Privacy Controls
Personal & Medical Data Security Requirements

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed Phone #, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Education, Income Range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status, Reasons for leaving**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal Background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Disclosure Restrictions	Who should decide on whether the data can be disclosed internally & externally?	Holder	Holder	Owner	Owner	Owner
Review of Authorizations	How often should authorization lists be reviewed? How often should user privileges be reviewed?	12 months 12 months	6 months 6 months	6 months 6 months	6 months; in addition, conduct a review with the data owner or designee once per year 6 months	6 months; in addition, conduct a review with the data owner or designee once per year 6 months
Authentication[I]	What level of authentication of the identity of the person attempting to view or update data is required?	Single factor authentication required	Single factor authentication required	Single factor authentication required. Two level (Example: Network and Application) authentication where possible.	Single factor authentication required. Two level (Example: Network and Application) authentication where possible.	Single factor authentication required. Two level (Example: Network and Application) authentication where possible.

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Contact details, Education, Income range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status, Leaving reason**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Storage of Data	How should information be stored on non-Company equipment	Encryption not required	Approval required for information stored on non-Company equipment.	Approval required for information stored on non-Company equipment.	Approval required for information stored on non-Company equipment.	Approval required for information stored on non-Company equipment.
	How should information be stored on Company desktops	Encryption not required	Non-employee: Protect based on non-disclosure agreement	Encryption recommended	Encryption Required	Encryption Required
	How should information be stored on Company laptops or portable storage devices	Encryption not required	Encryption required	Encryption required	Encryption required	Encryption required
	How should information be stored on Company servers	Encryption not required	Encryption not required	Encryption recommended	Encryption required	Encryption required
	Stored on a server owned by a third party	Encryption not required	Encryption required	Encryption required	Encryption required	Encryption required

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Phone #, Contact Details, Education, Income Range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status , Leaving reason**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Copying	Can the data be copied?	At discretion of holder	At discretion of holder	At discretion of owner	At discretion of owner	At discretion of owner
Sharing of data	With whom can the data be shared? Internal to Company:	Employees with a need to know	Employees with job-related need to know	Employees with job-related need to know	Employees with job-related need to know	Sharing with the data subject is at the discretion of the owner. Owner may release data only on a job-related need to know basis.
Sharing of data[II]	3rd Parties: What can each party do with the data?	3rd parties with written agreements containing data privacy clauses required for some data types.	3rd parties with written agreements containing data privacy clauses. Use based on job- related need as determined by the holder.	3rd parties with written agreements containing data privacy clauses. Use based on job- related need as determined by the owner.	3rd parties with written agreements containing data privacy clauses. Use based on job-related need as determined by the owner.	3rd parties with written agreements containing data privacy clauses. Use based on job-related need as determined by the owner.

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Contact Details, Education, Income range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status** [Leaving Reason]	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Access to Data by Subject	Should subject have access to this data?	Access is to be provided unless the data is commingled with others' personal data, or if the data is collected in relation to an investigation of the individual and access would compromise the investigation.	Access is to be provided unless the d a t a is commingled with others' personal data, or if the data is collected in relation to an investigation of the individual and access would compromise the investigation.	Access is to be provided unless the d a t a is commingled with others' personal data, or if the data is collected in relation to an investigation of the individual and access would compromise the investigation.	Access is to be provided unless the data is commingled with others' personal data, or if the data is collected in relation to an investigation of the individual and access would compromise the investigation.	For employee & medical related benefits data, data subject is entitled to have access to their personal data. Special rules apply for access to medical data. Check with data owner on the applicable rules.
	Should subject be able to provide corrections to their own data?	Procedures must be implemented to provide for correction of data requested by the subject.	Procedures must be implemented to provide for correction of data requested by the subject.	Procedures must be implemented to provide for correction of data requested by the subject.	Procedures must be implemented to provide for correction of data requested by the subject.	For employee & benefits medical data, the owner has the responsibility to ensure that procedures are implemented to address the data subject's ability to access and amend their personal records.

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed Phone #, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Contact Details, Education, Income range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status, leaving reason**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Hardcopies	How should data be handled in hardcopy format?	Must be in locked storage after business hours.	Must be in locked storage after business hours & access restricted when in use. If in a physically controlled environment, hardcopies do not need to be placed in locked storage when the holder's office is unoccupied.	Must be in locked storage after business hours & access restricted when in use. If in a physically controlled environment, hardcopies do not need to be placed in locked storage when the holder's office is unoccupied.	Must be in locked storage when not in active use & access restricted when in use. If in a physically controlled environment, hardcopies need to be placed in locked storage when the holder's office is unoccupied.	Must be in locked storage when not in active use & access restricted when in use. If in a physically controlled environment, hardcopies need to be placed in locked storage when the holder's office is unoccupied.

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed Phone #, Language, Country of Residence, Age Range**	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Contact Details, Education, Income range, Vet/Immigration status** [Any other personal data not identified]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status, leaving reason**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background Driver's license #**	**Medical-related benefits data, Employee medical data**
Transmission / Travel	Should data be encrypted for transmission internally or externally? Is encryption required when transmitting data through a public networks between computers?	No encryption required No encryption required	Encryption required for external transfer, may be accomplished through the network or software. No encryption required, however it is recommended	Encryption required for external transfer, may be accomplished through the network or software. Encryption required.	Encryption required for internal & external transfer, may be accomplished through the network or software. Encryption required.	Encryption required for both internal & external transfer, may be accomplished through the network or software. Encryption required.
	Should reports containing data be double wrapped for internal mail?	No Requirement	Security envelope[iii]	Lock boxes, or security envelopes	Lock boxes, or security envelopes	Lock boxes, or security envelopes
	Should reports containing data be double wrapped for external mail?	No Requirement	Security envelope	Security envelope	Security envelope	Security envelope
	For external mail, can this data be sent from Company to the subject on a postcard?	Can be sent on a postcard	Only the subject's home address data can be sent on a postcard to the subject.	Cannot be sent on a postcard	Cannot be sent on a postcard	Cannot be sent on a postcard

Action to be Taken or Controlled	Classification Label:	Public	Unrestricted Internal Use	Confidential	Restricted	(Medical Data) Restricted
	Bolded data items must be handled according to the controls listed. For Non-bolded items, the controls listed are recommended controls.	**Name, Home Address, Listed Phone #, Language, Country of Residence, Age Range** [Any other personal data not identified]	**Home email address, Non-medical related benefits data, Marital status, # of children, Date of Birth, Age, Gender, Citizenship, Internal ID numbers, Contact Details** [Education, Income Range, Vet / immigration status]	**Salary or Compensation or Performance Data, Corporate Tax ID, Race, National origin, Religion, Union membership, Sexual orientation, Political affiliations, Disability status, leaving reason**	**Credit card #, SSN, Bank account #, Credit history, Loan Account #, Consumer/Client Account #, Government ID #, Passwords, Criminal background, Driver's license #**	**Medical-related benefits data, Employee medical data**
Audit Trail	What audit records, if any, should be created for actions against this data besides system event logs & privileged user actions?	Audit records required for queries, changes and deletions to the data must be recorded.	Audit records required for queries, changes and deletions to the data must be recorded.	Audit records required for queries, changes and deletions to the data must be recorded. All access attempts should be recorded.	Audit records required for queries, changes and deletions to the data must be recorded. All access attempts should be recorded.	Audit records required for queries, changes and deletions to the data must be recorded. All access attempts should be recorded.
Recording Requirements	How must disclosures be handled? Does receipt of data need to be recorded?	Disclosures are required to be recorded Recording of receipt required	Disclosures need to be recorded. Recording of receipt not required	Disclosures need to be recorded. Recording of receipt as required by law.	Disclosures need to be recorded. Recording of receipt as required by law.	All disclosures must be documented. Recording of receipt as required by law.
Disposal/ Destruction	How should documents containing the data be disposed of? Do you need to destroy electronic media or does it require a controlled erasure?	Burn, shred or other approved means of controlled destruction, pulverize or destroy media if it cannot be repaired. Controlled erasure not required for redeployment within Company.	Burn, shred or other approved means of controlled destruction, pulverize or destroy media if it cannot be repaired. Controlled erasure required for redeployment	Burn, shred or other approved means of controlled destruction, pulverize or destroy media if it cannot be repaired. Controlled erasure required for redeployment	Burn, shred or other approved means of controlled destruction, pulverize or destroy media if it cannot be repaired. Controlled erasure required for redeployment	Burn, shred or other approved means of controlled destruction, pulverize or destroy media if it cannot be repaired. Controlled erasure required for redeployment

NOTES:

i Certain collections (spreadsheets, databases, etc.) of personal data may require two-level authentication and encryption at the direction of the Chief Information Security Officer.

ii If personal data is made available to Third Parties without the consent of the Data Subject, the Owner or Holder must ensure that each Third Party is contractually obligated to protect the security & privacy of such information as required by these Standards and Controls. Exceptions to this requirement exist when the personal data is Company property or when it is made available to the Third Party:

(i) pursuant to law, regulation, court order or administrative agency request; (ii) to comply with a legal obligation; (iii) for use by law enforcement personnel; or (iv) to protect the interests of an employee. For Personal Data, that may include Name, Language & Country of Residence, is available in the Public Domain, and when included in a file or database less than 1000 records this information is not subject to the contractual requirements stated above.

iii A security envelope is colored, lined or has inside markings sufficient to conceal the internal contents of the envelope when unopened.