Gallagher

Insurance | Risk Management | Consulting

Document ID: GPO_PDDS_00	**Title: Global Personal Data De-Identification Standard**
Effective Date: 1 June 2024	**Revision No. 0**
Business Process Owner:	**Global Chief Privacy Officer**
Document Type: Standard	**Exhibits: N/A**

Overview & Purpose

Our employees, clients and regulators expect and require that we protect their Personal Information (PI). Meeting these expectations and requirements is key to our ongoing success. Arthur J. Gallagher & Company and its subsidiaries and affiliates (the "Company", "Gallagher", "we", "us", "our") are committed to protecting PI under our care and complying with current laws and regulations.

We regularly use information to serve our clients and colleagues. Some of the information we use is considered Personal Information (PI). The processing of PI (which includes, without limitation, the collection, use, disclosure, transfer, and retention of PI) is typically subject to:

(i) Applicable legal and regulatory requirements;
(ii) Client-facing privacy notices, disclosures and statements;
(iii) Contractual obligations; and
(iv) Company policies and procedures.

As such the processing of PI beyond the intended purposes for which it was collected is often legally challenging. However, De-identified Information may not be subject to the same processing restrictions as PI. As such, we have adopted this Standard to inform when a dataset containing PI can be declared De-identified Information.

Capitalized terms have the meanings given to them in the Section 1.0 below.

Scope

This Standard is applicable to all officers, directors, permanent and temporary employees, contractors, consultants, and secondees of the Company ("you", "your", "Employees") and lays out your obligations with respect to the rules and controls that should be applied when a user of a dataset seeks to declare that the PI in the dataset is De-identified.

This Standard has been written in accordance with accepted industry standards and best practices and takes into account certain laws and regulations that have requirements on De-identified Information. It is not, however, meant to serve as a comprehensive guide to comply with every privacy law or regulation or to meet specific standards under applicable contracts, privacy statements or notices issued by the Company. Users of this Standard should always verify that there are no other stricter requirements that apply.

This Standard must be read in conjunction with local entity procedures, which may set more stringent requirements but which may not lower the requirements within this Standard, without the written authorization from the Global Chief Privacy Officer.

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

This Standard applies to all datasets that are meant to be declared as De-identified Information, whether the datasets are "structured" (data that conforms to a data model, has a well defined structure, e.g., databases), "semi-structured" (contains some level of organization or structure but does not conform to a rigid schema or data model, and may contain elements that are not easily categorized or classified, e.g., JSON) or "unstructured" (data that has not been structured in a predefined manner, e.g., file shares). In the event it is not possible to apply this Standard to a category of PI in the dataset, that PI must be deleted from the dataset in order to have it viewed as compliant with this Standard (unless an exception is sought from and approved by the Global Chief Privacy Officer).

This Standard supplements and does not replace requirements documented in other policies and standards, such as in the Global Information Privacy Policy, the Global Information Classification and Handling Policy and the Global IT Policy and Standards Manual.

If you have questions or concerns regarding how to apply this Standard, please contact GlobalPrivacyOffice@ajg.com .

In this Standard we use the word "must" to mean a mandatory requirement. In contrast, "should" indicates that the statement is best practice and it is recognised that there will be some circumstances in which the approach is not appropriate. You must be able to demonstrate why the approach is not appropriate if you do not adopt best practice.

Out of Scope

This Standard need not be consulted if you do not seek to declare a dataset containing PI as De-identified. This Standard also does not apply to the de-identification of commercial information (namely, data that is not PI).

Standard

1.0 Definitions

"**Aggregate Information**" mean PI that relates to a group or category of individuals, from which Direct Identifiers have been removed, and that is not linked or reasonably linkable to any unique individual. Aggregation is often done to produce high-level observations such as "demographics" or "trend analyses", also known as data analytics. Because in some cases it may be possible to reverse engineer the Aggregated Information to re-identify individuals, Aggregate Information is not automatically considered Anonymized Information. *In order to be considered Aggregate Information, the dataset must meet the minimum requirement set forth in section 3.0.*

"**Anonymized Information**" means De-Identified Information which, through the application of further techniques and measures, achieves **technically irreversible** De-identification. True Anonymization is a difficult standard to meet as it assumes that no other datasets and / or publicly available information can be used to reverse engineer the dataset into a re-identified form, whether done by the data owner, the Company or any third party who may obtain the dataset. *As a general rule we tend to avoid declaring any dataset as Anonymized Information because it will rarely be true.*

"**Cell**" means a group or individuals with the same Individual Identifiers. For example, a Cell within a dataset encompassing all Company employees is all female Legal colleagues in Rolling Meadows.

"De-identified", "De-identification" or "**De-identified Information**" means PI from which all Direct Identifiers *and* sufficient Indirect Identifiers have been removed (in accordance with this Standard), such that the resulting dataset can no longer **easily** identify or be linked to the individuals to whom it pertains. Because De-identified Information can ultimately be re-identified by the Company or others, it does not constitute Anonymized Information (for which re-identification is technically infeasible). However, in many jurisdictions De-identified Information is no longer considered PI, and is thus not subject to the same restrictions on processing, collection, use, disclosure, transfer, and retention of PI, with some important exceptions outlined in Section 4.0 below.

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

"**Personal Identifiers**" means data elements that can directly or indirectly identify a unique individual. Personal Identifiers are generally separated into two categories (see Appendix A for examples of each):

- "**Direct Identifiers**" means data elements that can directly identify a unique individual.
- "**Indirect Identifiers**" means data elements that do not directly identify a unique individual but can be used to identify the individual when combined together with other indirect identifiers or other information.

"**Personal Information (PI)**" as defined in the Global Information Privacy Policy, means any information relating to an identified or identifiable natural person, i.e., any PI that directly identifies a person and PI that if used in combination with other information identifies a particular person or relates to an identifiable person.

"**Pseudonymized Information**" means PI from which all Direct Identifiers have been removed and replaced with other pseudo-identifiers such that the information cannot be attributed to a specific individual without the use of additional information to reverse the pseudo-identifier. While Pseudonymization offers some limited protection for PI, Pseudonymized Information is generally easy to re-identify and is treated the same as PI under various legal standards.

2.0 De-Identification Principles

1. PI does not need to be De-identified when it is used to provide the service for which it was collected or to fulfil contractual obligations related to the PI. This includes use of the PI to directly market to the individuals who gave us their PI for such a purpose (subject to any applicable marketing-related legal and regulatory requirements).
2. PI should be De-identified whenever it is shared with another Gallagher entity, function, service provider or other third party that does not have a need to know the information in connection with the service being provided, or if the disclosure is for a purpose materially different than the purpose for which the information was collected.
3. Where another Gallagher entity, function, service provider or third party is given access to information in connection with a service being provided and such access also results in access to PI, the PI must not be used for any purpose not authorized by the dataset owner.
4. If an internal or external third party is performing the De-identification, and such De-identification process requires that they have access to the fully identifiable dataset, the recipients must be bound by documented confidentiality obligations and obligations to never seek to re-identify the information information within the dataset.

3.0 Methods of De-identification

Unless otherwise noted in Section 4 below, De-identification can be achieved by four methods:

1. **Removal of Direct and Indirect Identifiers –** as a general rule, a dataset can be declared De-identified if it meets the following criteria:

    a. **No Direct Identifiers** for any individual included in the dataset.

    b. **Indirect Identifiers** are allowed only if the number of unique individuals associated with any possible permutation of Indirect Identifiers in the dataset is 10 or more (the "**Cell Size Rule**")

        i. Note that in order to meet the Cell Size Rule, it may be necessary to mask or Aggregate the data associated with a particular Indirect Identifier. For example, instead of identifying a specific date of birth, consider using ages (e.g., years of birth or numeric age) or age ranges (e.g., 20-30 year olds). As a simple illustration, consider a dataset that includes no Direct Identifiers and three Indirect Identifiers per record: gender, country of residence, and date of

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

birth. If you filter by male + Schaumburg + December 1, 1980, and your result includes only two records, your dataset would fail the Cell Size Rule. To render the dataset De-identified, consider replacing date of birth with birth year and re-running the query. If you have ten (10) or more results for male + Schaumburg+1980 – and for all other possible queries of the dataset – your dataset is sufficiently De-identified to meet this Standard.

For examples of technical steps that may be taken to confirm the Cell Size Rule, see Appendix B.

2. **Aggregation –** in order for Aggregate Information to be considered De-identified under this Standard, the Cell of individuals whose information is being summarized, categorized, or presented must meet the Cell Size Rule in the underlying dataset. In other words, as long as the Aggregated result is produced by querying a Cell which has 10 or more individuals, the Aggregate result is De-identified. This is true even if additional non-Personal Identifiers are used to narrow the Aggregated result down to fewer than 10 individuals.

   For example, 200 individuals are surveyed about their experience with a call center. 10 respondents are females between the ages of 30-40. A report or analytics tool may display the fact that 10 individuals who took the survey were females aged 30-40, as this meets the Cell Size Rule. The Aggregate results for this Cell rated their satisfaction with their call center experience as “low”. Because level of satisfaction is not an Indirect Identifier, this display does not violate the Cell Size Rule. If, however the same subgroup was further refined by another Indirect Identifier (e.g., city), and all 10 respondents did not share the same city, then the underlying Cell size would drop below 10 and the reporting would not be considered De-identified. (Note: The Aggregate Information may still be used / displayed if De-identification is not required based on the intended audience or purpose of the report.)

3. **Pseudonymization –** in order to achieve Pseudonymization, a dataset that contains PI needs to manipulated to meet all of these criteria:

   a. All Direct Identifiers are removed from the original dataset and placed in a new dataset in which a random unique identifier is generated representing the unique individual and / or the unique record or each member of the dataset.

   b. Indirect Identifiers may remain in the original dataset provided the dataset meets the Cell Size Rule to avoid a risk of identification of individuals.

   c. The random unique identifier must not be derived from or related to PI of the individual (including the use of an irreversible one-way hash of such PI) as this creates a risk of unauthoirized re-identification.

      Acceptable Alternative – if there is a business justification to use a non-random unique identifier, meaning one based on the PI, then one of the following options must be adhered to:

      i. The underlying PI should be manipulated (a/k/a “salted”) and an irreversible one-way hash is applied; or

      ii. The party receiving the dataset with the non-random unique identifier has destroyed the original dataset; or

      iii. A third party is engaged to perform the generation of the non-random unique identifier and destroys the original dataset.

   d. The new dataset that includes the random unique identifiers and the Direct Indentifiers must be encrypted and kept separate from the original dataset (which no longer contains Direct Identifiers) and is subject to technical and organizational measures to prevent co-mingling with the original dataset. This dataset may not be used or disclosed for any purpose other than an authorized re-identification of the original dataset.

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

As an illustration, consider a dataset with Gallagher employee names and compensation information. If you strip out the names and replace them with a random number, the dataset would be Pseudonymized, provided the dataset that maps the random numbers to the names is encrypted and held separate from the original dataset. The encryption key must also be kept separately. This Pseudonymized dataset could only be declared De-identified if the dataset that maps the names to the random numbers was deleted and no longer exists, thus removing the ability to re-identify the data.

4. **Expert Determination** – this is a method whereby a person or persons, typically external to the Company, with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

    a. Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

    b. Documents the methods and results of the analysis that justify such determination.

    It is recommended that this method be used only when available under a given law (such as the Health Insurance Portability and Accountability Act (HIPAA)), and in that case it should follow the process described in such law.

4.0 Exceptions to the Above General Methods for De-identification

a) PI Subject to the EU GDPR/ UK Data Protection Act remains PI even if it meets this Standard. Only truly "Anonymized Information" is no longer considered to be PI under the GDPR/UK Data Protection Act. However, since Gallagher's general recommendation is not to declare any information as "Anonymized Information", this means that all EU/UK data used in analytics must either be subject to consent or another legal basis under the GDPR/UK Data Protection Act to use the data for analytics prior to any such use. The consent or the legal basis must be documented prior to use and approved by the Global Chief Privacy Officer.

b) PI Subject to HIPAA – the Methods of De-idenification listed above do not apply to protected health information (PHI) subject to HIPAA. PHI can only be considered De-identified if it meets the requirements provided under HIPAA, which are outlined in Appendix C. Further, any De-identification by a (sub-)Business Associate (as defined by HIPAA) should be permitted under the (sub-)Business Associate Agreement governing the relationship between the (sub-) Business Associate and the Covered Entity (as defined by HIPAA).

c) PI subject to U.S. State privacy laws (including, without limitation, the California Consumer Privacy Act, the California Privacy Rights Act and applicable regulations (collectively referred to as "CCPA"), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Virginia Consumer Data Protection Act and the Utah Consumer Privacy Act) may only be declared De-identified if, in addition to this Standard, the Company can evidence that:

    i. It takes reasonable measures to ensure that a person cannot associate the data with an individual;

    ii. It publicy commits to maintain and use the data only in De-identified form and not attempt to re-identify the data; and

    iii. It contractually obligates any recipient of the De-Identified Information to comply with these same requirements, it exercises reasonable oversight to monitor compliance with the contractual obligations and it takes appropriate steps to address any breaches of such obligations.

d) PI subject to specific client contractual commitments may only be declared De-identified if it meets the relevant contractual standard. If no De-identification standard is specified in the contract, and no other other exception applies. De-identification under this Standard is

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

acceptable.

e) Deviations – if a team using the dataset wishes to deviate from this Standard, it must seek prior approval from the Global Chief Privacy Officer and a member of the team that owns the dataset.

5.0 Other Requirements for De-identification

b) Respecting Choices – to the extent possible, whenever using a dataset, the user must discuss the use with the dataset owner and determine if there are any limitations imposed on the intended use of the dataset reflected in any applicable client or individual contractual commitments or choices (if so offered) in which case such restrictions must be honored.

c) Testing – once the appropriate De-identification method or Aggregation threshold has been applied, it is recommended that the dataset owner test it to assess whether it meets the Cell Size Rule or otherwise allows an individual to be reasonably identified from the dataset, either alone or in combination with other publicly available information,. The testing and its results should be documented.

d) Re-Assessing the Risk – the risk of re-identification should be regularly considered and, where a dataset presents a risk (due to its size or the value of the underlying information) were it to be re-identified, further steps should be taken to minimize the risk. In some cases, it may be necessary to withdraw released datasets, where the identities of individuals can no longer be reasonably protected. Steps that the dataset owner can take, where deemed necessary, include:

i. Keeping a register of all the De-Identified and Aggegated datasets created and shared both internally and externally; or

ii. Considering the published datasets against newly published datasets (internally or externally) to see if they could be combined or cross referenced to re-identify individuals.

e) Sharing with Unaffiliated Third Parties – in the event a Gallagher entity shares De-identified Information with an unaffiliated third party, it must do so pursuant to a contractual agreement that includes an assurance that, unless otherwise specified, the third party will:

i. Not attempt to re-identify the information provided by the Company;

ii. Only use the dataset for the agreed purposes;

iii. Not share the dataset with any other party without Company's express written authorization and without contractually obligating the other party to agree to the requirements set forth in Sections 4 c) ii and iii above; and

iv. Provide all records and information reasonably requested by the Company to demonstrate its compliance with these obligations.

6.0 Anonymization

In order to be deemed Anonymized, (i) information must not reveal the identity of any individual and (ii) re-identification of an individual by any party (inside or outside the company) with any amount of information must not be technically feasible. Generally, Gallagher does not commit in contracts or policies to Anonymizing PI. Exceptions to this general rule must be approved by a member of the Global Privacy Office. This Standard does not address the technical process to achieve Anonymization.

7.0 Non Compliance with This Standard

Non-compliance with this Standard may result in disciplinary action by Gallagher, up to and including termination of your employment.

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Where there is a justifiable business case for non-compliance with this Standard, a waiver can be requested from the Global Chief Privacy Officer.

8.0 Related Documents

Global Information Classification and Handling Policy
Global Information Privacy Policy
Global IT Policy and Standards Manual.

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Appendix A – PI Categorization Table*

*See Appendix C for Indentifiers under HIPAA.

Note that Indirect Identifiers include, without limitation, the data elements identified below. Any team seeking to De-identify a dataset must consider the context of the dataset to determine whether a particular data element, though not PI and not listed in the table below, could nevertheless be used in combination with other information to identify a particular individual. By the same token, certain use cases may justify a different treatment to a data element than indicated below.

As a reminder, a data element can be PI without being a Direct or Indirect Identifier.

Category of PI	Data Element	Personal Identifier (Director or Indirect)
Identification numbers	National Identification Number / Social Security Number	Direct
	Passport or Visa Number	
	Social Insurance Number	
	Health Insurance Number	
	Pension Number	
	Individual Tax ID Number	
	Work Permit or Residency Number	
	Voter ID Number	
	Drivers Licence Number	
	Any other federal, national, state or provincial issued personal identity number	
	Car Licence Plate Number	
	Car Vehicle Identification Number (VIN)	
	Any non-governmental unique identification number including, but not limited to, Company Employee Identification Number, Policy Number, Medical Provider Identification Number, Insurance Policy Number, Claim Number, Membership Number (e.g, car rental, airline, hotel), etc.	
Insurance Claims Data	Date of loss	Not an Identifer
	Type of loss	
	Body part injured	
	Nature of injury	
	Make or model of vehicle claiming the loss	
	Make year of vehicle on which loss is claimed	
	Type of vehicle claiming the loss	
	Claimant age at time of claim	Indirect
Personal Financial Data	Individual's bank, brokerage or other financial institution account number	Direct
	Credit or debit card numbers and PINs	
	Any other credit /debit card data such as expiration date, CVV / CCV data	Not an Identifer
	Compensation Data (including, but not limited to, base pay, bonus, overtime payments, Long Term Incentive Grants/Payments (LTIPs) and any related information)	Indirect
	Employee benefits-related account balances including individual savings accounts and any other similar financial benefit accounts offered by an employer	
	Inferred data (creditworthiness)	
	Employment Title with Company Affiliation	Direct
	Employment Title	
	HR data (e.g., title, employment history, start & end dates, working hours, attendance, annual leave, travel booking details, life events, etc)	

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Category of PI	Data Element	Personal Identifier (Director or Indirect)
Other Personal Data	Educational records and professional qualifications	Indirect
	Marital status, beneficiaries, dependents, relatives, next of kin	
	Background or sanctions check elements (excluding criminal records), credit checks, anti-fraud checks	
	Credit/Consumer Report elements	
	Nationality or racial or ethnic origin	
	Political Opinion	
	Religious or philosophical affiliation	
	Trade Union Membership	
	Veteran status	
	Sex life or sexual orientation	
	Sexual Identity	
	Information from Motor Vehicle Record	
	Criminal record element (excluding Motor Vehicle Records)	
	Any unique characteristic that can be used to identify an individual	
	Health information including treatment, injury, diagnosis, claims, drug tests, drinking or smoking habits, or disability status (other than uniquely identifying characteristics)	Not an Identifer
	Insurance plan enrolment information	
	Gender	Indirect
	Genetic data	Direct
	Biometric data	
	Name	
	Home address – street	
	Home address – city	Indirect
	Home address – county	
	Home address - state / province	Not an Identifer
	Home address – country	
	Home address – zip/postal code (5 digits or less)	Indirect
	Home address – zip/postal code (6 or more digits)	Direct
	Place of work	Indirect
	Business address – street	
	Business address – city	
	Business address – county	
	Business address – state / province	Not an Identifer
	Business address – country	
	Business address – postal / zip code	Indirect
	Business telephone number	
	Date of birth	
	Fax number	
	Personal telephone number	Direct
	Personal email address	
	Business email address	
	Signature	
Photos / Videos / Audio	Photos used for biometric access or profiling	Direct
	Photos – other	
	Audio or visual recordings (e.g., CCTV footage, call centre recordings or MS Teams (or equivalent) meeting recordings)	
Access Security Credentials	Password	Direct
	PIN	

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Category of PI	Data Element	Personal Identifier (Director or Indirect)
	Biometric access identifiers, including fingerprints, facial / voice recognition, retina scans	
Technical Data	Wearable / sensor data	Not an Identifier
	Internet or other electronic network activity, including browsing / search history, information about interaction with website / application / ad / cookies	
	IP Address	Indirect
	Any unique mobile or device ID (e.g., UID, SMEI, MAC address)	
	Geolocation data	
Transactional Information	Purchase history, service records, commercial property, customer service records, communication / payment preferences, market research, survey data, data collected for qualifications	Not an Indentifier
Individual Profiles	Inferences used to create a profile about an individual reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes (e.g., interests / hobbies, professional interests, scores)	Not an Identifier

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Appendix B – Confirming the Cell Size Rule

The following are examples of how to confirm the Cell Size Rule:

Excel

- Create a pivot table with all Indirect Identifiers as rows. Select Count(unique_identifier) as the value to display. Sort the table on the resulting count column. The count must be greater than or equal to 10.

Unix / Linux

- Command-line “awk” (where the Indirect Identifiers are in columns 2, 3…to N): awk’{cellsize[$2,$3,…$N]++} END {for(i in cellsize) print i, cellsize}’ | sort -n k2

SQL

- SELECT indirect_identifier1, indirect_identifier2, …indirect_identifierN, Count(unique_identifier) as cell_size
- FROM deidentified_dataset
- GROUP BY indirect_identifier1, indirect_identifier2, …indirect_identifierN
- ORDER BY cell_size ASC;

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.

Appendix C – De-Identification Under HIPAA

In accordance with the US Department of Health and Human Services (HHS) Guidance Regarding Methods for De-identification of Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability (HIPAA) Privacy Rule, all of the following identifiers must be De-identified prior to using or sharing the information for any purpose other than in connection with the services:

- Name;
- Address (all geographic subdivisions smaller than state, including street address, city, county, precinct and full zip code, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
    - (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
    - (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89);
- Telephone numbers;
- Fax number;
- Email address;
- Social Security Number;
- Medical Record Number;
- Health Plan Beneficiary Number;
- Account Number;
- Certificate or License Number;
- Vehicle identifiers and serial numbers, including license plates;
- Device identifiers and serial number;
- Web URL;
- Internet Protocol (IP) Address;
- Biometric identifiers, including finger or voice print;
- Photographic image – photographic images are not limited to images of the face; and
- Any other unique identifying number, characteristic, or code.

See 24 C.F.R. §164.514(a) for further information

Confidential – not to be distributed outside Gallagher without the consent of the Standard Owner.