptions may apply, the HR Director will consult with the International Legal Director to determine the response to the access request.

- When denying or limiting an access request, McKesson must to demonstrate the applicability of one or more of the circumstances delineated above and provide the employee with the International Legal Director's contact information for any follow up or related inquiries.

Providing Access

- If no reason exists for limiting the access of the employee to the record, the HR Director should set an appointment with the employee and review the records with them in person.
- When holding the meeting, the HR Director will verify the employee's identity by requesting to see a suitable picture ID.
- In cases where the HR Director cannot practically meet in person with the employee, the HR Director will make a copy of the records and arrange for the records to be sent to the employee's supervisor. The supervisor will meet with the employee and assist in the review of the records.



- McKesson will respond to an access request with the denial notice or with a proposed date for a meeting to review the records within five business days from receiving an access request in writing.
- When providing access, the HR Director may reformat the information as is deemed practical for both responding to the request and for the legibility of the data to the employee.
- The HR Director will inform the International Legal Director / UK Data Privacy Manager when providing employees with access to their records in response to an access request.



Security Procedures

Policy

McKesson will take reasonable precautions to protect personal information in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Procedures

Implementation for the following Security procedures: Any McKesson representative in the EU and the US who handles European personal information that is transferred to the US.

Mail

- All mail containing European personal information is to be delivered in sealed envelopes that are clearly marked as containing confidential information with the name of the sender and authorized recipient clearly marked.
- Internal mail containing personal information will only be addressed to the McKesson employee who is intended to receive it.
- When mailing European personal information to entities outside of McKesson, McKesson will take reasonable efforts to identify the individual authorized to receive the information and address the mailing accordingly.
- Misdirected mail containing European personal information will be resealed and marked as confidential before being rerouted to the appropriate individual that is authorized to receive it.
- McKesson will take reasonable steps to help ensure that all European personal information mailings it receives are appropriately protected from intentional and unintentional misuses and non-permitted disclosures as discussed above.

Fax

- Before faxing European personal information, McKesson will take reasonable steps to help ensure that the information is protected from unintentional disclosures by verifying that:
 - The fax machine on the other end can only be accessed by individuals authorized to handle the information, or
 - An authorized individual on the receiving end has been notified and is available to receive the information.
- When faxing European personal information, McKesson employee will use a cover sheet marked "Confidential" and addressed to the individual confirmed to be authorized to receive it.

Paper Documents

- McKesson will take reasonable steps to help ensure that European personal information is not left unattended at any time. To do so, McKesson will:



Electronic Documents

- Use locked file cabinets.
- Avoid leaving work related material on an open desk (i.e., a “clean desk” policy) to mitigate the risk of leaving personal information unattended during and at the end of the work day.
- Lock mail (internal and external) that contains European personal information at the end of the workday. Mail should not be left unattended in mail boxes located in open areas.
- Access to offices, rooms, and cabinets where McKesson maintains personal information will be limited to only those employees with authorized access.
- Shredding or burning will be used by McKesson for discarding all documents containing personal information (including scrap paper and fax confirmation sheets). McKesson will ensure the existence of a locked central repository for that purpose (e.g., locked burn box).
- When leaving their desk, McKesson employees will lock their computer terminals to avoid unauthorized access.
- Electronic documents containing European personal information will be emailed only in password protected files.
- This requirement applies to all email communication within the McKesson email system – from Europe to the US, as well as in the US.
- When sending a password protected file, the sender will provide the password to the recipient over the phone.
 - The sender may leave the password in a voice mail for the recipient, if the recipient is not available to receive the call.
 - The sender will not sent the password via email.
- When sending European Personal Information via email, the communication must be marked "Confidential" and an appropriate confidential label must be used.
 - Confidentiality notice: This e -mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.
- McKesson will consult with the ESG regarding any electronic security procedures, including the use and update of passwords, the implementation of software and hardware, and the transmittal of European personal information in electronic format (e.g., email) on the intranet and the Internet.
- Communications with third parties and agents will follow McKesson's Safe Harbor security procedures.
- The ESG will review the electronic transmission of European data to a third party or agent when:
 - Contracting with a new third party or agent

Consultation with the
Enterprise Security Group



- Changing the form of communication with a third party or agent.

- For additional information regarding secure electronic communication see McKesson's policies that are maintained by the ESG and can be found at <http://mcknethost.mckesson.com/esg/secpol.asp>. If there are any specific questions about information security, please forward them to the ESG.

Retention

- Following McKesson's policy, European employee personal information in hardcopy will be retained for a period of seven years.
- Electronic documents containing personal information will be retained on business units' secure shared drives.
- McKesson will consult with and follow the guidance of the ESG regarding the appropriate security standards applied for the retention of sensitive information.
- Retention of other European personal information in any format will follow McKesson's Corporate Record Retention Schedule. Any questions pertaining to how long a record must be retained according to the current Corporate Record Retention Schedule should be directed to Linda Phillips, Corporate Records Manager, who is located in Carrollton, TX; Linda.Phillips@mckesson.com, 972-446-4251.

Remote Access to European Personal Information

- When required to remotely connect from the US to a system that is located in the EU and that contains personal information (e.g., for providing third tier technical support to the UK affiliate), McKesson will:
 - Utilize tools and mechanisms, such as PCAnywhere, that will leave the control over the remote access in the hands of the European representative handling the system. The remote access cannot be initiated in the US without the control and cooperation from the EU side.
 - Avoid directly accessing the personal information on the system if not required for performing the task at hand.
 - Avoid retaining any personal information from the system in any format (printing, making electronic copies, capturing image of the data, etc.) that is not necessary to fulfill a business need.

Administering Access to Systems Containing European Personal Information

- Access to European personal information will be assigned on a need to know basis, limiting employee access to information only to those data categories directly related to their work requirements.
- McKesson will follow a formal and documented process for submitting and evaluating access requests to systems with European personal information (e.g., HR PeopleSoft)
- Access requests will be evaluated and approved by the McKesson representative in charge of the information and/or individuals to which the information pertains (e.g., the payroll manager will approve access to payroll data).
- Access to European personal information will only be granted after the requesting employee has completed the Safe Harbor privacy training.



- The access control lists of systems containing European personal information will be reviewed quarterly to identify and eliminate any outdated access privileges.



Dispute Resolution Procedures

Policy

Any questions or concerns regarding the use or disclosure of personal information should be directed to the McKesson Privacy Office at the address given below. McKesson will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this Policy. For complaints that cannot be resolved between McKesson and the complainant, McKesson has agreed to participate in the dispute resolution procedures of the panel established by the European data protection authorities to resolve disputes pursuant to the Safe Harbor Principles.

Procedures

Implementation for the following Dispute Resolution procedures: Any McKesson representative in the EU and the US who handles European personal information that is transferred to the US.

Dispute Resolution

- Since McKesson transfers employee personal information to the US from Europe, McKesson is required to cooperate with the European Authorities for the purpose of complaint investigation and dispute resolution.
 - The Associate General Counsel will pay the annual fee for cooperation with the European Data Protection Authorities for privacy dispute resolution.
- McKesson will attempt to resolve complaints and concerns directly so that those issues will not need to escalate to the European Data Protection Authorities.

Employee Complaints

- When faced with a privacy concern or complaint that is raised in Europe, the HR Director will:
 - Respond directly within one business day, or
 - Refer the employee to the International Legal Director, or in the UK to the UK Data Privacy Manager. When referring the employee, the HR Director should contact the International Legal Director / UK Data Privacy Manager to alert them of the fact that they will be contacted by the employee.
 - The International Legal Director / UK Data Privacy Manager should respond to the employee complaint within one business day. The Associate General Counsel should be contacted to support the resolution of the complaint/concern as necessary.

Other Complaints

- The International Legal Director / UK Data Privacy Manager should handle privacy complaints.



The Data Protection
Authorities Involvement with
Resolving Employee
Complaint

- An initial response to a complaint, even if just a confirmation that the complaint was received and is investigated, should be provided to the complaining individual/entity within one business day. The Associate General Counsel should be contacted to support the resolution of the complaint/concern if it involves the transfer of personal information to the US.
- The Associate General Counsel, International Legal Director, and UK Data Privacy Manager should be contacted immediately when a McKesson affiliate company is contacted by a Data Protection Authority (DPA) in response to a privacy complaint or concern.
- All communications with the DPA should be handled directly by the Associate General Counsel.
- Dispute resolution decisions (also referred to as “advice”) issued by a DPA should be complied with within 25 days, unless otherwise instructed by the DPA.



Enforcement Procedures

Policy

McKesson will conduct compliance reviews of its relevant privacy practices to verify adherence to this Policy. Any employee that McKesson determines is in violation of this policy will be subject to disciplinary action up to and including termination of employment.

Procedures

Ongoing Compliance Reviews

Implementation: Associate General Counsel

- During the year, the Associate General Counsel will conduct compliance reviews to ensure that the Safe Harbor Privacy Policy and Procedures are effectively implemented.
- The Associate General Counsel will choose and conduct three of the compliance review options listed below.
- If the review suggests a consistent failure to directly comply with the procedures requirements (e.g., not complying with a specified timeframe for a response or action on McKesson's side), the Associate General Counsel will review the existing processes to determine what changes should be implemented.

Compliance Review Options

Notice

- Review recent requests for copies of the Safe Harbor Privacy Policy and verify whether recent requests were answered within two business days as specified in the Notice procedures.

Choice

- Review the documentation around the opt out process of employees. This review should include a review of the written preference requests submitted by employees, the documentation of the employee preference in the Employee Preference Log, and adherence to the timeframe indicated in the procedures.
- Verify the opt out implementation by requesting from the Corporate Secretary and the Employee Stock Purchase Program (ESPP) Administrator the list of employees that are transferred to Merrill Lynch and eTrade and compare those lists with the most current version of the "European Employees Choice Preference Inventory.
- Verify that the Employee Safe Harbor Privacy Notice (Notice) and McKesson Safe Harbor Privacy Policy (Policy) are included in the enrollment packet for the ESPP.

Data Integrity

- Verify that terminated and retired employees are accurately excluded from benefits systems (e.g., Transcentives).

**Access**

- Verify that access requests received by HR Directors are followed up on within the required timeframe indicated in the procedures.

Security

- Verify that access to European personal information was only granted after the requesting employee has completed the Safe Harbor privacy training.
- Review the Access Control List of PeopleSoft for European employee data to identify whether inappropriate or outdated access privileges exist.

Employee Discipline

Implementation: Associate General Counsel, US HR Directors

- Any violation of the Safe Harbor Privacy Policy and Procedures by a McKesson employee are to be reported to the Associate General Counsel.
- When becoming aware of an employee privacy violation, the Associate General Counsel will:
 - Arrange a confidential meeting with the individual(s) who are making the allegation against the employee.
 - Arrange a confidential meeting with the employee(s) who are identified as allegedly failing to comply with the privacy requirements.
 - Conduct a confidential investigation of the facts involved in the allegation.
 - If confirmed, notify HR and document the violation in the employee record as well as any other business unit specific operational reports.
 - In cooperation with the local HR Director, determine the sanction to impose on the employee.
 - Ensure that HR document any reached resolution and imposed sanction.

Sanctions

- Sanctions will be imposed as appropriate to the nature of the privacy violation committed based on McKesson's Progressive Discipline Guidelines.
- Imposed sanctions may range from a warning to termination of employment.
- In considering disciplinary actions against an employee McKesson will take the following into consideration:
 - The severity of the violation
 - Whether the violation was intentional or unintentional
 - Whether the violation indicates a pattern or practice of improper use or disclosure of personal information.
- Employee privacy violations will be taken into consideration in any internal process of employee evaluation.