Privacy and Data Protection Risk Assessment Questionnaire

Notice:	
Question:	**Response (Yes, No, Some)**
Has your business area provided notice to each person where it is either legally or otherwise required by Lilly or local regulations?	
Please indicate whether each of the following are included in these notices: • Purpose for collection and use of the information • Information as to how individuals can contact the company with concerns, questions, or issues • Types of third parties to whom this information is disclosed • How the organization limits its use and disclosure of this information	

Choice: - Please place an "x" by each set of individuals that the business area collects, stores, or processes information about. For each set of individuals with whom you collect, store or process information, please note the type of notice you provide to these individuals prior to managing their information (Written, Electronic, Verbal, None)

Individuals:	**Response (Yes, No)**	**Written, Electronic, Verbal, None (if response was no, leave this column blank)**
Employee		
Health Care Professional		
Consumers		
Clinical Investigator		
Clinical Trial Patient		
Other data subject (please specify)		
Question:	Response (Yes, No, Some)	
Does the business area have documented procedures or processes to manage requests from individuals that allows them access to, copies of, corrections to, or removal of their personal information?		

Privacy and Data Protection Risk Assessment Questionnaire

Onward Transfer:	
Question:	**Response (Yes, No)**
Do third parties manage information for the business area?	
Does the business area have an inventory of where personal information is collected, stored, processes or managed?	
If yes, does this inventory document what is collected, stored and processed?	
If yes, is this data transferred to another organization or entity within Lilly?	
If PI is transferred, place an "x" by each type of control used to protect the PI. • SOPs • Access Control Lists • Periodic Reviews of Access Control Lists • Secure Email • Virtual Privacy Network • File-based encryption • Secure, dedicated line transfer	
Are there documented agreements in place with external organizations, when transferring data between a company entity and an external organization, requiring the external organization to comply with the company's privacy expectations?	

Security:	
Question:	**Response (Yes, No, Unsure)**
Please verify whether the business has control procedures (SOPs, access requirements, periodic reviews, etc.) in place to limit company agent (employee, contractor, vendor, alliance partner, etc.) access to PI ONLY to those having a business need for such access?	
Can the business produce a list of all individuals having access to PI (whether it is electronic data, hard copy data, etc.)	
Question:	**Response (Quarterly, Semiannually,Annually, Biennially. Never, Other)**
How often is systems access reviewed and individual access rights updated?	
Question:	**Response (Yes, No)**
Which of the following methods do you use when transferring PI? • SOPs • Access Control Lists	

Privacy and Data Protection Risk Assessment Questionnaire

• Periodic Reviews of Access Control lists • Secure Email • Virtual Privacy Networks • File-based encryption • Secure, dedicated line transfer	
Place an "x" by the security measures the business area regularly uses to physically protect PI? • Security card access – building • Security card access – room or work area • Locked file cabinets • Clean Desk Policy / Procedure	
Is the business area following privacy guidance when collecting, storing, or processing PI via electronic, audio, visual or print media?	

Data Integrity:	
Question:	**Response (Yes, No)**
Does your business area comply with the Global Records Retention Schedule with regard to PI or SPI?	
Do you routinely access / review / monitor your affiliate or business area to determine whether the PI collected, stored, or processed is necessary to meet the stated business objectives?	
Are privacy stewards aware they must report unauthorized PI disclosures (for example, lost backup tapes containing PI) to the Global Privacy Office or to the Chief Privacy Officer?	
Enforcement: Has management actively informed employees of their responsibility, except where prohibited by law, to report incidents or suspected incidents involving personal or	