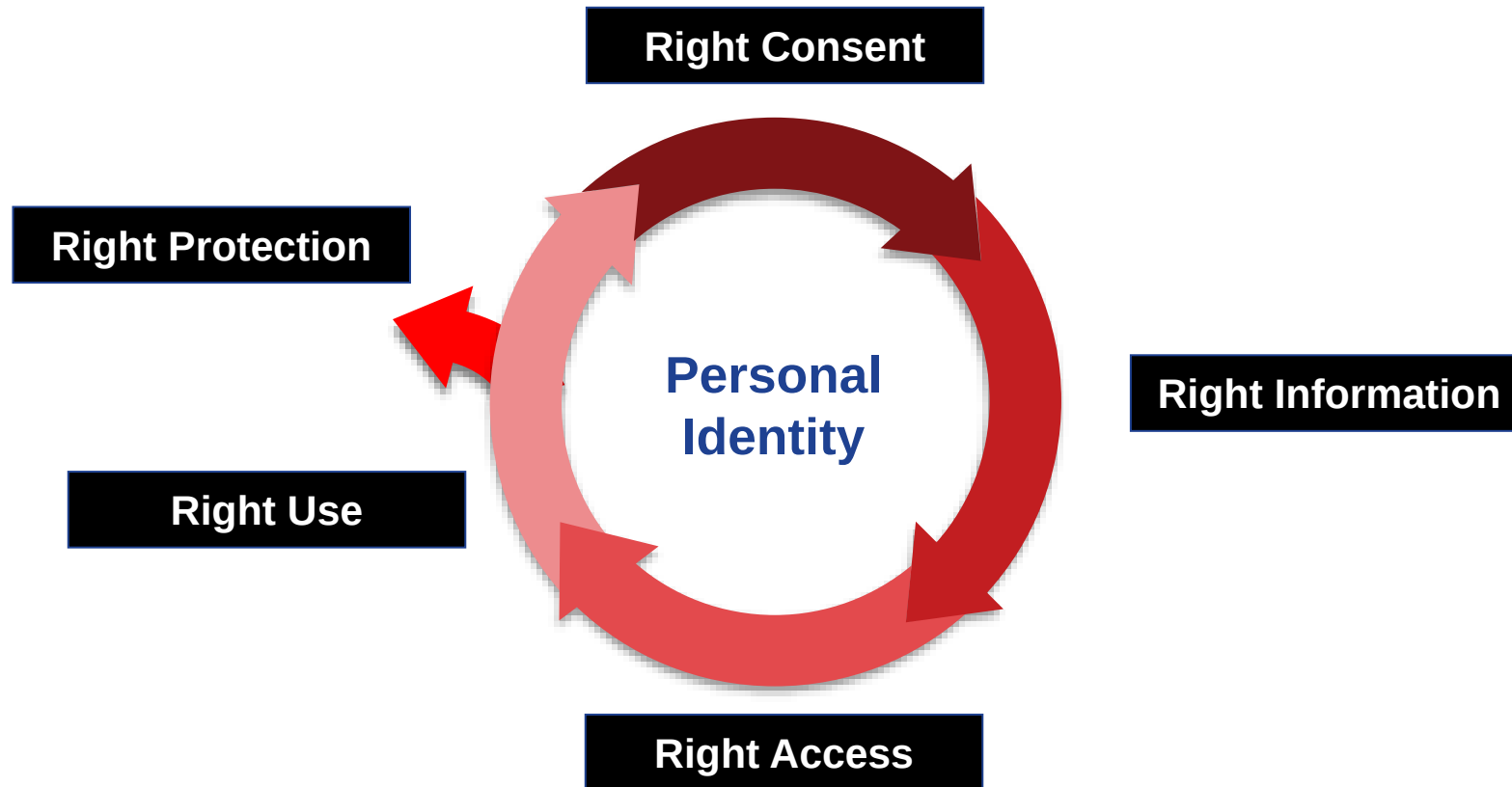




The 5 Rights of My Identity™



Welcome



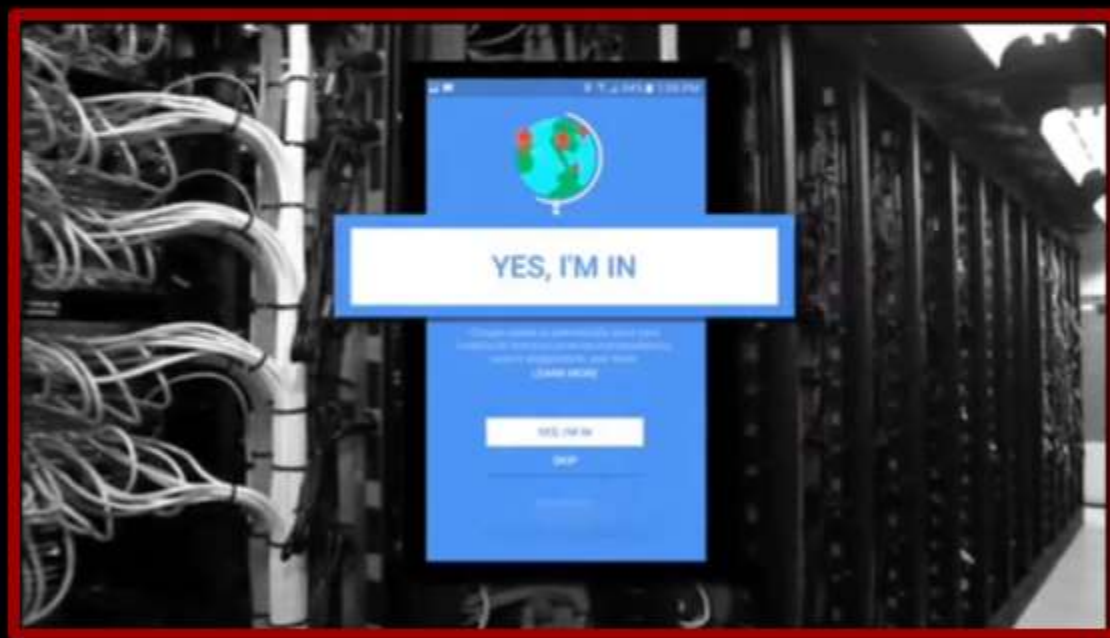
Charles Denham, MD

Chairman, TMIT Global

**TMIT High Performer Webinar
December 21, 2023**

Webinar 211

Big Brothers Watchin'





U.S. Department of Health and Human Services
Office of Inspector General

Eye on Oversight – Medical Identity



SOURCE: [Eye on Oversight - Medical Identity Theft | Office of Inspector General | Government Oversight | U.S. Department of Health and Human Services \(hhs.gov\)](#)

6 Ways Your Identity Can Be Stolen Intro



SOURCE: <https://www.youtube.com/watch?v=9ST5cMEXmDU>



U.S. Department of Health and Human Services
Office of Inspector General

2023 Health Care Fraud Nationwide Enforcement Action



2023 HEALTH CARE FRAUD
NATIONWIDE ENFORCEMENT ACTION

CHRISTIAN J. SCHRANK

DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS

in announcing a major Enforcement Action
to combat health care fraud.

SOURCE: [HHS-OIG Remarks on the 2023 Health Care Fraud Nationwide Enforcement Action – YouTube](#)



[LEAD Hospital Initiatives](#)
[Patient Safety Documentaries](#)
[Research Programs](#)
[Webinars & Meetings](#)
[Patient Programs](#)
[Multimedia Center](#)

[Home](#)
[Discussions](#)
[FAQs](#)
[About](#)

Consent to Save Your Life: The 5 Rights to My Identity™
December 21, 2022

[MORE INFO](#) [REGISTER](#)

Surfing the Healthcare Tsunami Hospital Leaders Toolbox

The Surfing the Healthcare Tsunami Hospital Leaders Toolbox has been released online! Go deeper into the subject matter of the documentary by exploring the 5 Rights to My Identity™, the Bystander, Rising & Action, and much more. [Click here](#) for more details.

[Click here](#) to watch the online 10-minute documentary online.

Med Tac Bystander Rescue Care Program

Join us at Med Tac Global to learn from our experts how the public can better follow the rescue of victims and loved ones from the most common emergencies. [Click Here](#)

High Performance 5 Rights Collaborative

We are conducting high impact research activities in the areas of Imaging of Adults and Children, Pain Care, Back Care, Testing, and Surgery to connect leaders in value and health to leading. For more information on each collaborative, click [Imaging Children, Back, Pain, Testing, Cancer, or Surgery](#).

Trademarks and Tools

The Information Power Grid™ is a proprietary and continuously updated decision support system that provides relevant partners and customers with the information they need to make good decisions. Information obtained through TMIT National Research Test Bed services, expert presentations, interviews, and data pertaining to specific topics within HCC Global and its affiliates to continuously improve the data and evidence that its network partners and customers use for optimal decision-making. Such efforts include TMIT Global and CareUniversity®. Such projects include the Med Tac Certificate advanced first aid program and communities of practice including a Threat Safety R&D Community. Information Power Grid™ is a registered trademark of HCC Global.

External Sources

AMRE® (The Safety Network) (PDR)
 Assent for First Aid in Intensive Care
 American Hospital Association
 AMRE
 Centers for Medicare & Medicaid Services
 4000 Collaborating Centers for Patient Safety Solutions
 Davenport Institute
 National Patient Safety Foundation
 NCR Institute
 Institute for Safe Medication Practices
 Veterans Admin Patient Safety Center
 Joint Commission Resources
 World Health Organization
 National Practice Partnership

Powered by HCC Global's Information Power Grid™ System
 SafetyLeaders® and CareUniversity® are trademarks of HCC Global. Sponsored by TMIT Global

[LEAD Hospital Initiatives](#)
[Patient Safety Documentaries](#)
[Research Programs](#)
[Webinars & Meetings](#)
[Patient Programs](#)
[Multimedia Center](#)

[Home](#)
[Discussions](#)
[FAQs](#)
[About](#)

High Performer Webinar

December 21, 2022, 12:00 pm - 1:30 pm CT / 1:00 pm - 2:30 pm ET

[REGISTER](#) [JOIN EVENT](#)

Consent to Save Your Life: The 5 Rights to My Identity™

Session Overview

Along with the benefits of the development of machine learning and artificial intelligence comes enormous risks.

First party data comes from a continuous relationship between you and an organization. Second party data is that which is shared about you by such a relationship. Third party data is generated by many sources unbeknownst to you. Cookies are going away. Regulations are coming to protect you. Know about them!

Join us to address the 5 Rights to My Identity™

The Right to Consent: Informing consent to data use and if privacy preferences. **The Right to Information:** The right information can save your life... the wrong information may harm you.

The Right to Access: The right access to your information means you agree to use and to the conditions of both access.

The Right to Use: The right means you agree to the details of the use of your personal information.

The Right to Protection: The right protection means your data is stored and used with minimal risk of breach or use by fraudsters.

Join us to address the threat to our caregivers, patients, families and consumers as we address the incredible value of our personal information and the incredible threat and financial risk to us if that information is misused. Learn why you need a medical power of attorney and why you need to understand consent.

We offer these online webinars at no cost to our participants.

Webinar Video, and Downloads

The webinar video will be available within five (5) business days after the webinar.

Speaker Slide Set:

The slides will be posted here before the webinar begins.

Date, Time, Dial-In Information, & Objectives

December 21, 2022

01:00 PM to 2:30 PM Eastern Time
 12:00 PM to 1:30 PM Central Time
 11:00 AM to 12:30 PM Mountain Time
 10:00 AM to 11:30 AM Pacific Time

Dial-In: Audio will be provided through your computer (VoIP) if no cost to you. If VoIP is not an option on your computer, or if you choose to pay by phone only, you can use either of the following numbers to dial in: 1-888-800-6822 OR 1-888-875-8623. Webcode ID: 914 1517 3886. If you use this dial-in number, you will be charged by your local phone company or long-distance provider for the call.

Learning Objectives:

[LEAD Hospital Initiatives](#)
[Patient Safety Documentaries](#)
[Research Programs](#)
[Webinars & Meetings](#)
[Patient Programs](#)
[Multimedia Center](#)

[Home](#)
[Discussions](#)
[FAQs](#)
[About](#)

TMIT Global, approved by the California Board of Registered Nursing, Provider Number 10886, will be hosting 1.5 contact hours for this webinar. TMIT Global is only providing nursing credit at this time.

To request a Participation Document, please [click here](#).

Session Speakers and Panelists

C. R. Denton, R. MD

[BO](#)

Vicki King

[BO](#)

Gladstone McDowell, R. MD

[BO](#)

William Adcox, MBA

[BO](#)

Gregory Bels, MD

[BO](#)

John Nance

[BO](#)

Randy Steyer

[BO](#)

Jennifer O'Grady

[BO](#)

Emerging Threats Community of Practice Application

Name *

Last

First

Email *

Phone *

Organization *

Position at the Organization *

Insert your Topics of Interest

[Submit](#)

Questions about the Webinar video or need technical assistance?
 Email webinars@safetyleaders.org

Powered by HCC Global's Information Power Grid™ System
 SafetyLeaders® and CareUniversity® are trademarks of HCC Global. Sponsored by TMIT Global

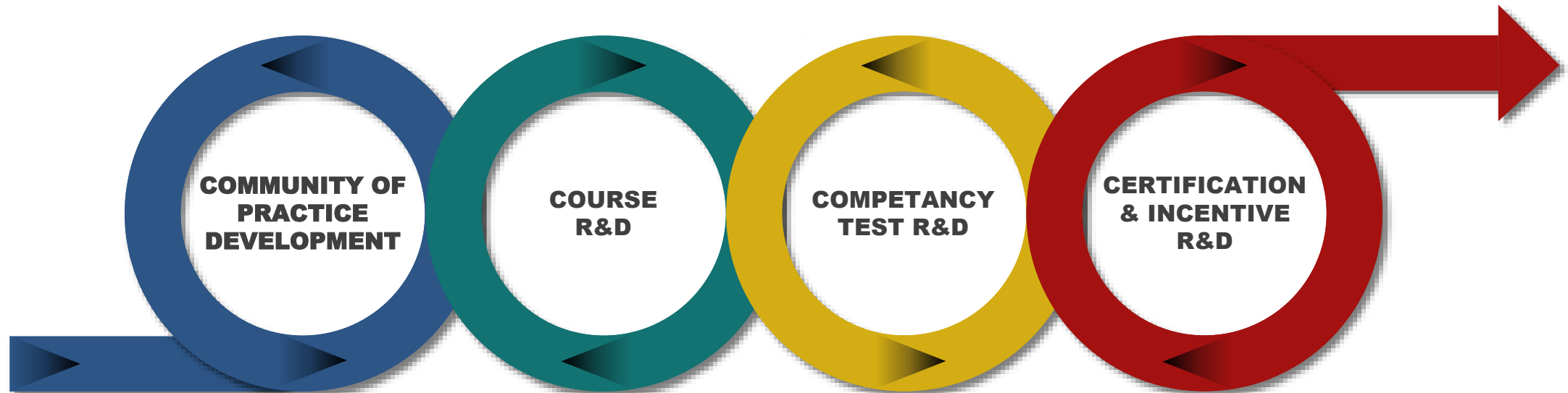
© 2023 TMIT Global

7

TMIT Global



Learning Management System



CareUniversity®



**TMIT Global
Research Test Bed**



SafetyLeaders®

Certificates for Med Tac Program



100+years

AMERICAN COLLEGE OF SURGEONS
*Inspiring Quality:
Highest Standards, Better Outcomes*



American
Heart
Association®

Heartsaver® First Aid CPR AED

Emerging Threats Speakers and Reactors



Jennifer Dingman



Vicki King



John Nance JD



Randy Styner



Dr. Gladstone McDowell



Chief William Adcox



Gregory Botz MD



Charles Denham MD

Current 2023 Workplace Violence & Fraud Series

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

The Imposters: Emerging Threats to Safety



The diagram features an iceberg with the visible tip representing obvious threats and the submerged part representing hidden threats. To the right, a circular diagram is labeled 'Insider Threat' and includes categories like Cyber, Physical, and Economic. Next to it is a simple line drawing of a person's head and shoulders.

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

Workplace Violence in 2023: A Threat to Caregivers, Staff, Educators, and the Community



This illustration depicts several scenarios of workplace violence using black stick figures. It includes physical fights, one person shouting or threatening others, and a group confrontation. A large red octagonal sign with a white hand in the center, indicating a stop or prohibition, is positioned in the middle of the scenes.

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

Workplace Violence II: Beyond Physical Harm – Systems Issues



This illustration shows workplace violence scenarios with a focus on systems issues. It includes cyber-related threats (represented by a person at a computer), sabotage (represented by a person with a wrench), and group confrontations. A red octagonal stop sign is centered among the scenes.

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

Workplace Violence III: Threat Impact Scenarios



The slide features a 2x2 matrix titled 'Impact Scenarios'. The vertical axis is labeled 'Impact' and the horizontal axis is labeled 'Volume'. The quadrants are: Top-Left (High Impact, Low Volume), Top-Right (High Impact, High Volume), Bottom-Left (Low Impact, Low Volume), and Bottom-Right (Low Impact, High Volume). To the right of the matrix are several illustrations of threat scenarios, including physical fights, threats, and group confrontations.

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

Workplace Violence IV: Hunting and Howling in 2023



This illustration depicts 'hunting and howling' scenarios. It includes a wolf attacking a person, a person pointing a gun, and a person howling. Social media icons for Facebook, Twitter, LinkedIn, and others are shown at the bottom right.

TMIT Global Research Test Bed High Performer Webinar SafetyLeaders.org

Workplace Violence V: Insider Threats in 2023



This slide features an iceberg diagram with the visible tip representing obvious threats and the submerged part representing hidden threats. To the right, a circular diagram is labeled 'Insider Threat' and includes categories like Cyber, Physical, and Economic. Next to it is a simple line drawing of a person's head and shoulders.

Workplace Violence & Fraud Series 2023 Speakers and Reactors



Jennifer Dingman



David Morris PhD JD



Vicki King



John Nance JD



Randy Styner



Ann Rhoades



C. Clements MD PhD



Chief William Adcox



Gregory Botz MD



Charles Denham MD

Voice of Patient and Family



Jennifer Dingman

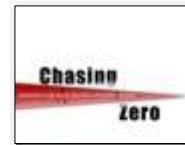
Founder, Persons United Limiting
Substandard and Errors in Healthcare
(PULSE), Colorado Division
Co-founder, PULSE American Division
TMIT Patient Advocate Team Member
Pueblo, CO



If you wish to follow us on Twitter,
go to: <http://twitter.com/TMIT1>
or use **#safetyleaders** hashtag



Also, go to:
www.facebook.com/SafetyLeaders
and related sites





Our Purpose, Mission, and Values



Our Purpose:

We will measure our success by how we protect and enrich **the lives of families...patients AND caregivers.**

**EMERGING THREATS
COMMUNITY OF PRACTICE**

Our Mission:

To accelerate performance solutions that **save lives, save money, and create value** in the communities we serve and ventures we undertake.

CAREUNIVERSITY®

Our ICARE Values:

Integrity, **C**ompassion, **A**ccountability, **R**eliability, and **E**ntrepreneurship.

Disclosure Statement

The following panelists certify that unless otherwise noted below, each presenter provided full disclosure information; does not intend to discuss an unapproved/investigative use of a commercial product/device; and has no significant financial relationship(s) to disclose. If unapproved uses of products are discussed, presenters are expected to disclose this to participants. None of the participants have any relationship medication or device companies discussed in their presentations.

Dr. Gladstone McDowell has nothing to disclose

Vicki King has nothing to disclose

John Nance JD has nothing to disclose

Chief William Adcox has nothing to disclose

Dr. Botz has nothing to disclose

Randy Styner has nothing to disclose

Jeni Dingman has nothing to disclose

Charles Denham, MD, is the Chairman of TMIT; a former TMIT education grantee of CareFusion and AORN with co-production by Discovery Channel for *Chasing Zero* documentary and Toolbox including models; and an education grantee of GE with co-production by Discovery Channel for *Surfing the Healthcare Tsunami* documentary and Toolbox, including models. HCC is a former contractor for GE and CareFusion, and a former contractor with Siemens and Nanosonics, which produces a sterilization device, Trophon. HCC is a former contractor with Senior Care Centers. HCC is a former contractor for ByoPlanet, a producer of sanitation devices for multiple industries. He does not currently work with any pharmaceutical or device company and has not done so for more than 5 years. His current area of research is in threat management to institutions including conflict of interest, healthcare fraud, and continuing professional education and consumer education including bystander care. Dr. Denham has been a collaborator with the late Professor Christensen at Harvard Business School.



Disclosure Statement

The following panelists certify that unless otherwise noted below, each presenter provided full disclosure information; does not intend to discuss an unapproved/investigative use of a commercial product/device; and has no significant financial relationship(s) to disclose. If unapproved uses of products are discussed, presenters are expected to disclose this to participants. None of the participants have any relationship medication or device companies discussed in their presentations.

David Grinsfelder has not
Randy Styner has nothing
Chief William Adcox has
Danny Policichio nothing
Dr. Gladstone McDowell
Dr. Botz has nothing to di
Charlie Denham III has no
Jeni Dingman has nothing

The TMIT Global High Performer Webinar Series has been entirely funded by private family philanthropy. No direct, indirect, or affiliated financial support has ever been or ever will be provided by healthcare pharmaceutical or device companies.

Charles Denham, MD, is t
Channel for *Chasing Zero*
for *Surfing the Healthcare Tsunami* documentary and Toolbox, including models. HCC is a former contractor for GE and CareFusion, and a former contractor with Siemens and Nanosonics, which produces a sterilization device, Trophon. HCC is a former contractor with Senior Care Centers. HCC is a former contractor for ByoPlanet, a producer of sanitation devices for multiple industries. He does not currently work with any pharmaceutical or device company and has not done so for more than 5 years. His current area of research is in threat management to institutions including conflict of interest, healthcare fraud, and continuing professional education and consumer education including bystander care. Dr. Denham has been a collaborator with the late Professor Christensen at Harvard Business School.

ction by Discovery
Channel for *Chasing Zero*

documentary and Toolbox, including models. HCC is a former contractor for GE and CareFusion, and a former contractor with Siemens and Nanosonics, which produces a sterilization device, Trophon. HCC is a former contractor with Senior Care Centers. HCC is a former contractor for ByoPlanet, a producer of sanitation devices for multiple industries. He does not currently work with any pharmaceutical or device company and has not done so for more than 5 years. His current area of research is in threat management to institutions including conflict of interest, healthcare fraud, and continuing professional education and consumer education including bystander care. Dr. Denham has been a collaborator with the late Professor Christensen at Harvard Business School.

1,000 Worker Study

The 5 R's of Safety



HEAD



HEART



HANDS



VOICE

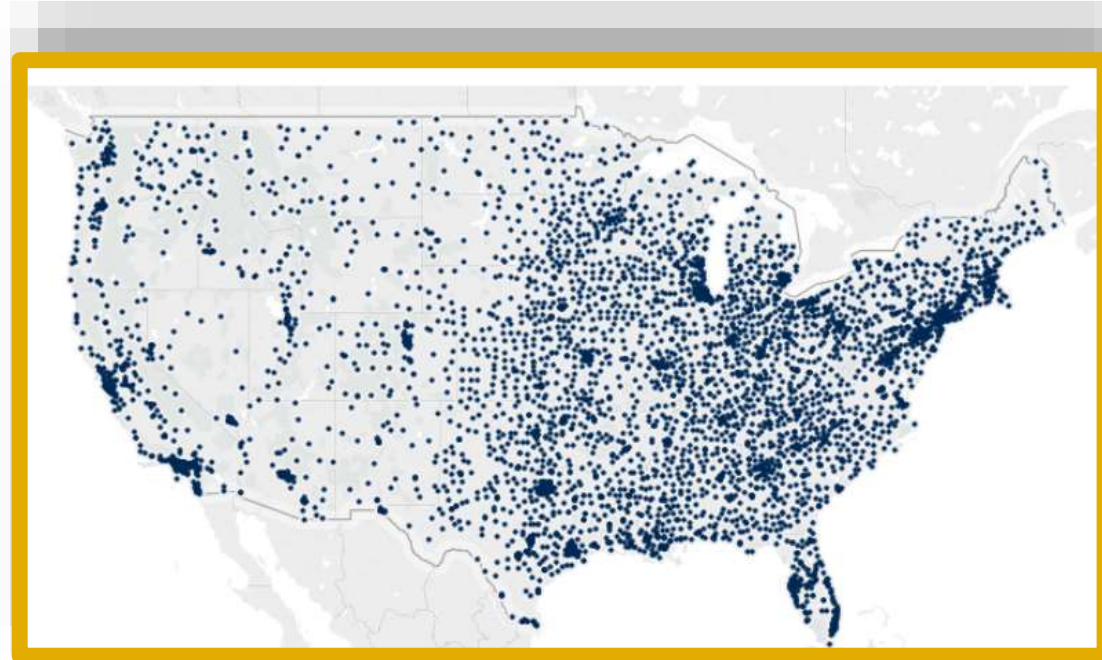
The 5 R's of Safety



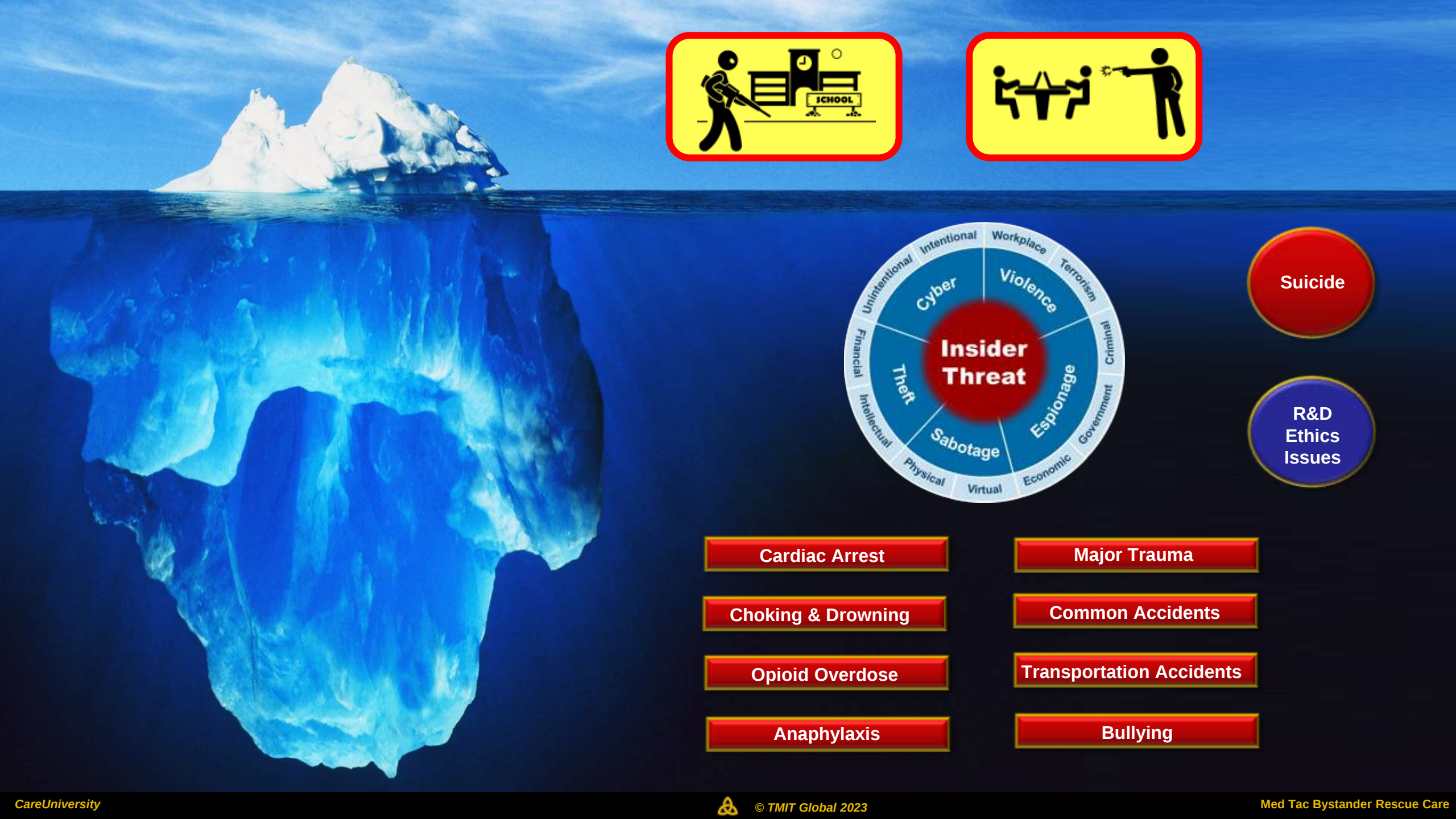
TMIT Global Research Test Bed

3,100 Hospitals in 3,000 Communities

500 Subject Matter Expert Pool Developed over 39 Years



Turn the Science into Safety™



Suicide

R&D
Ethics
Issues

Cardiac Arrest

Major Trauma

Choking & Drowning

Common Accidents

Opioid Overdose

Transportation Accidents

Anaphylaxis

Bullying

Emerging Threats

Community of Practice



0:00:02



0:09:08



Global Patient Safety Forum

Global Patient Safety Forum

The GPSF is a convening alliance with a mission to save lives, save money, and build value in the community it serves. The Forum was expressly founded to make available important content that the collaborators want to share more broadly. This website is not intended to compete with any other initiative and will meet its objectives if collaborators and those interested in the topics share the information with their communities. There are no financial requirements of users of the site. Certain communities are private in order to protect those we serve and those who serve. Those we serve are patients and their families. Those who serve are the caregivers, administrators, researchers, educators, and staff in the healthcare industry.

Global Innovators Network

We are a global network of leaders from academia, industry, NGOs, philanthropy, and faith-based organizations who are best practices in leadership of innovation. Spawned to meet the needs of innovators in healthcare and patient safety, our work has multiple sectors with a focus on mentorship and development. There is no specific commercial purpose of this website. No financial support of any type from the healthcare industry or communities of practice served here. This website is entirely free.

Featured Leaders

Global Webinars & Summits

Patient Safety Community Of Practice

Med Tac Bystander Care Program

Emerging Threats Community Of Practice

CareUniversity & Continuing Education



Thomas Zeltner, MD
Expert leader in Public Health
Former Special Envoy of the WHO
Former Secretary of State for Health
Swiss Federal Office of Public Health, Bern, Switzerland

[Read bio...](#)

[View video clip](#)



The private community of practice addresses a number of sensitive topics and subject matter that should not be made public for security reasons.

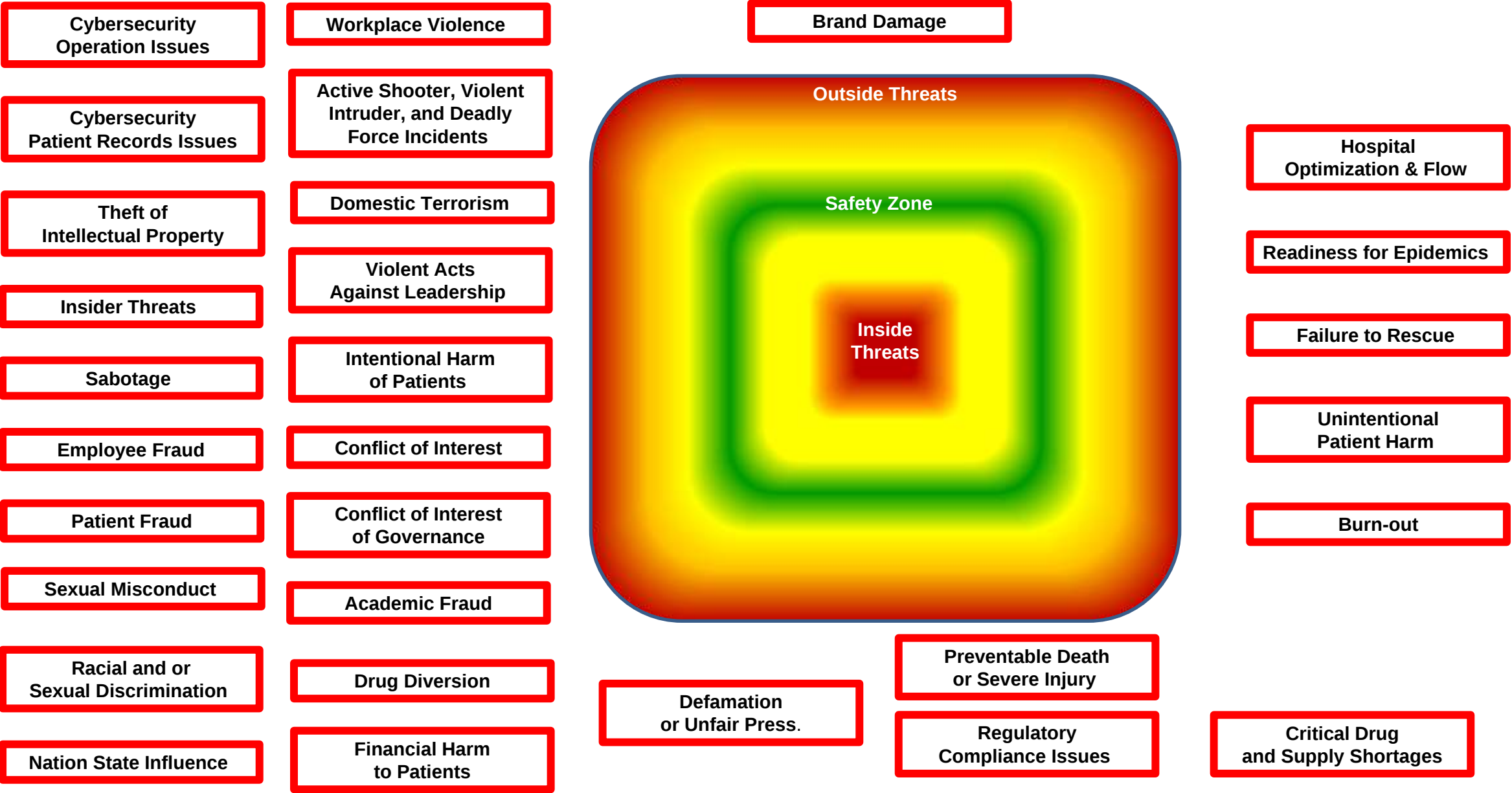
- **Brand Damage** from Outside, Inside, and or Mixed Outside-Inside Threats including cyberterrorism.
- **Workplace Violence** including physical, verbal, sexual, or emotional harassment, bullying or harm to caregivers, staff, students, or patients.
- **Active Shooter, Violent Intruder, and Deadly Force Incidents** including events causing physical harm to staff, caregivers, students, or patients.
- **Domestic Terrorism** such as organized attacks using chemical, biologic, radiologic, nuclear, and explosive weapons as well as weaponization of transportation & vehicles (CBRNET)
- **Violent Acts Against Leadership** where administrative, clinical, or governance leaders are specifically targeted by insiders or outsiders.
- **Intentional Harm of Patients** by caregivers who commit harmful acts against patients with or without enablers who do not report such harm.
- **Unintentional Patient Harm** through errors of omission from systems failures such as those identified by mortality reviews including diagnostic errors or NQF Never Events.
- **Failure to Rescue** in pre-hospital, hospital, and post-hospital continuity of care.
- **Preventable Death or Severe Injury** of staff or students on or off campus or site.
- **Financial Harm** to patient families by aggressive payment policies and actions.
- **Hospital Optimization & Flow** with overcrowding & boarding/transfer issues.
- **Readiness for Epidemics** including preparedness for volume care need surges.
- **Sexual Misconduct** including sexual harassment, abuse of power, and or harm to caregivers, staff, students, or patients.
- **Racial and or Sexual Discrimination** against those we serve including patients and their families and or those who serve in the organization.
- **Cybersecurity Patient Records Issues** including breach, theft, and contamination of medical records leading to patient and caregiver harm.
- **Cybersecurity Operation Issues** including breach, theft, and contamination of operational records, invasion of data systems, and ransom crimes.
- **Insider Threats** of intentional clinical, operational, or financial harm.
- **Theft of Intellectual Property** by insiders, outsiders, or nation-states.
- **Sabotage** of service, information systems, clinical care, and property.
- **Employee Fraud** including false identity/credentials, testing/vaccinations, attestations of truth, or false witness against patients or staff.
- **Patient Fraud** including false identity, testing/vaccinations, attestations of truth, or false witness against other patients or staff.
- **Nation State Influence** through academic espionage, financial conflicts of interest, or other means.
- **Drug Diversion** by staff including caregivers and pharmacists who divert medications for themselves or others.
- **Conflict of Interest** of staff including physicians, researchers, staff, or administrators including undisclosed as well as disclosed financial relationships.
- **Conflict of Interest of Governance** including undisclosed financial as well as disclosed financial relationships.
- **Academic Fraud** including fabrication, falsification, or plagiarism in publications or dishonest grant documentation including applications or reports.
- **Defamation or Unfair Press** by investigative reporting, false whistleblowers, or harm due to misinformation, disinformation, or mal-information publicized.
- **Burn-out** of caregivers, leadership, and staff.
- **Critical Drug and Supply Shortages** such as I.V. fluids, medications, and key supplies.
- **Regulatory Compliance Issues** including evolving risks of non-compliance.



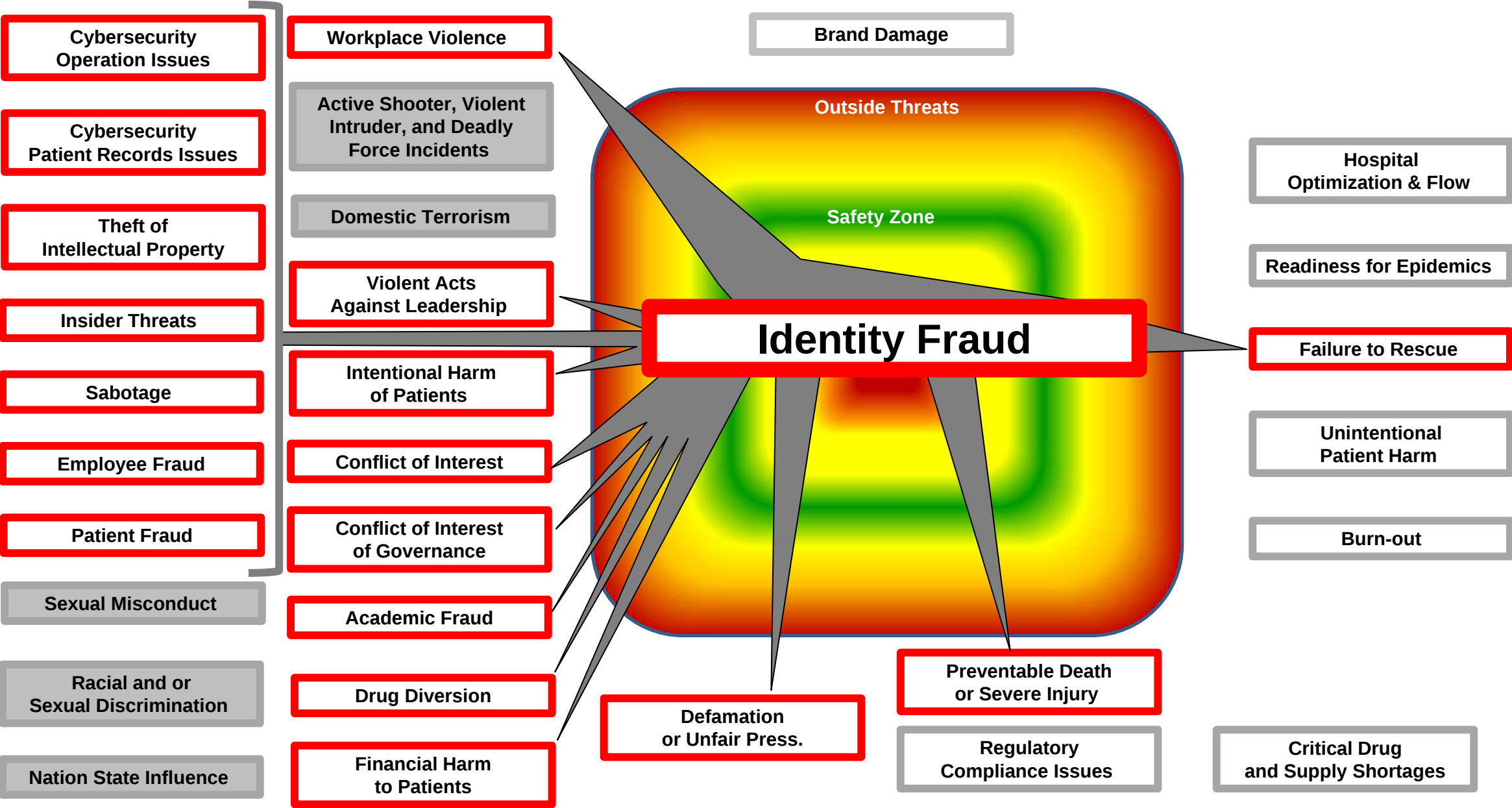
The private community of practice addresses a number of sensitive topics and subject matter that should not be made public for security reasons.

- **Brand Damage** from Outside, Inside, and or Mixed Outside-Inside Threats including cyberterrorism.
- **Workplace Violence** including physical, verbal, sexual, or emotional harassment, bullying or harm to caregivers, staff, students, or patients.
- **Active Shooter, Violent Intruder, and Deadly Force Incidents** including events causing physical harm to staff, caregivers, students, or patients.
- **Domestic Terrorism** such as organized attacks using chemical, biologic, radiologic, nuclear, and explosive weapons. Also weaponization of transportation & vehicles (CBRNET)
- **Violent Acts Against Leadership** where administrative, clinical, or governance leaders are specifically targeted by insiders or outsiders.
- **Intentional Harm of Patients** by caregivers who commit harmful acts against patients with or without enablers who do not report such harm.
- **Unintentional Patient Harm** through errors of omission from systems failures identified by mortality reviews such as diagnostic errors.
- **Failure to Rescue** in pre-hospital, hospital, and post-hospital continuity of care.
- **Hospital Optimization & Flow** with overcrowding & boarding/transfer issues.
- **Readiness for Epidemics** including preparedness for testing and volume surges.
- **Sexual Misconduct** including sexual harassment, abuse of power, and or harm to caregivers, staff, students, or patients.
- **Racial and or Sexual Discrimination** against those we serve including patients and their families and or those who serve in the organization.
- **Cybersecurity Patient Records Issues** including breach, theft, and contamination of medical records leading to patient and caregiver harm.
- **Cybersecurity Operation Issues** including breach, theft, and contamination of operational records, invasion of data systems, and ransom crimes.
- **Theft of Intellectual Property** by insiders, outsiders, or nation-states.
- **Sabotage** of service, information systems, clinical care, and property.
- **Employee Fraud** including misrepresentation of identity or qualifications, safety related issues such as vaccination and testing status, and attestations of truth.
- **Patient Fraud** including misrepresentation of identity, safety related issues such as vaccination and testing status, and attestations of truth.
- **Nation State Influence** through academic espionage, financial conflicts of interest, or other means.
- **Drug Diversion** by staff including caregivers and pharmacists who divert medications for themselves or others.
- **Conflict of Interest** of staff including physicians, researchers, and administrators including disclosed and undisclosed financial relationships.
- **Conflict of Interest of Governance** including undisclosed financial relationships and disclosed financial relationships.
- **Academic Fraud** including fabrication, falsification, plagiarism, or dishonest grant documentation including applications and reports.
- **Defamation or Unfair Press** by investigative reporting or false whistleblowers.
- **Burn-out** of caregivers, leadership, and staff.
- **Critical Drug and Supply Shortages** such as I.V. fluids, medications, and key supplies.
- **Regulatory Compliance Issues** including new risk for non-compliance.

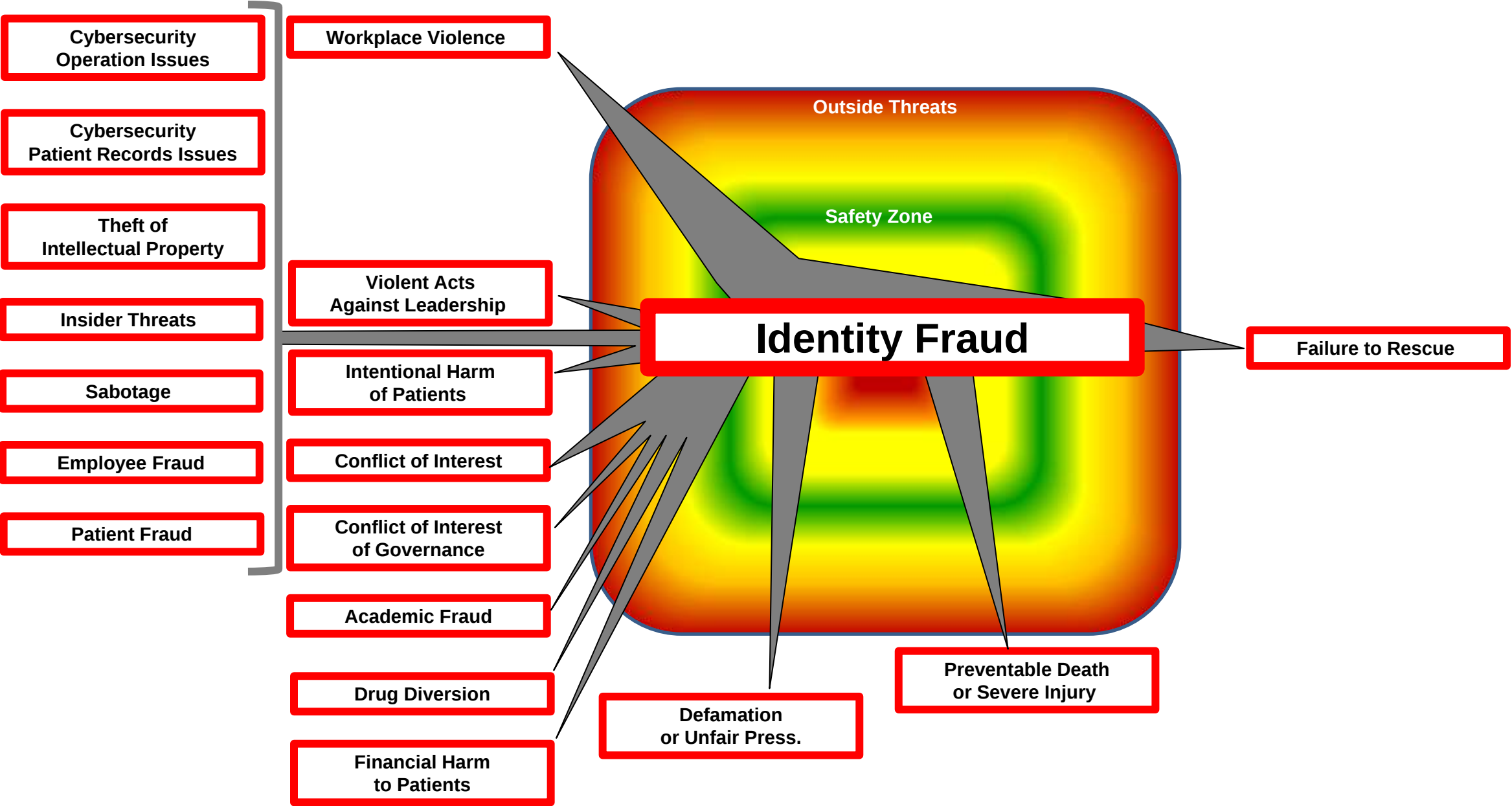
Inside & Outside Threats and Resilience Building



Inside & Outside Threats and Resilience Building



Inside & Outside Threats and Resilience Building



Emerging Threats: The Fraud Factor



TMIT High Performer Webinar October 21, 2021
<https://www.safetyleaders.org/webinartoctober2021/>



Fraud Definition

In law, fraud is intentional deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud can violate civil law (e.g., a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation) or criminal law (e.g., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities), or it may cause no loss of money, property, or legal right but still be an element of another civil or criminal wrong.

Source: <https://en.wikipedia.org/wiki/Fraud>



Safety of Rising Freshmen: Battling Failure to Rescue

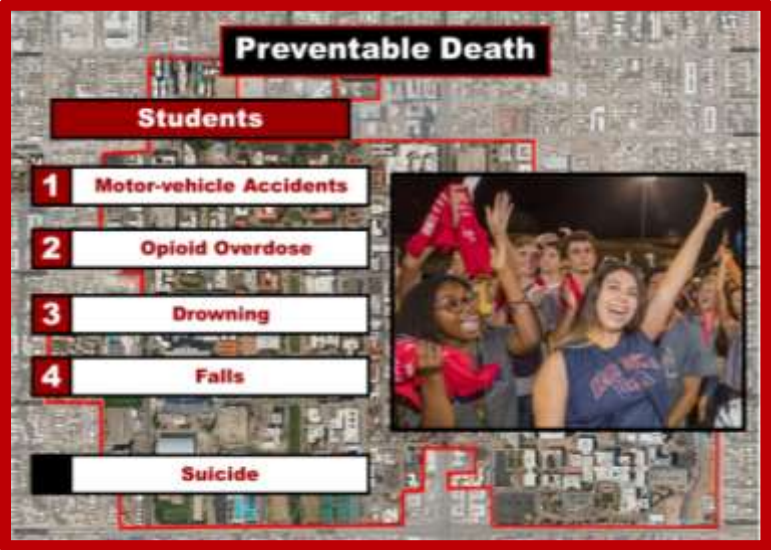


TMIT High Performer Webinar
August 17, 2023
Webinar 207

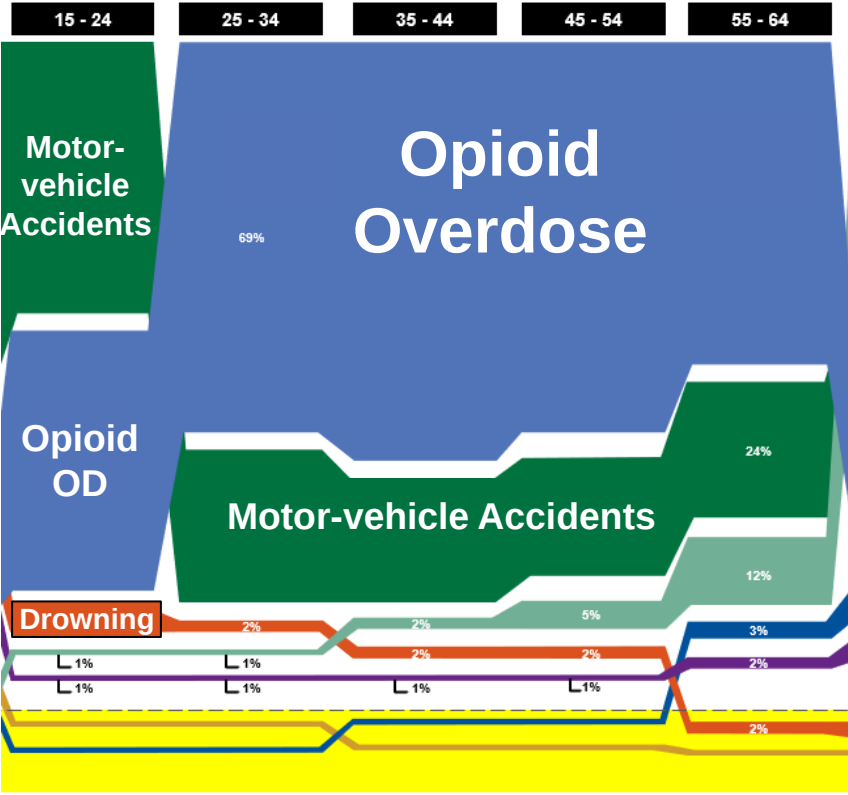
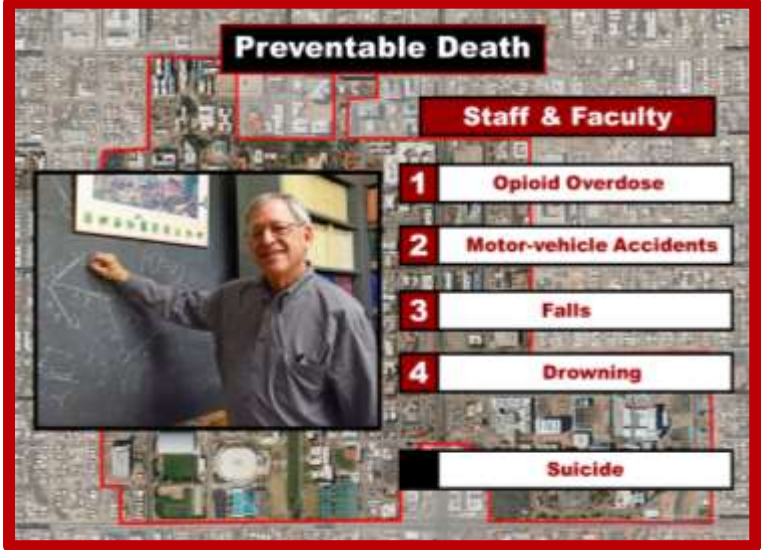
Top Causes of Unintentional Death By Age - 2020

2020 Data

Students

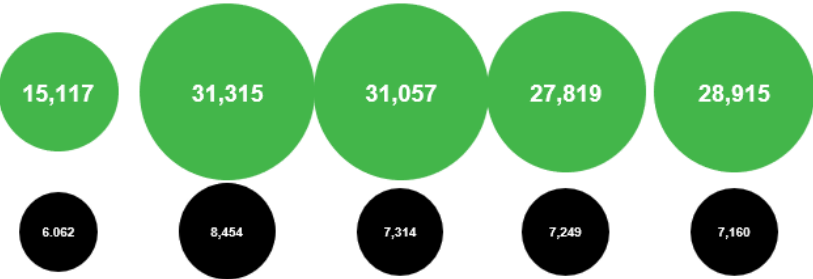


Faculty & Staff



Total unintentional deaths by age group

Total Suicide Deaths: 44,298



Source: Adapted from the National Safety Council Injury Facts, 2020 Edition

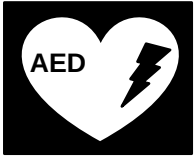
The TRANQ: The Zombie Effect



<https://www.youtube.com/watch?v=bRj3Sa-Q41A>

The Problem: Failure to Rescue

Cardiac Arrest



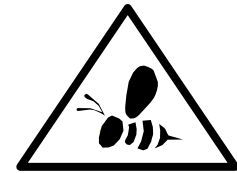
Choking & Drowning



Opioid OD & Poisoning



Anaphylaxis



Major Trauma



Infection Care



Transportation



Bullying



The Solution: Bystander Rescue Care

Cardiac Arrest



Sudden Cardiac Arrest: There is an epidemic of SCA with one quarter of the SCA events in children and youth occurring at sporting events. CPR and AED use have a dramatic impact on survival.

Possible Lives Saved in the US: 41 adults every hour and 19 children per day. 25% of SCA deaths in children occur at such events – 4 per day.

Choking & Drowning



Choking: More than 100,000 lives have been saved with the Heimlich Maneuver. Most choking deaths are preventable.

Possible Lives Saved in the US: 13 per day

Drowning: By population, drowning and near drowning events are very common. Since much of the OC population is near water, the numbers are likely much greater.

Possible Lives Saved in the US: 11 per day

Opioid OD & Poisoning



Opioid Overdose and Poisoning: An exploding opioid OD crisis is gripping our nation with a great toll on families. Narcan opioid reversal agents, rescue breathing and positioning, and rapid EMS response saves lives. Awareness drives prevention.

Possible Lives Saved in the US: There are 293 OD deaths per day. Up to 11 lives may be saved per hour.

Anaphylaxis



Anaphylaxis & Life Threatening Allergies: Many events are unreported; however 22% occur in children without a prior diagnosis of allergies. More than one in twenty adults will have an anaphylactic event in their lifetime. Epinephrine auto-injectors save lives within minutes.

Possible Lives Saved in the US: 2 per day

Major Trauma



Major Trauma & Bleeding: Bystander care especially for major bleeding using Stop-The-Bleed techniques of wound pressure, bandages, and tourniquets can have an enormous impact on survival.

Possible Lives Saved in the US: 14 per hour

Infection Care



Infection Care: Epidemics, pandemics, and seasonal infections are a leading cause of death. Prevention, preparedness, protection, and performance improvement strategies and tactics are critical to save lives and inform all Med Tac efforts. They are a feature of all Med Tac Bystander Rescue Care.

Possible Lives Incalculable – More than 1 Million from COVID alone. Almost 1,000 per day from sepsis.

Transportation



Non-traffic Related Vehicular Accidents: The incidence of non-traffic related drive-over accidents near schools and home is greater than 50 per week. More than 60% of the drivers are a parent or friend.

Possible Lives Saved in the US: Including adults, there are 1,900 deaths per year; many are preventable.

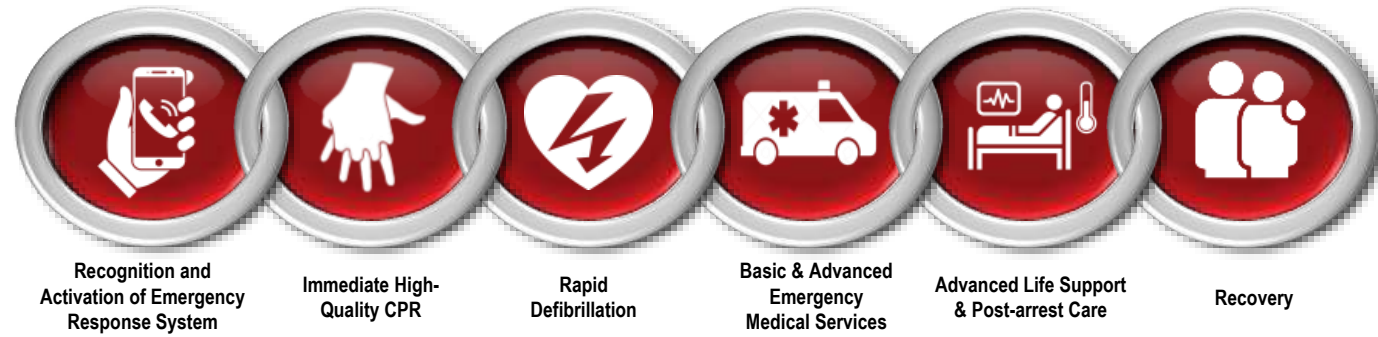
Bullying



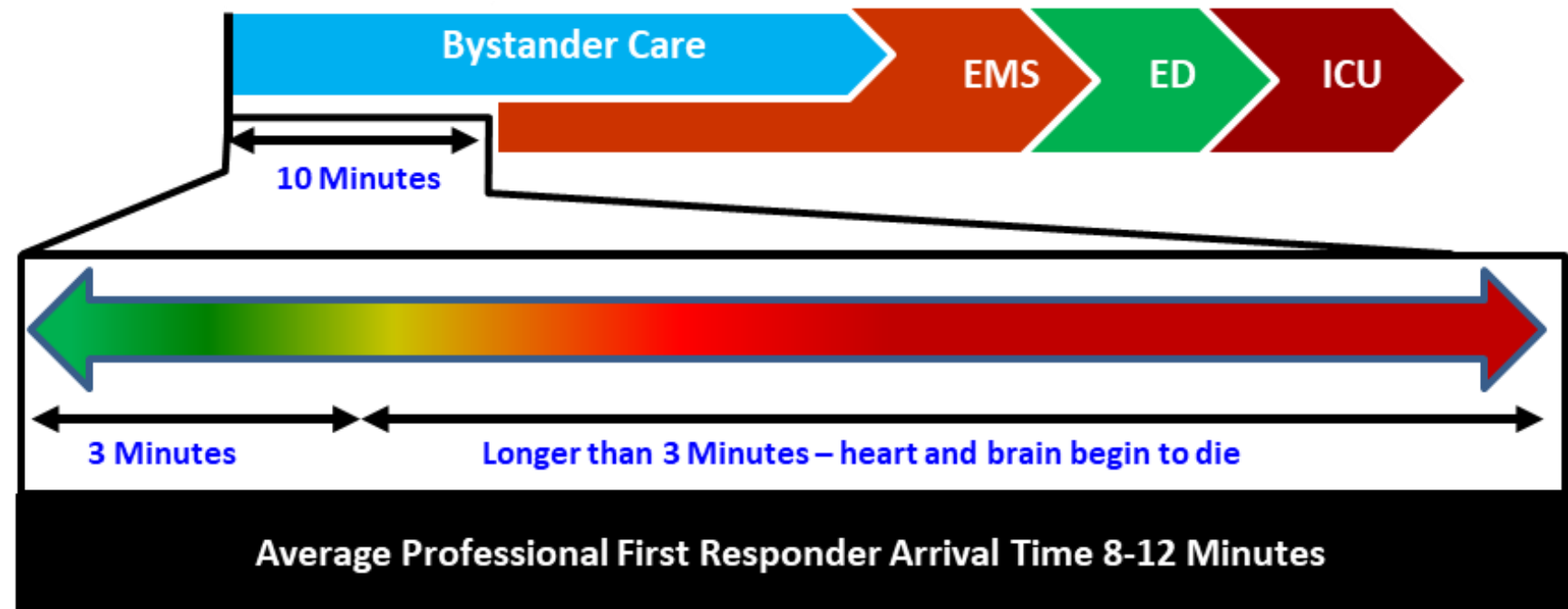
Bullying & Workplace Violence: Bullying and abuse of power in schools and at work can lead to suicide, workplace violence, violent intruders, and active shooter events.

Possible Lives Saved in the US: Difficult to estimate, however the consensus is that they are likely to be very significant.

The Problem: ***FAILURE TO RESCUE***



The Solution: ***Bystander Care***



“Frankenstein” Synthetic Medical Identity Theft





The Threat of Online Relationships



Randy Styner

**Director Emergency Response
University of California Irvine
Community Leader
Best Selling Author**



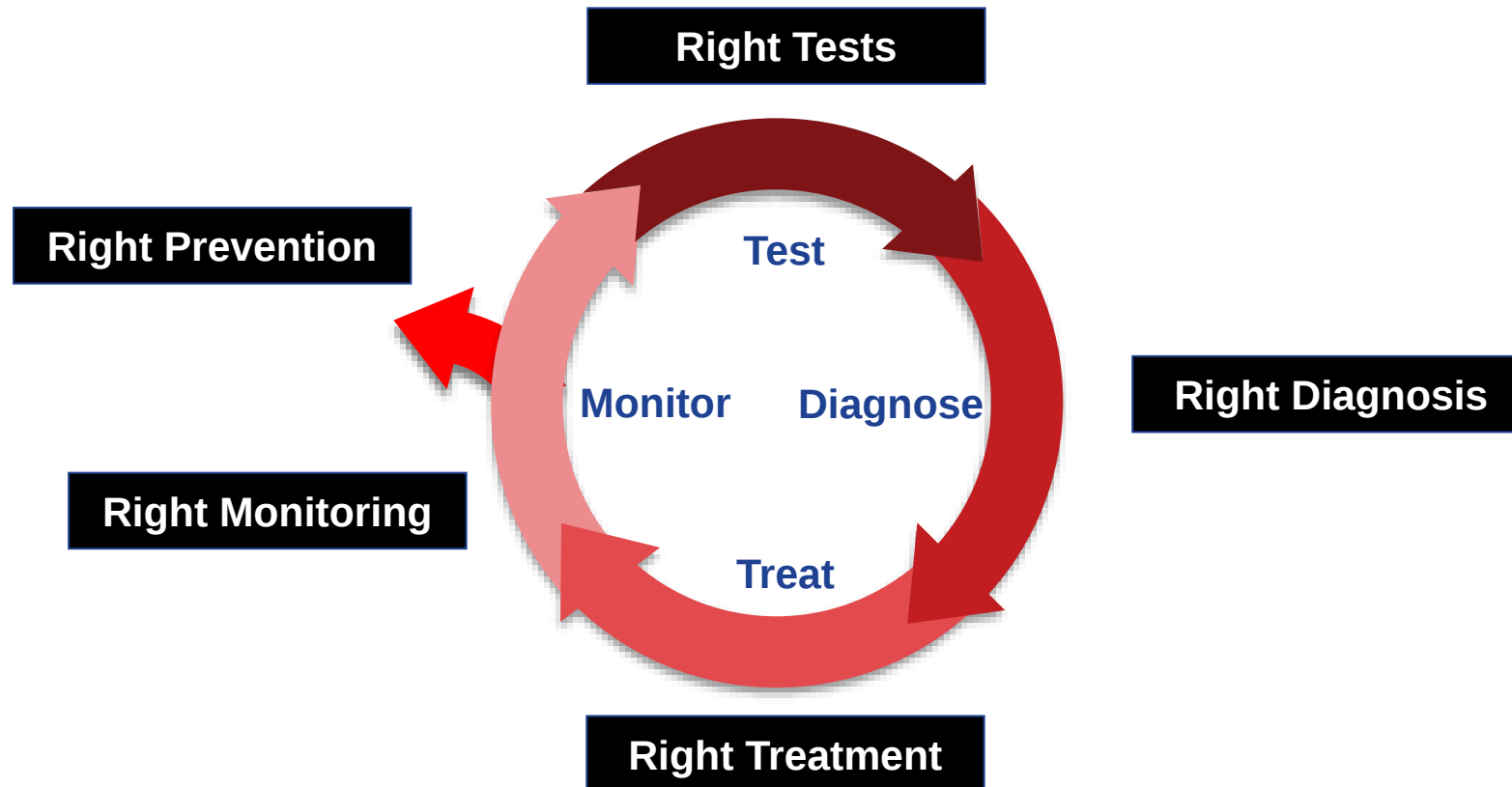
The 5 Rights of Pain Management



Gladstone C. McDowell, II, MD

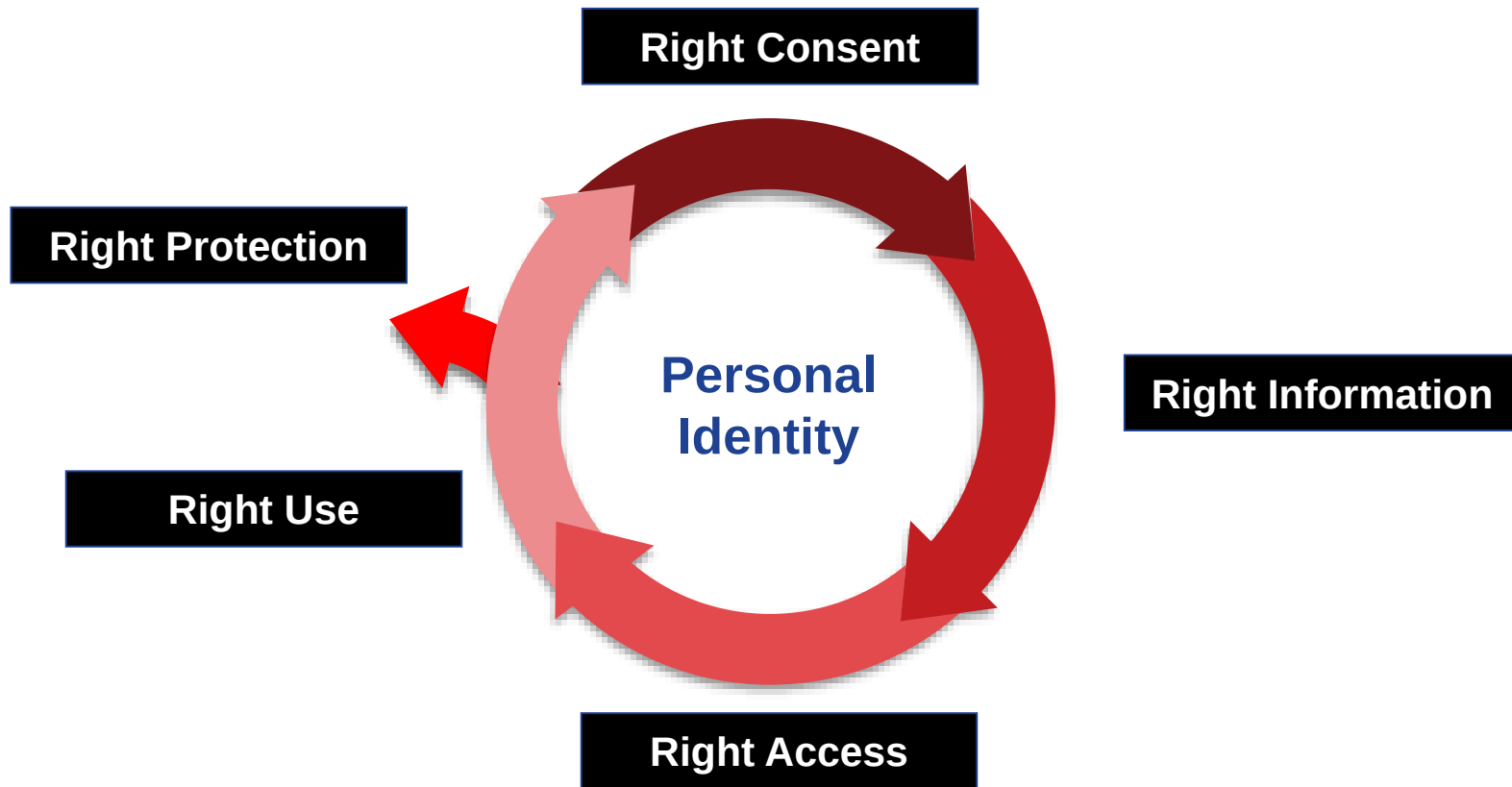
Pain Management Specialist
Urologic Oncologist
Director, Task Force Leader
Texas Medical Institute of Technology (TMIT)
Austin, TX

The 5 Rights of Pain Care®



Source: Denham, CR; McDowell, GM CareUniversity CME Program

The 5 Rights of My Identity™



Sources: HCC Global



© TMIT Global 2023



General Data Protection Regulation and California Consumer Protection Act



SOURCE: <https://dataprivacymanager.net/ccpa-vs-gdpr/>

CCPA VS. GDPR	
	
WHO IT APPLIES TO?	
It applies to profit entities that process personal data of residents of California and either • have 24 million \$ in annual revenue • Hold personal data of 50,000 consumers • have at least half of their revenue from the sale of personal data	• It applies to any organization that processes personal data of European citizens and residents, even if the organization is outside of European Union.
BASIS FOR CONSENT	
• Opt out	• Opt in
PENALTIES	
• \$2,500 per record for each unintentional violation • 7,500 \$ (or actual damages) for each intentional violation,	• 4% of annual turnover or 20 million EUR, whichever is greater • 2% of global annual turnover or €10 million, whichever is higher
ENFORCEMENT	
January 1st 2020	From May 25th 2018
RIGHTS OF INDIVIDUALS	
• Right to request information • Right to data portability • Right to opt-out • Right to access data • Right of disclosure • Right to deletion	• Right to be informed • Right of access • Right to rectification • Right to erasure • Right to restrict processing • Right to data portability • Right to object to processing • Rights in relation to automated decision making and profiling

What is “1st Party, 2nd Party, and 3rd Party Personal Data”?

First-party, second-party, and third-party data are terms used in the context of data collection and ownership, particularly with regard to personal information about consumers. They describe different sources and relationships regarding the data:

1st Party Data

► First-Party Data:

- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner.

2nd Party Data

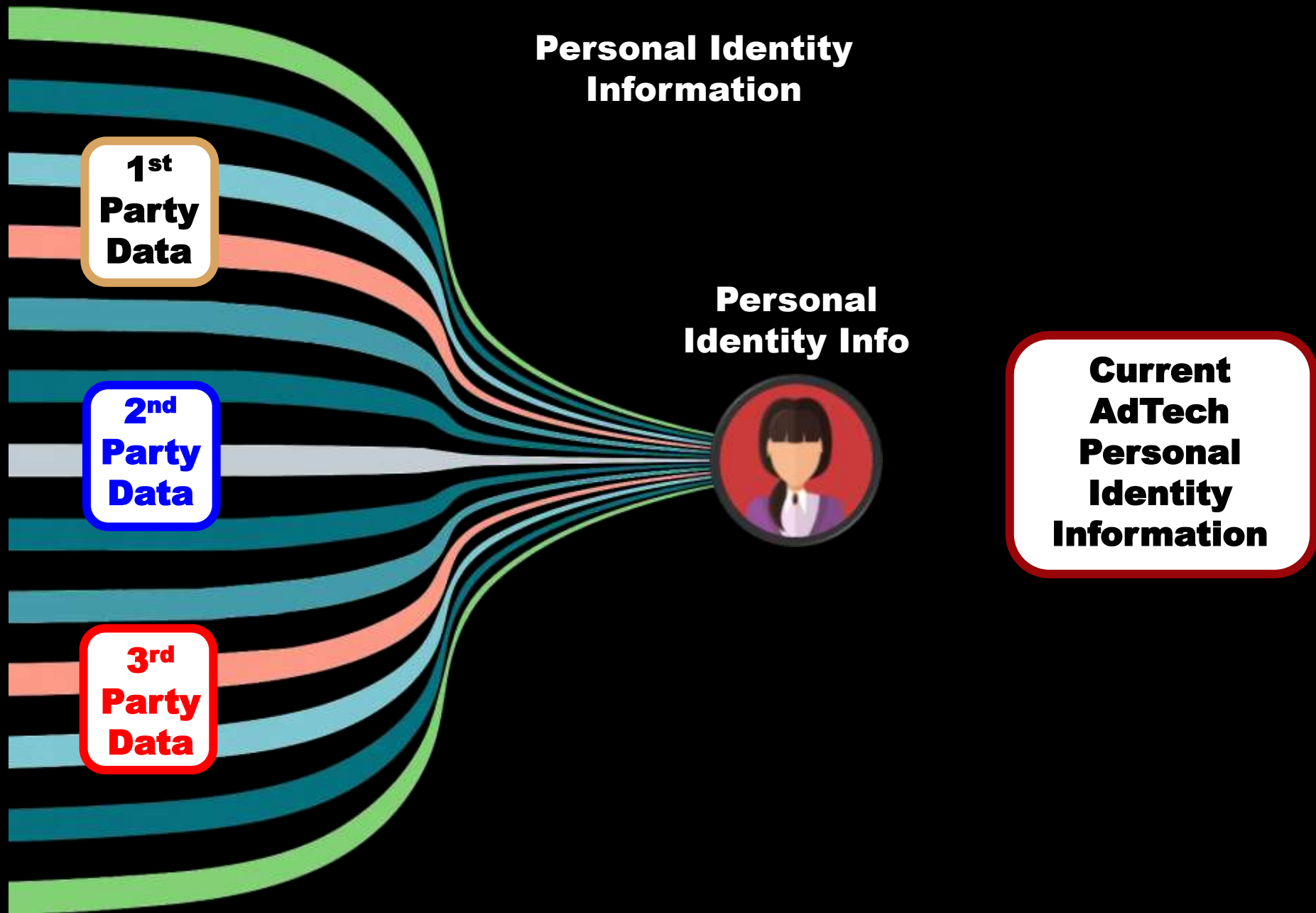
► Second-Party Data:

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.

3rd Party Data

► Third-Party Data:

- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



**Personal Identity
Information**

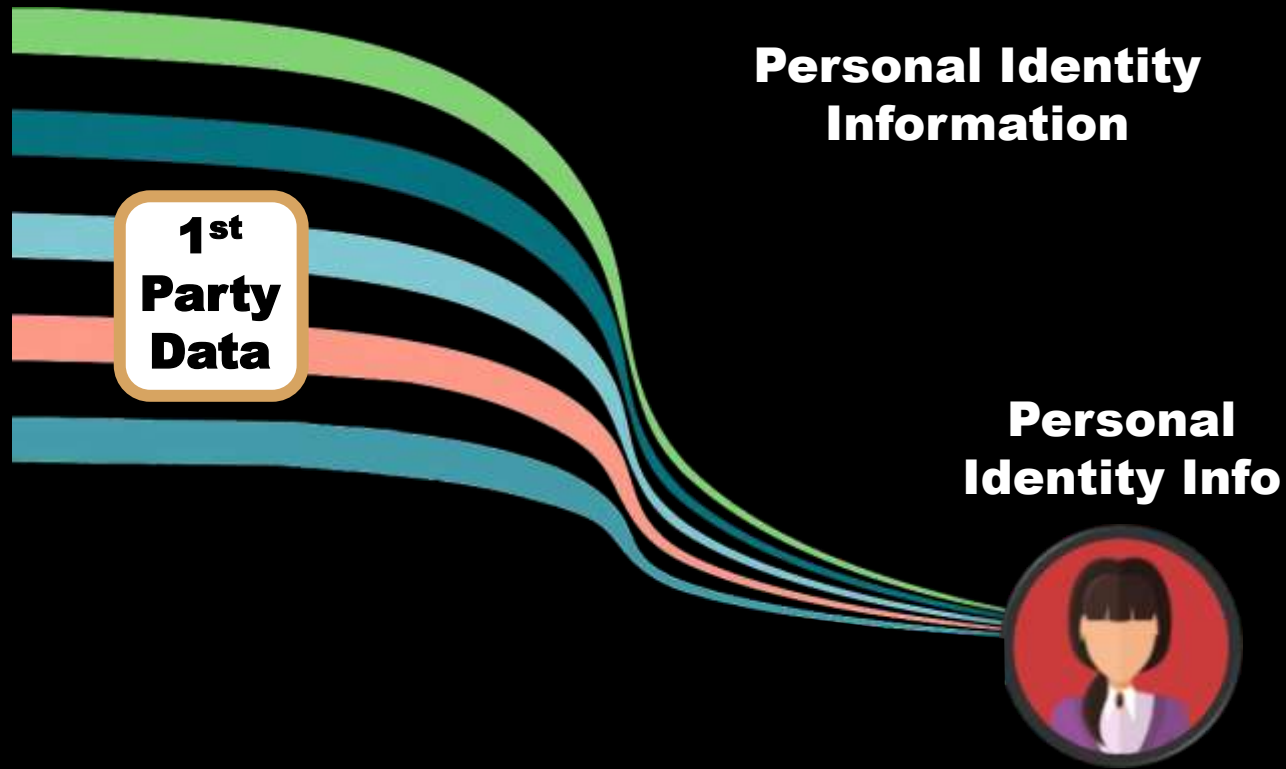
**1st
Party
Data**

**2nd
Party
Data**

**3rd
Party
Data**

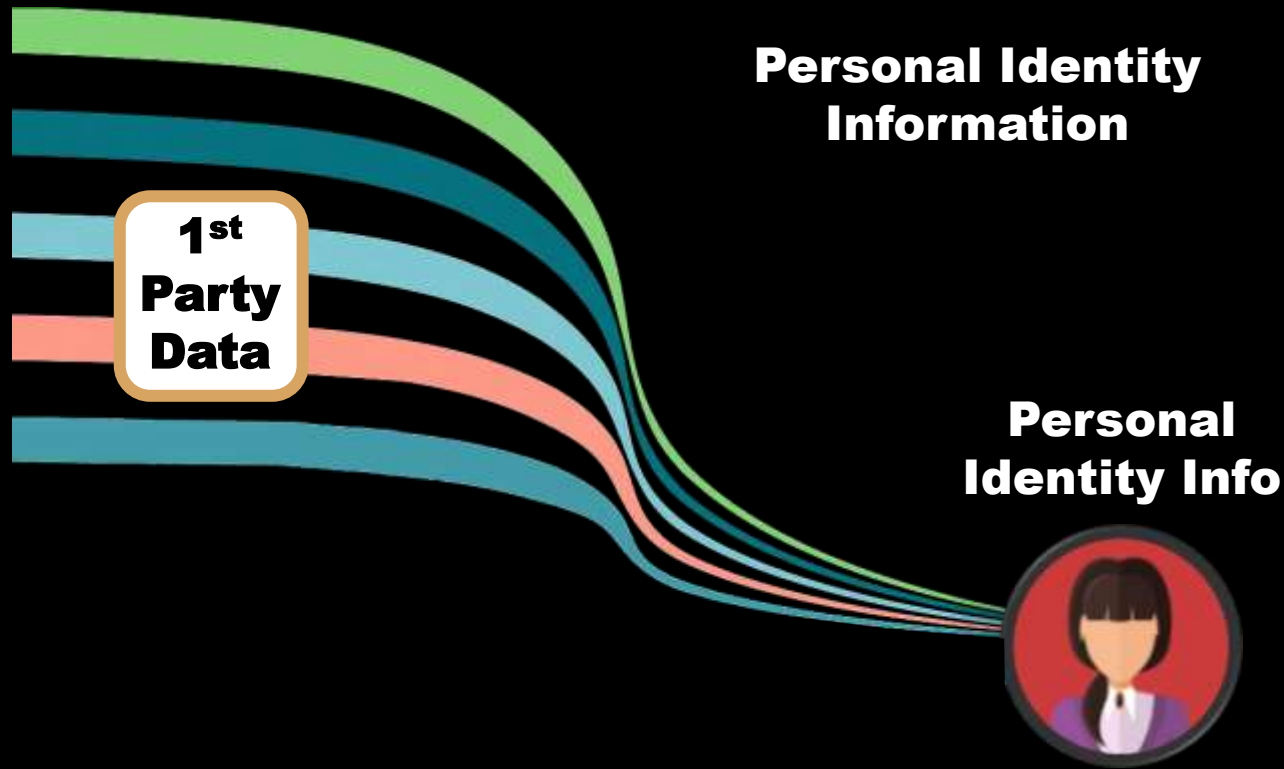
**Personal
Identity Info**





► **First-Party Data:**

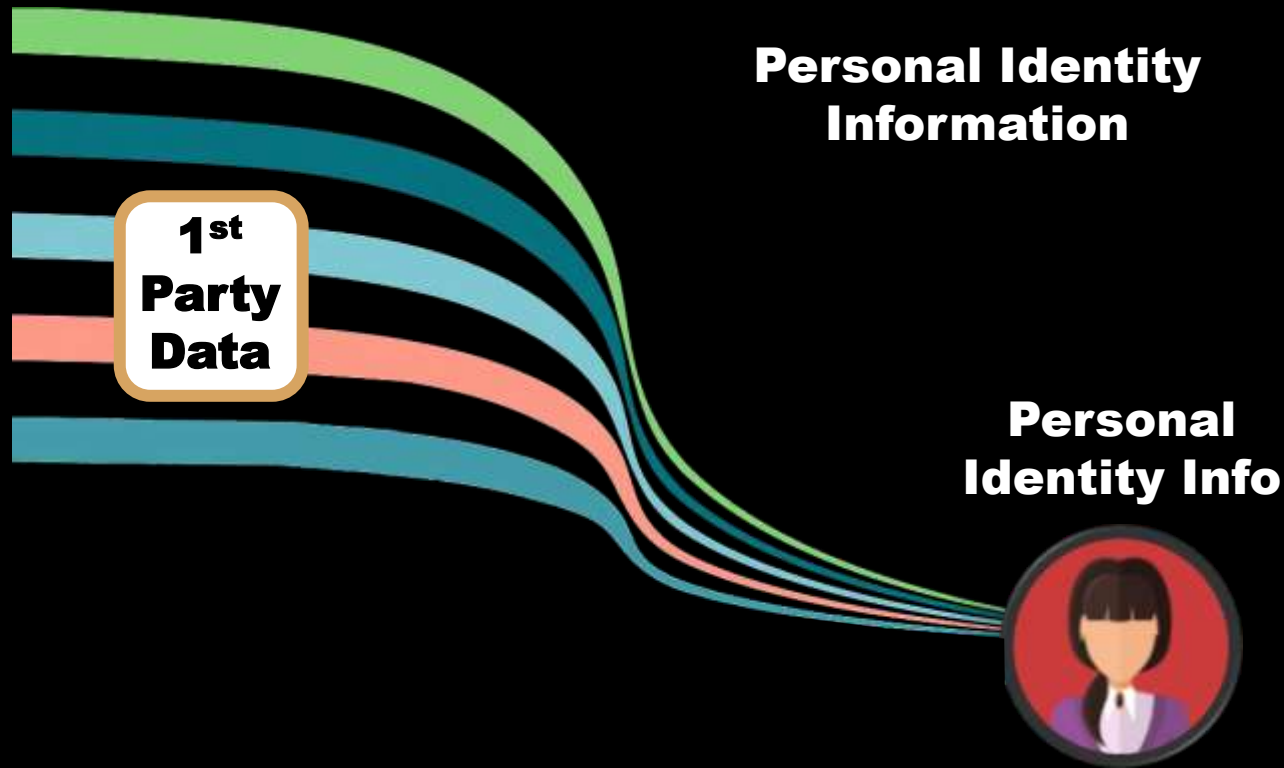
- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner.



First-Party Data
Direct relationship with the customer
Collected with consent
Individual data
High accuracy and reliability
Not shared
Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

► First-Party Data:

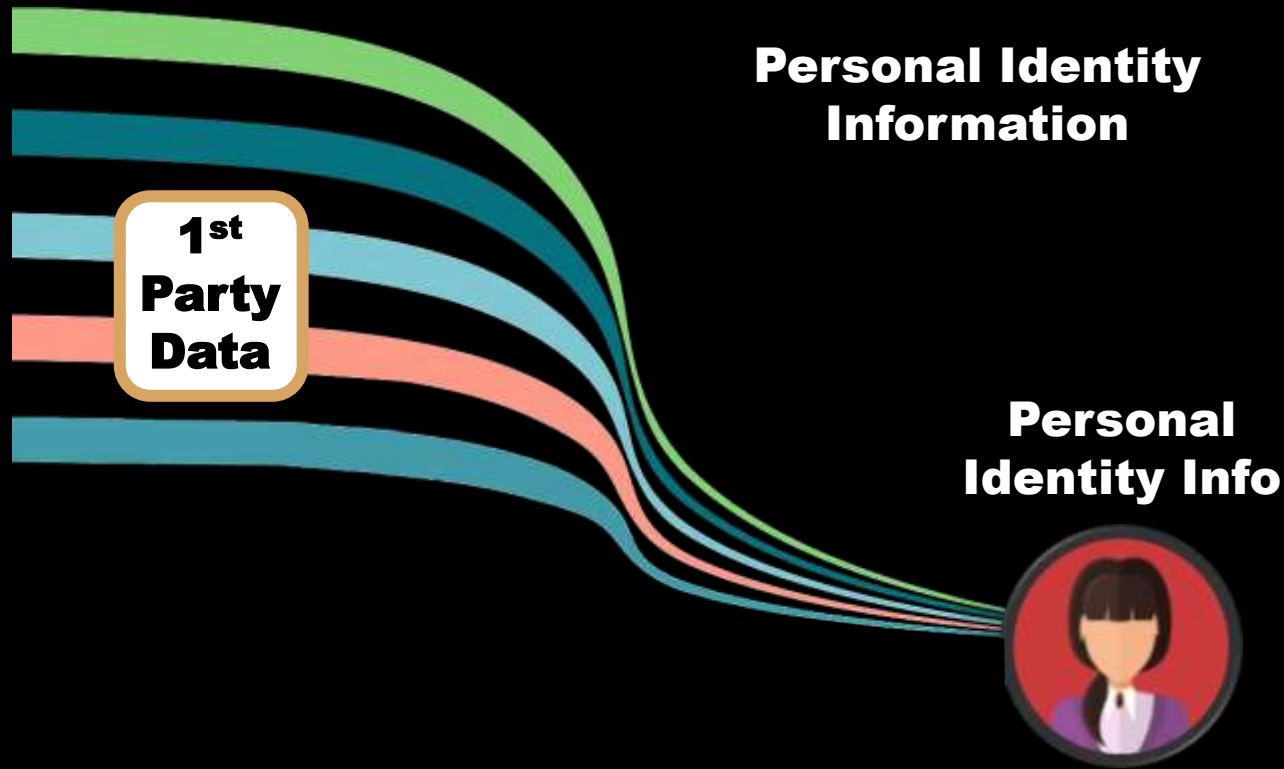
- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



First-Party Data
Direct relationship with the customer
Collected with consent
Individual data
High accuracy and reliability
Not shared
Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

► First-Party Data:

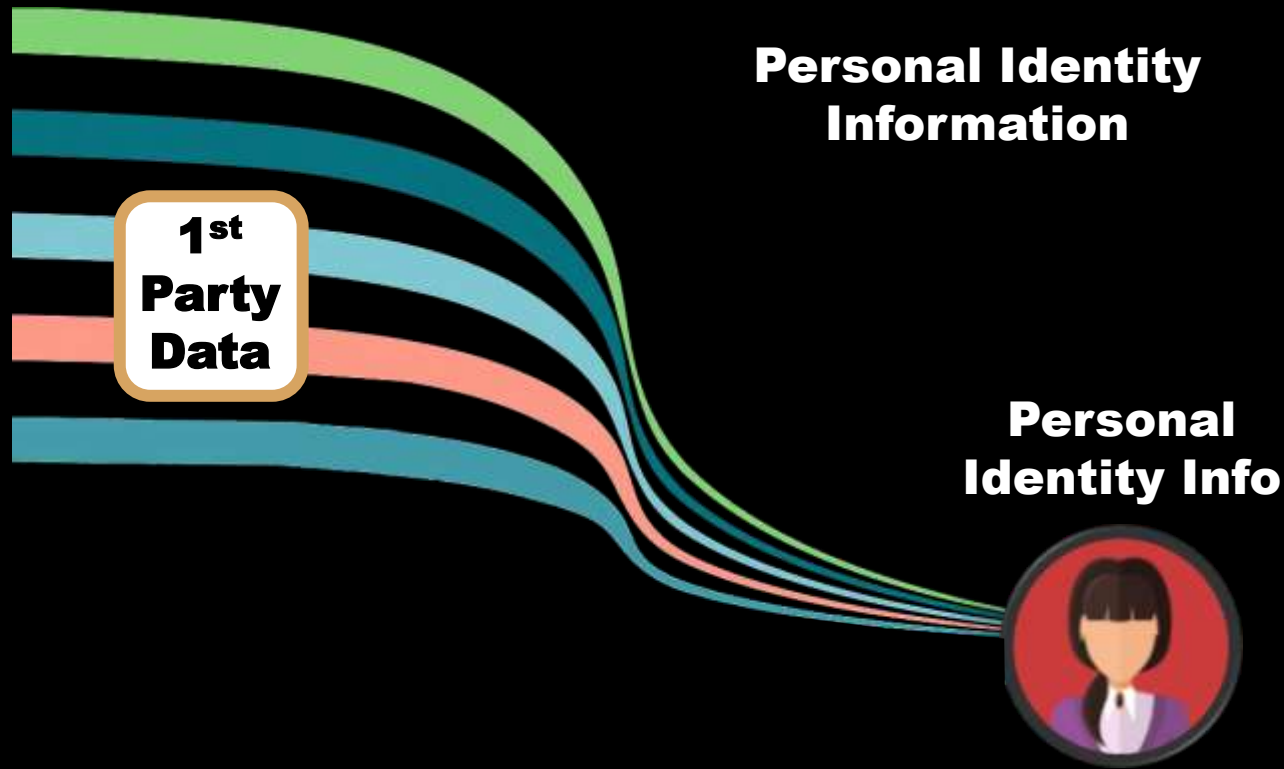
- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



First-Party Data
Direct relationship with the customer
Collected with consent
Individual data
High accuracy and reliability
Not shared
Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

► First-Party Data:

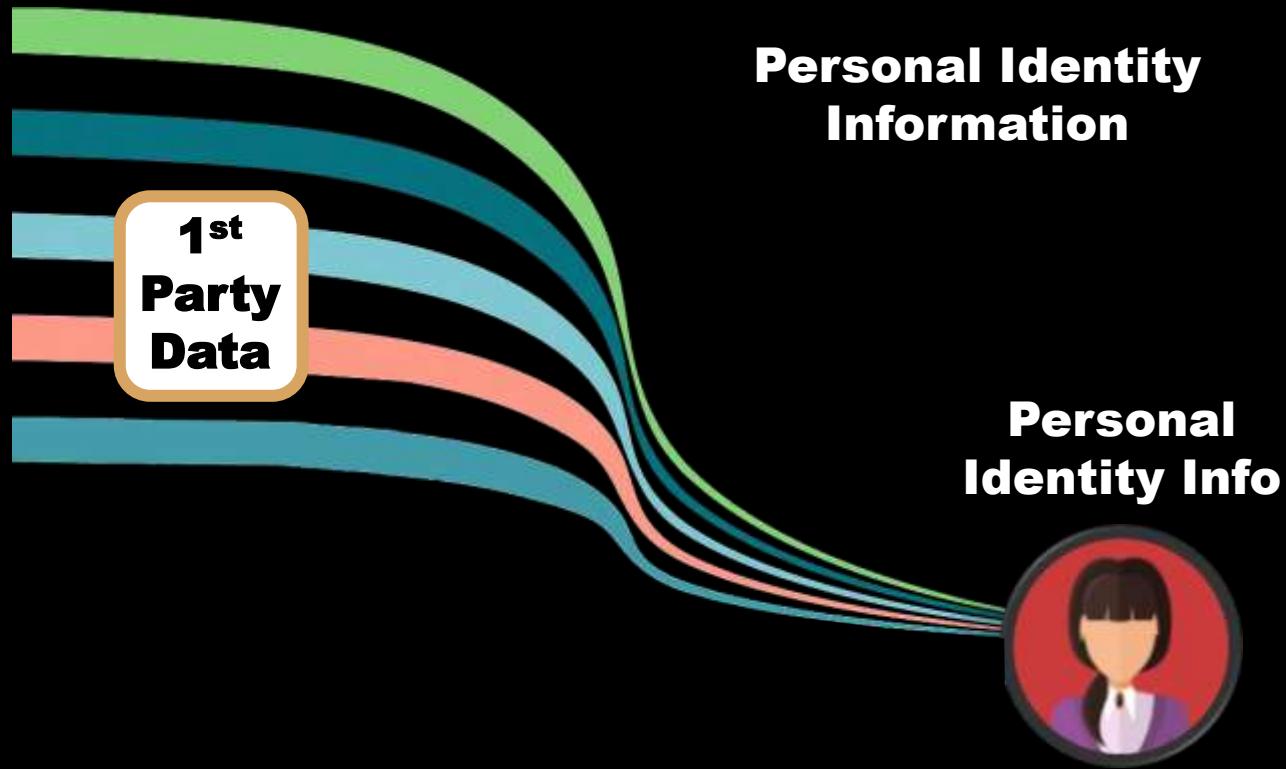
- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



First-Party Data
Direct relationship with the customer
Collected with consent
Individual data
High accuracy and reliability
Not shared
Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

► First-Party Data:

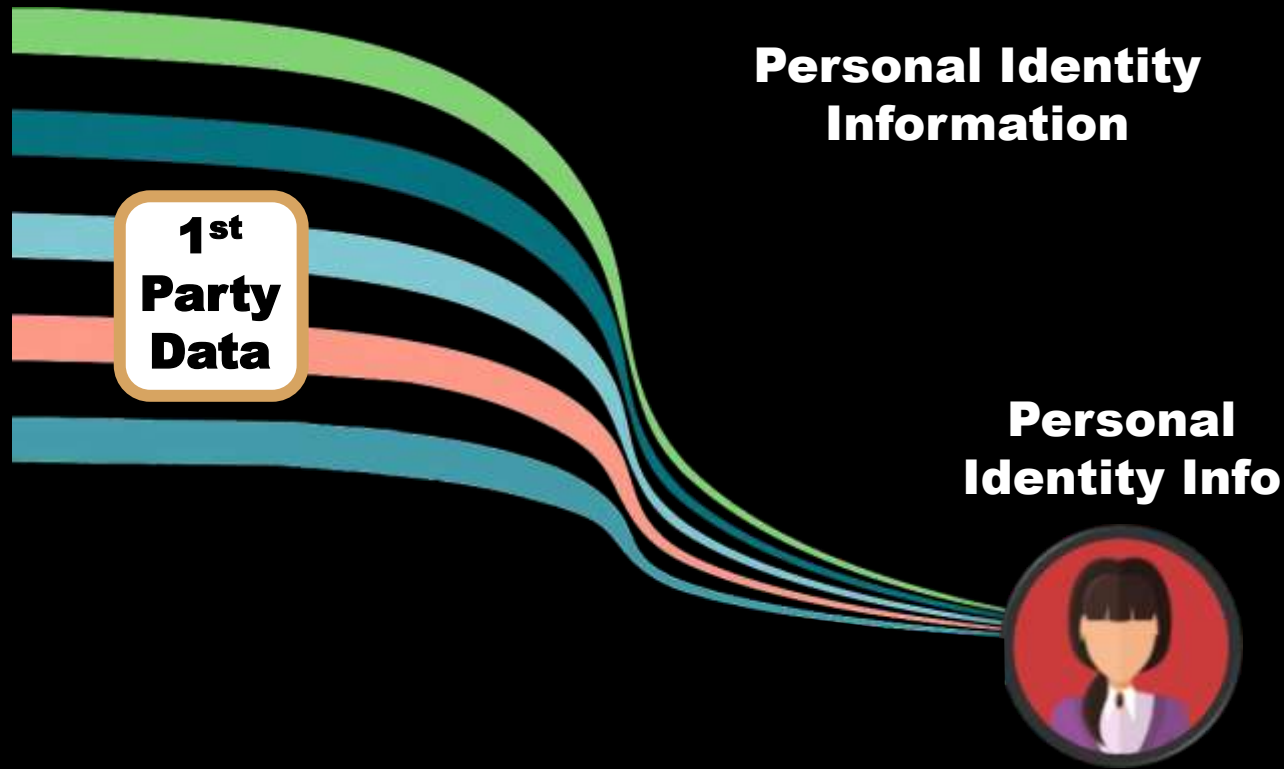
- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



First-Party Data
Direct relationship with the customer
Collected with consent
Individual data
High accuracy and reliability
Not shared
Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

► First-Party Data:

- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



First-Party Data

Direct relationship with the customer

Collected with consent

Individual data

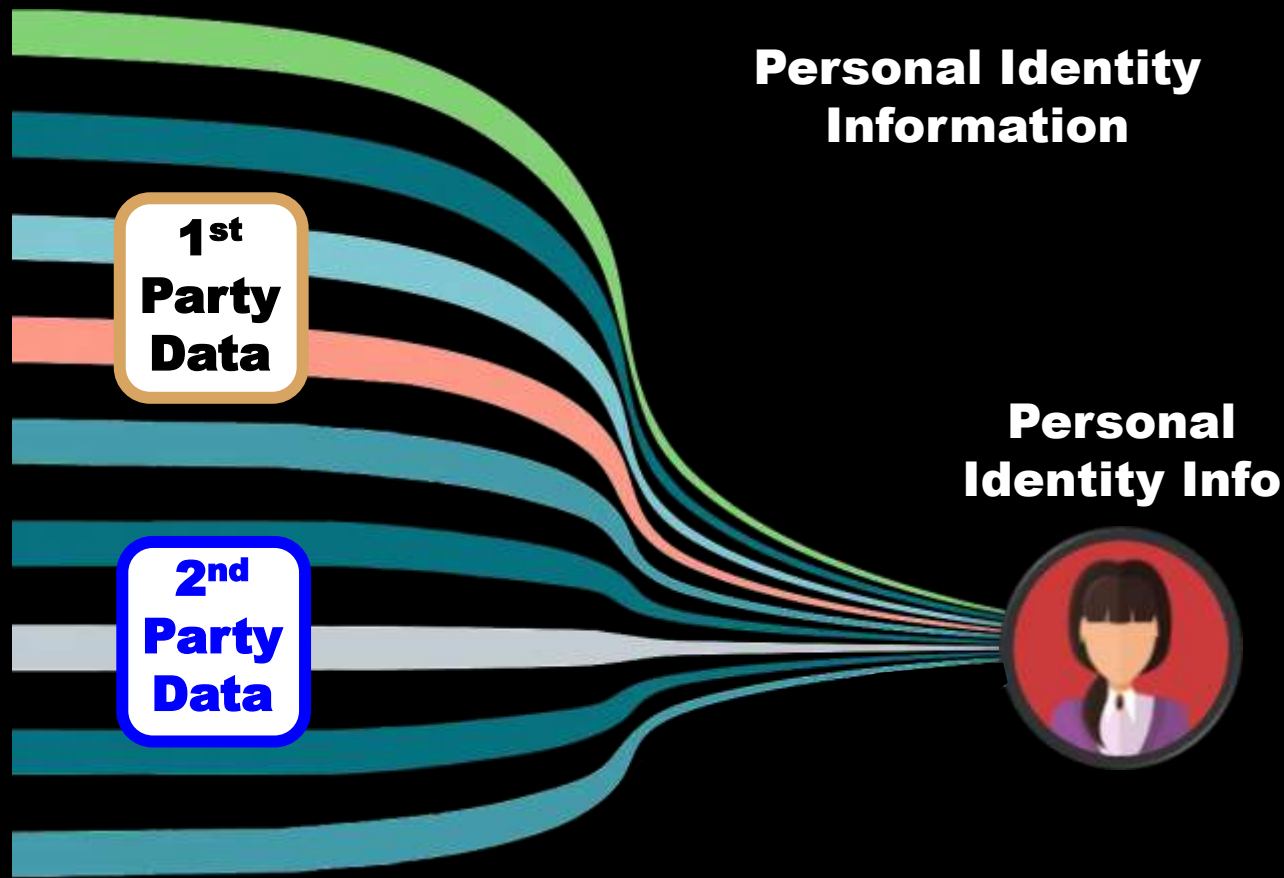
High accuracy and reliability

Not shared

Examples:- Customer email- Phone number- Purchase history- Support history- Loyalty program info

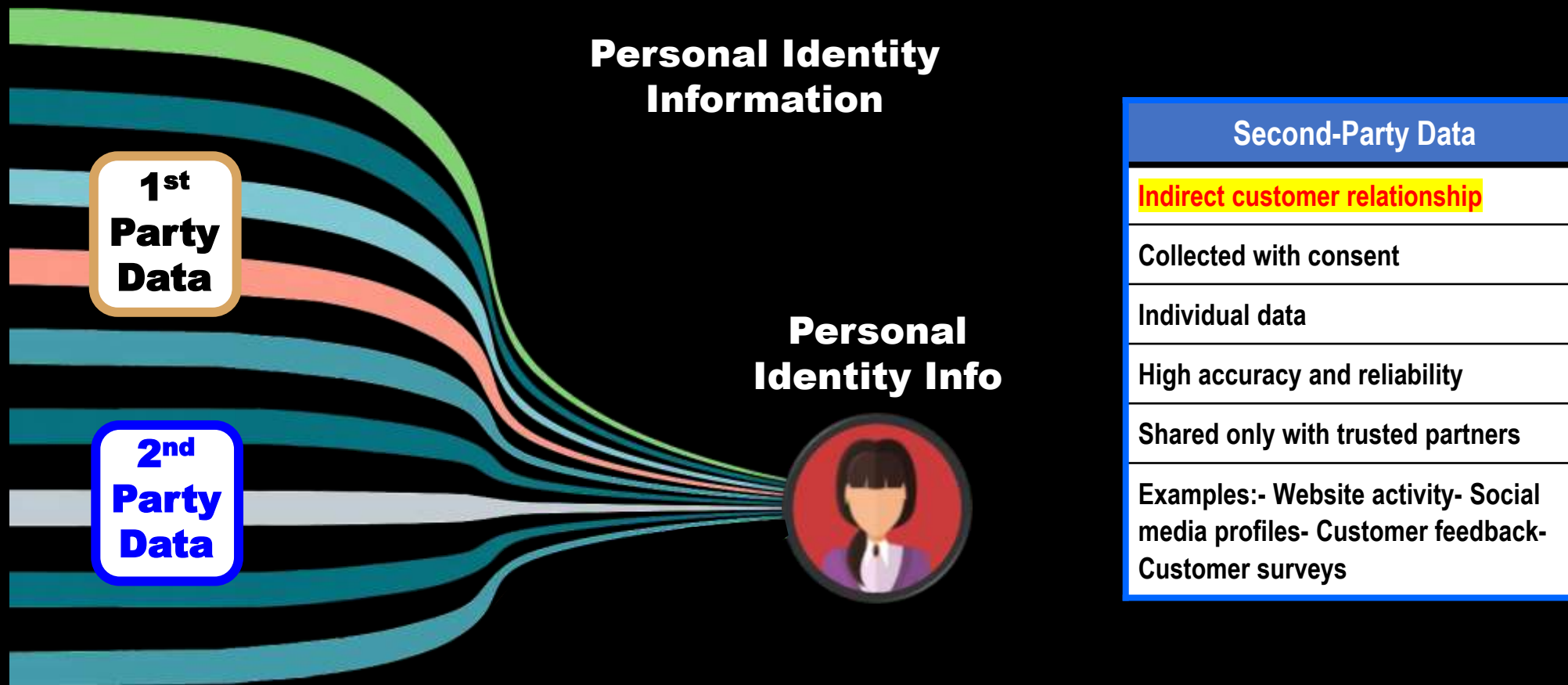
► First-Party Data:

- **Definition:** First-party data refers to information that an organization collects directly from its own customers or users. It is data that the organization owns and controls because it is gathered from its interactions with individuals.
- **Example:** When a website collects data on user behavior, such as website visits, product views, or user preferences, that data is considered first-party data for the website owner..



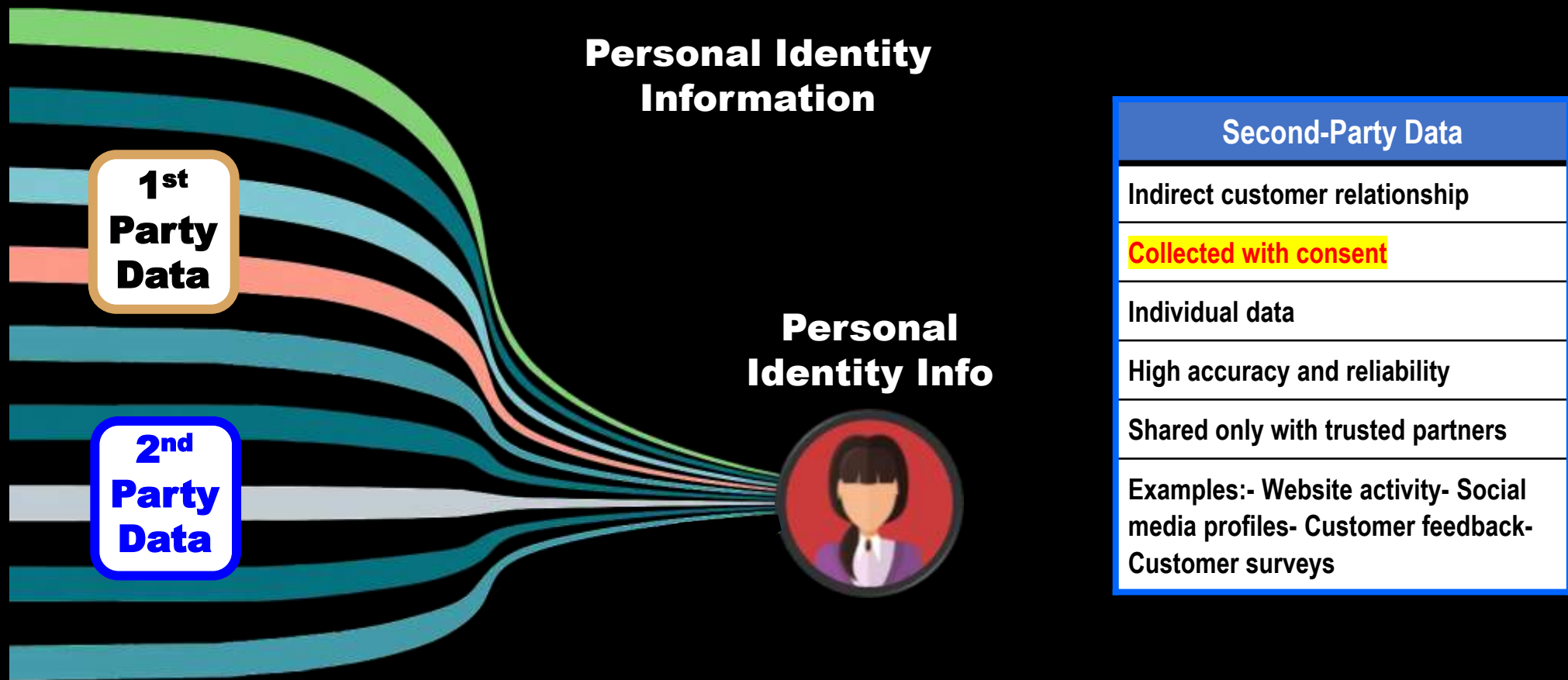
► **Second-Party Data:**

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



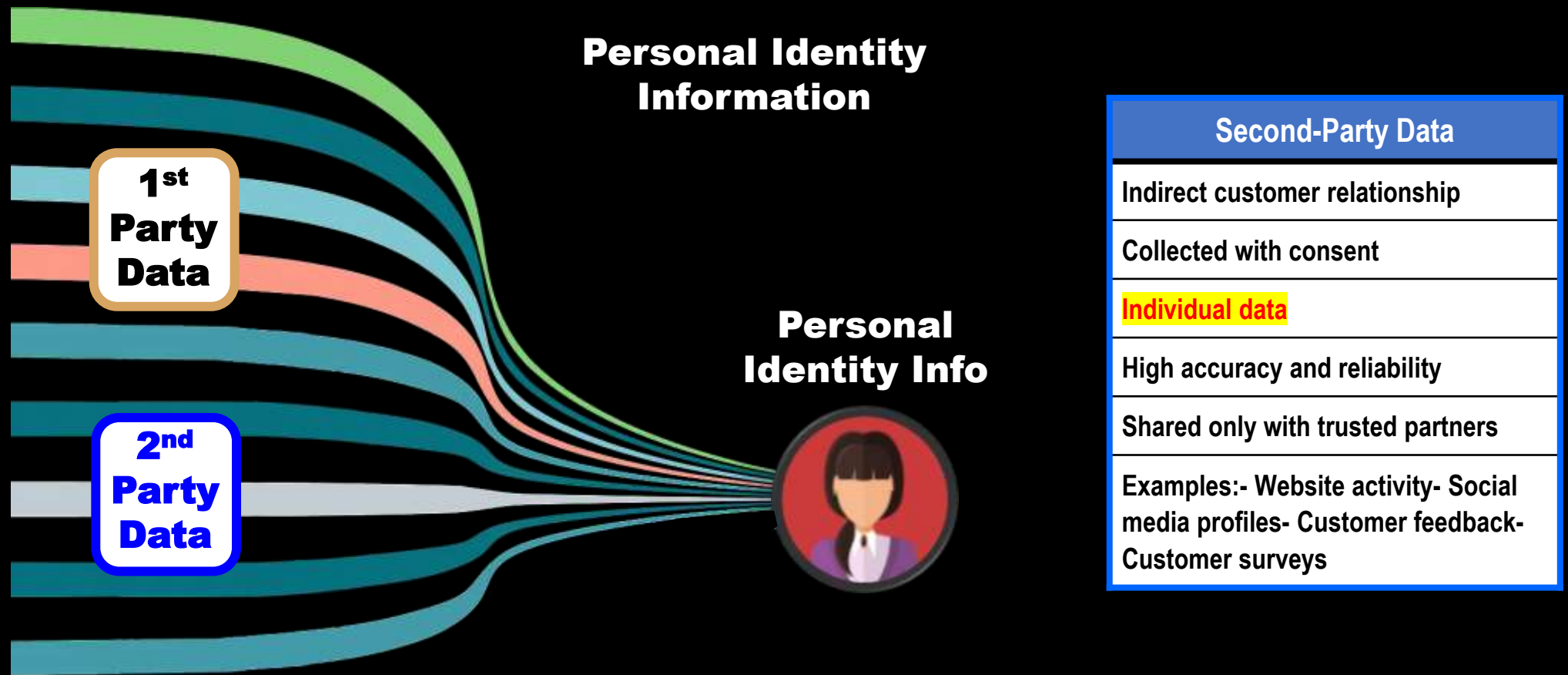
► Second-Party Data:

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



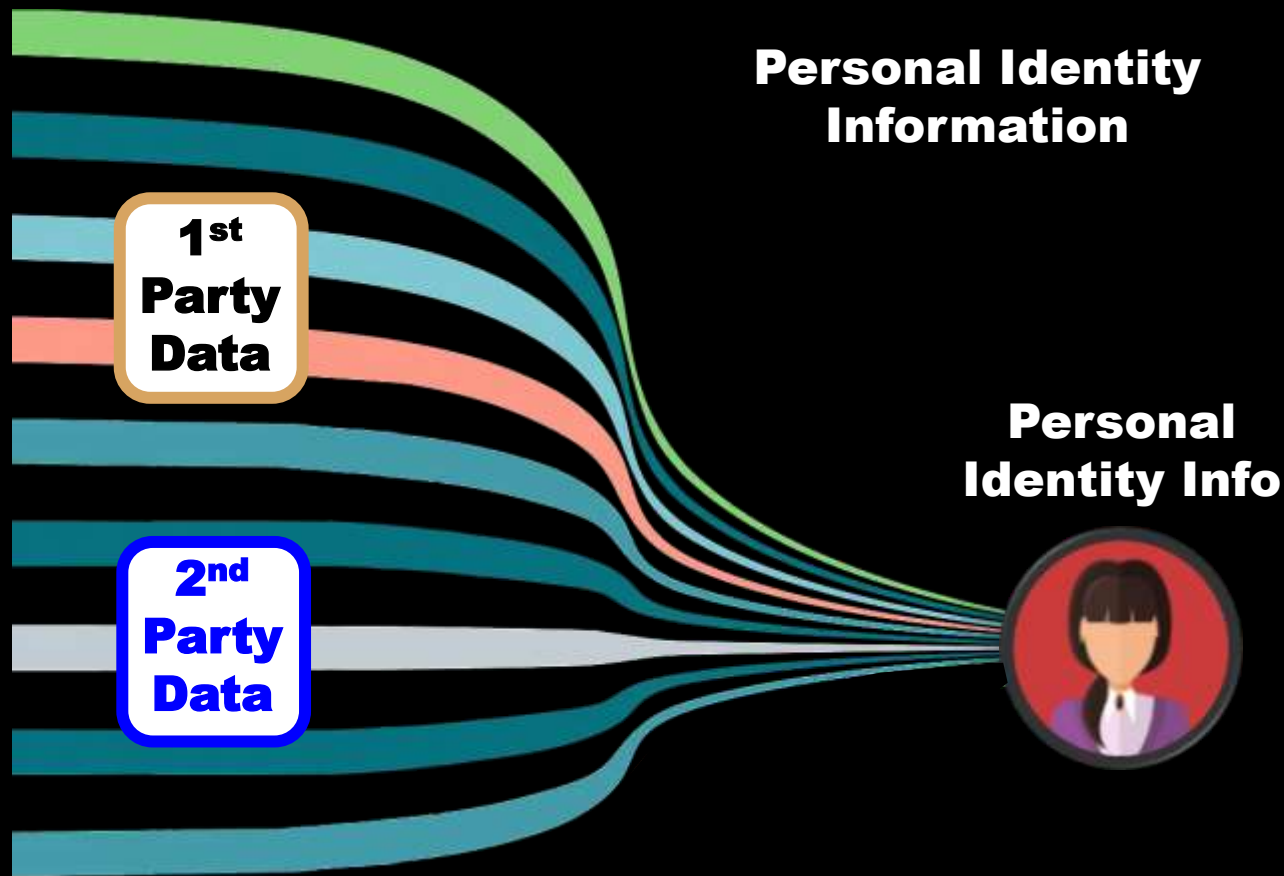
► Second-Party Data:

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



► Second-Party Data:

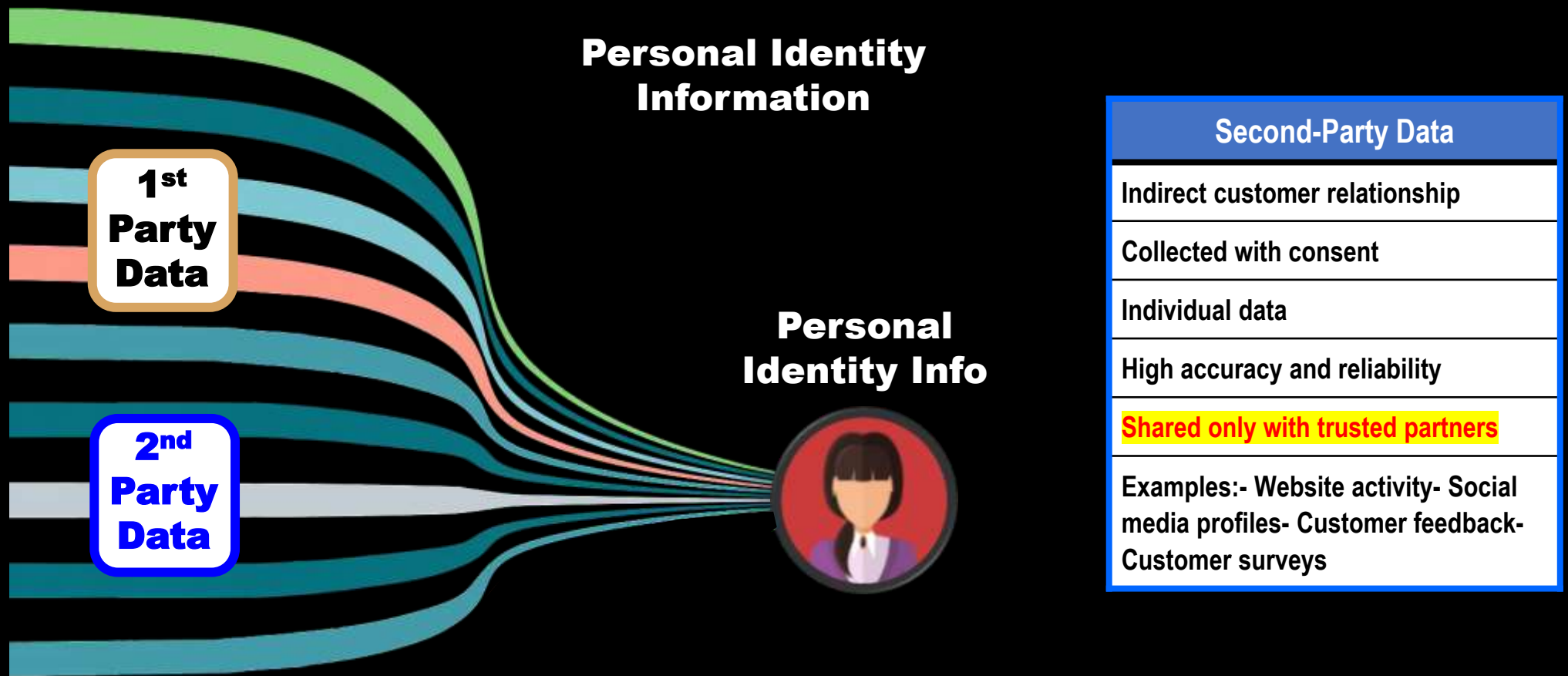
- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



Second-Party Data
Indirect customer relationship
Collected with consent
Individual data
High accuracy and reliability
Shared only with trusted partners
Examples:- Website activity- Social media profiles- Customer feedback- Customer surveys

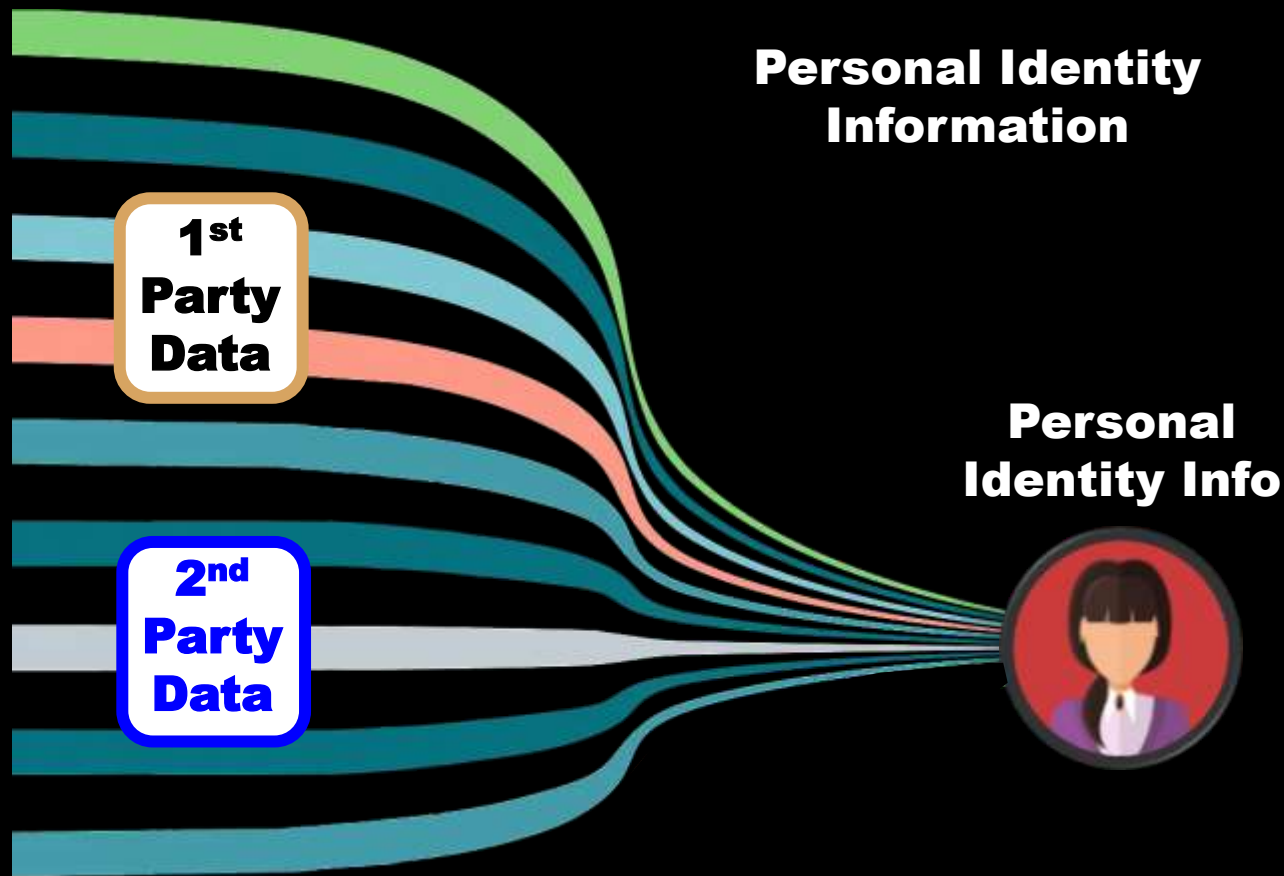
► Second-Party Data:

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



► Second-Party Data:

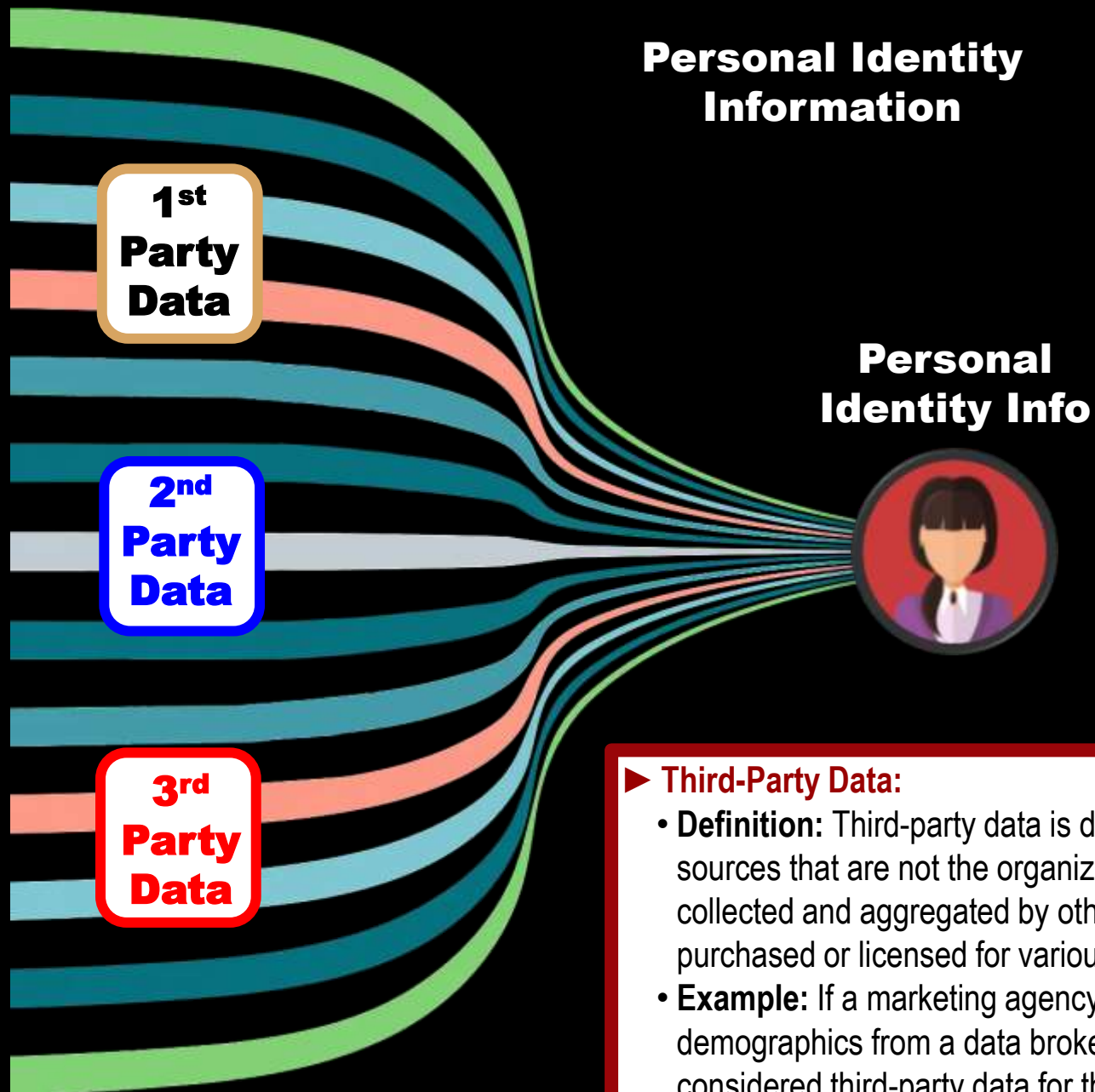
- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



Second-Party Data
Indirect customer relationship
Collected with consent
Individual data
High accuracy and reliability
Shared only with trusted partners
Examples:- Website activity- Social media profiles- Customer feedback- Customer surveys

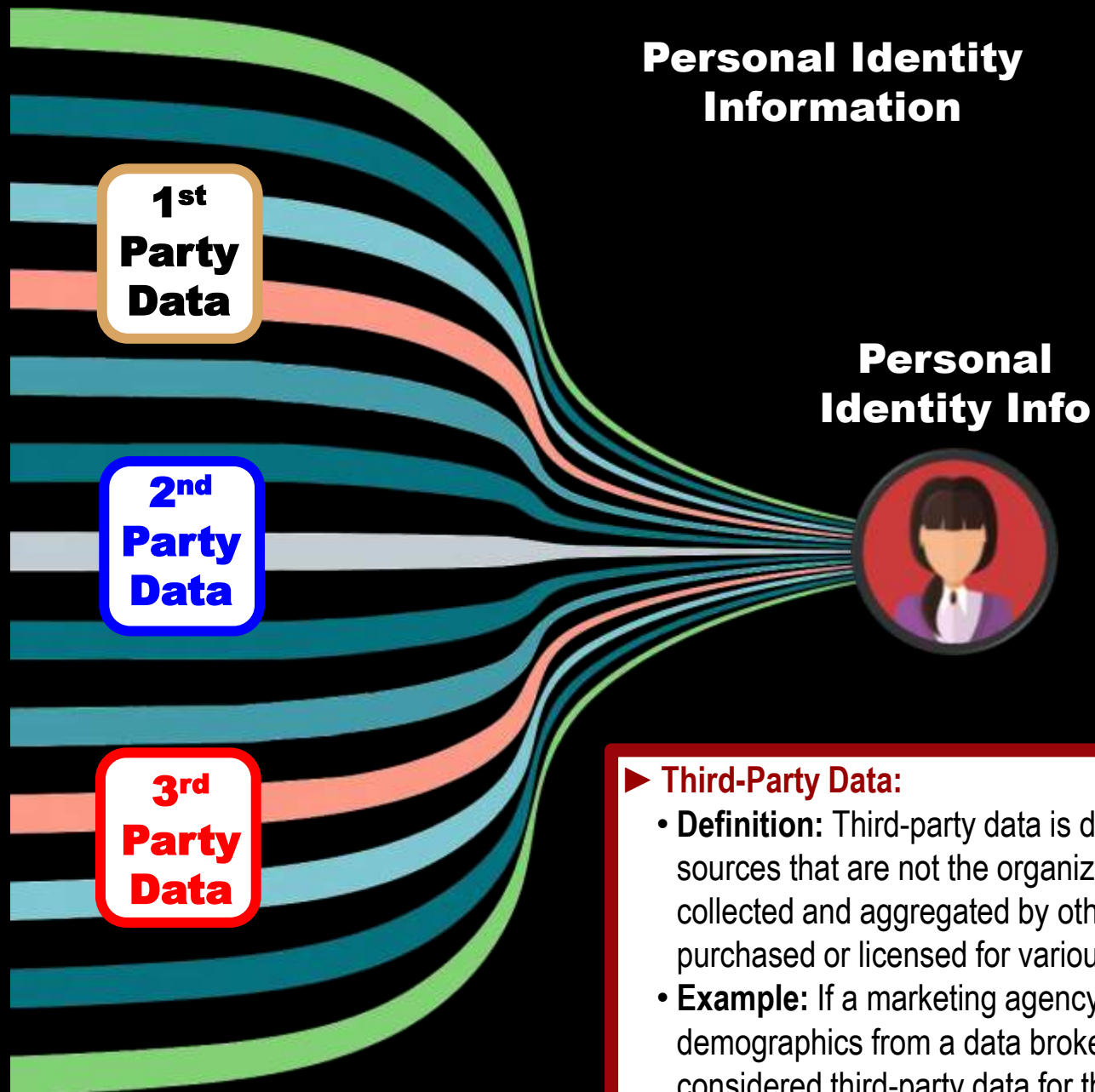
► Second-Party Data:

- **Definition:** Second-party data is essentially someone else's first-party data that is shared with your organization through a direct partnership or agreement. It is data collected by another organization and then shared with your organization, typically in a mutually beneficial arrangement.
- **Example:** If an e-commerce company partners with a complementary business, such as a travel booking platform, to exchange customer data (with consent and privacy compliance), the travel platform's customer data, when used by the e-commerce company, becomes second-party data for them.



► **Third-Party Data:**

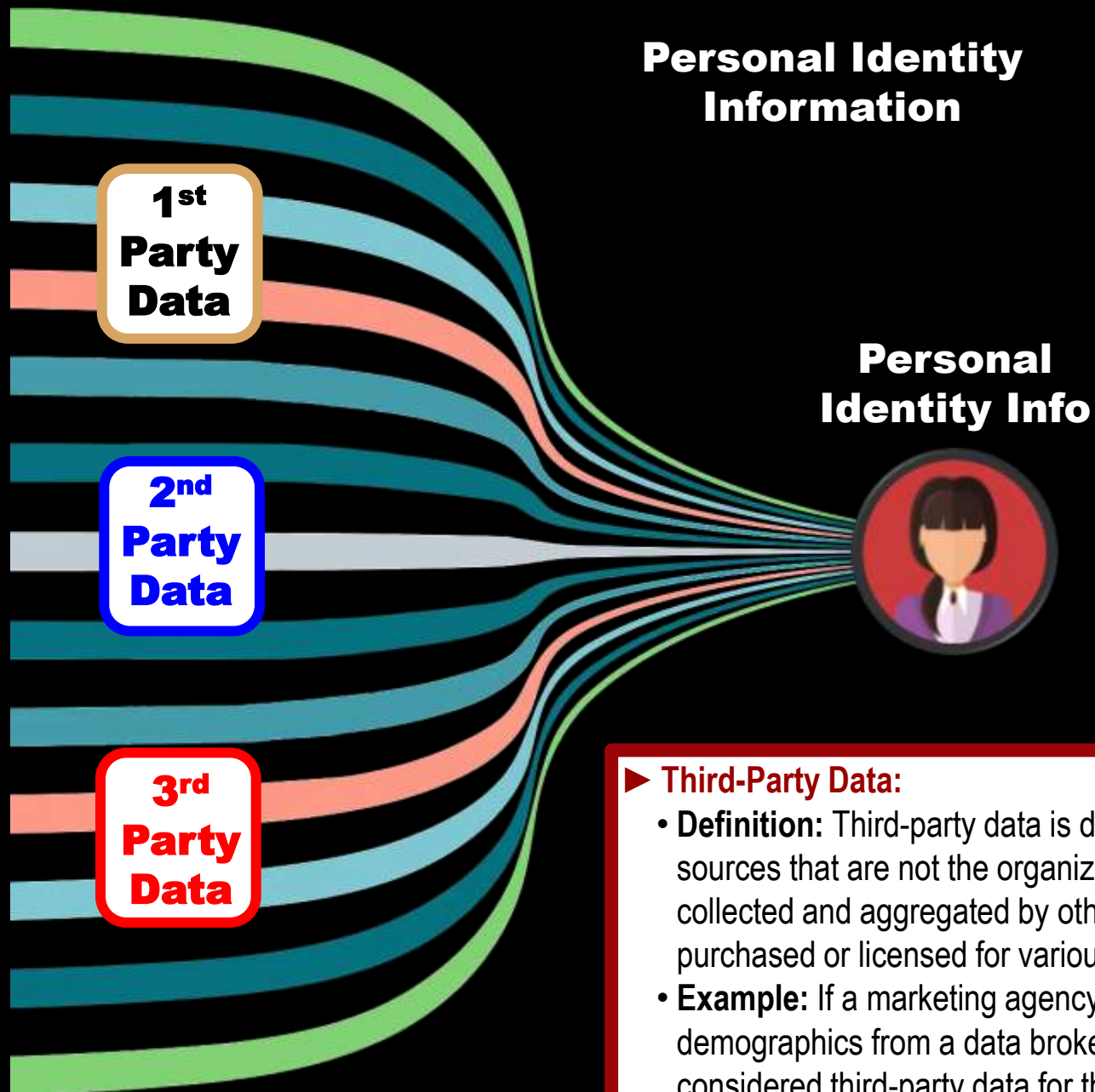
- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► Third-Party Data:

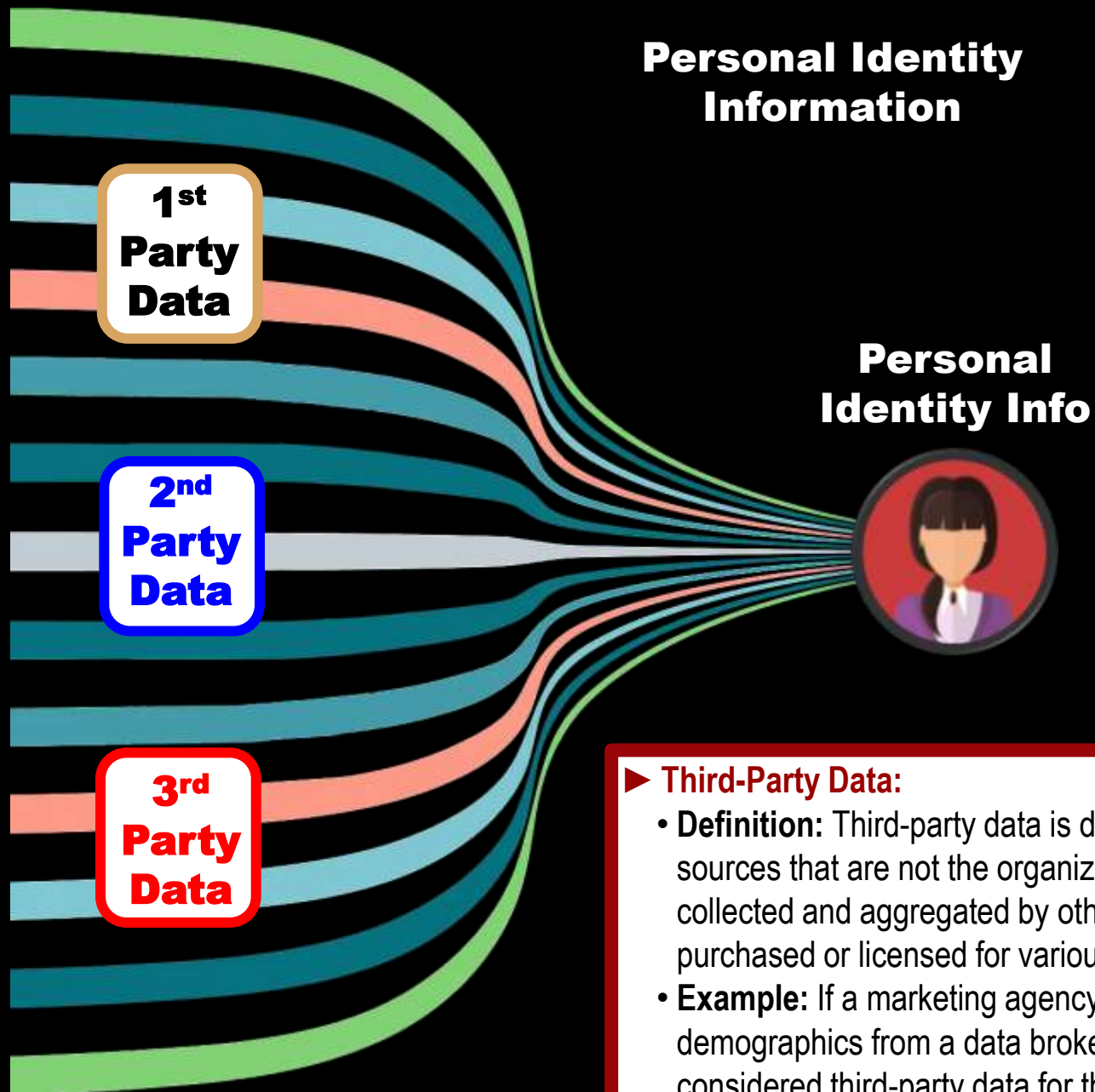
- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► Third-Party Data:

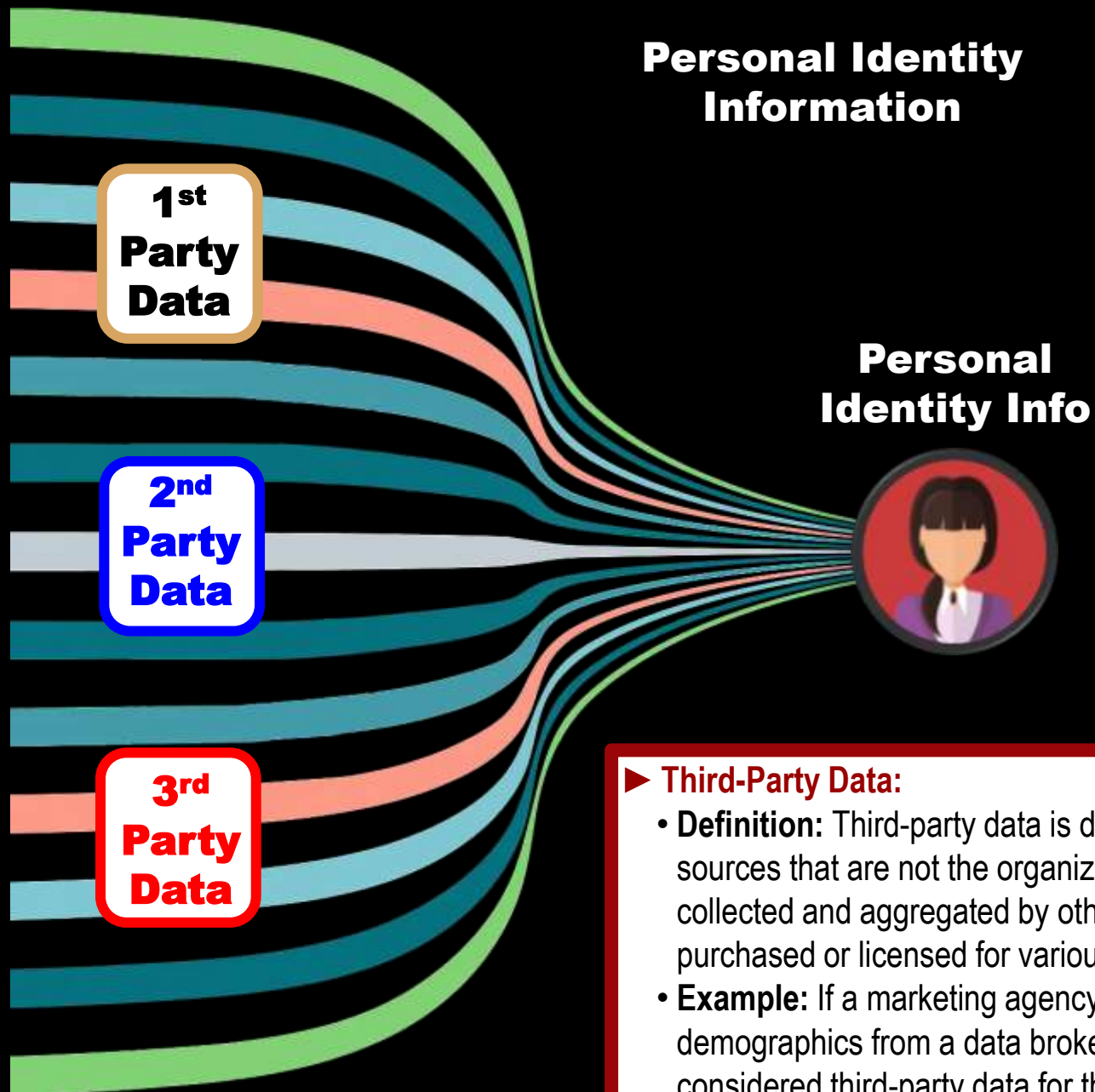
- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► **Third-Party Data:**

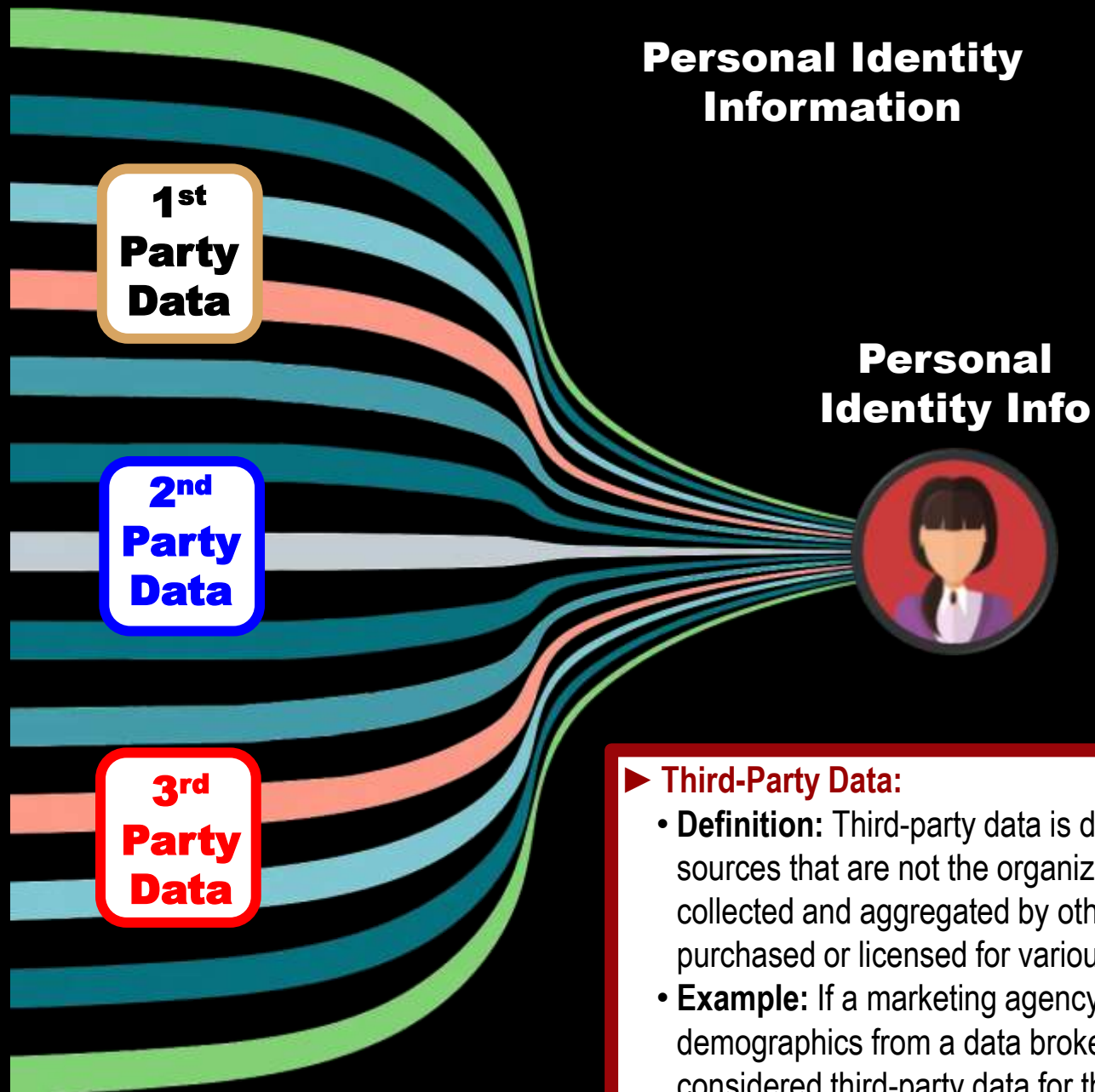
- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► Third-Party Data:

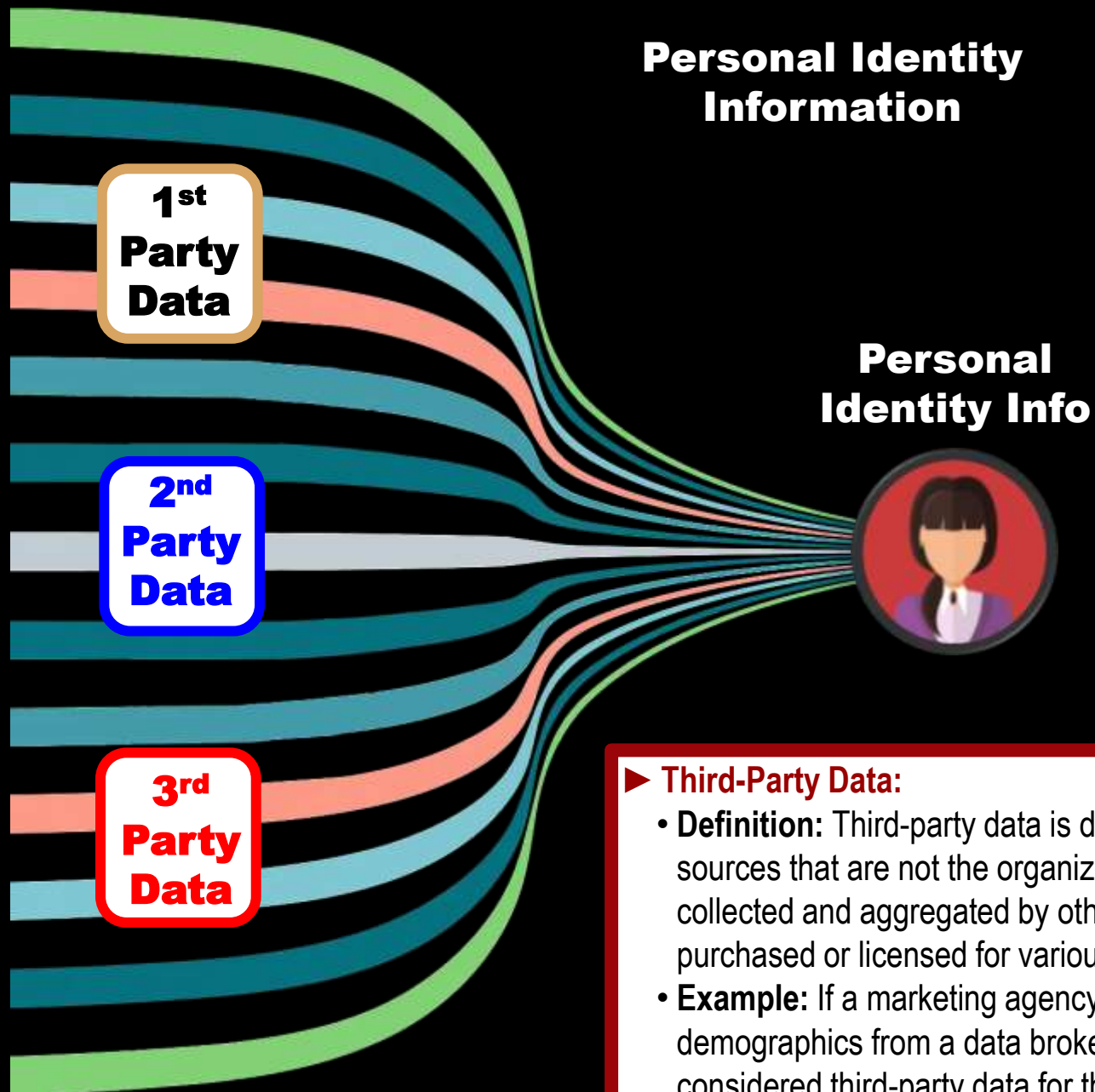
- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.



Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► **Third-Party Data:**

- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.

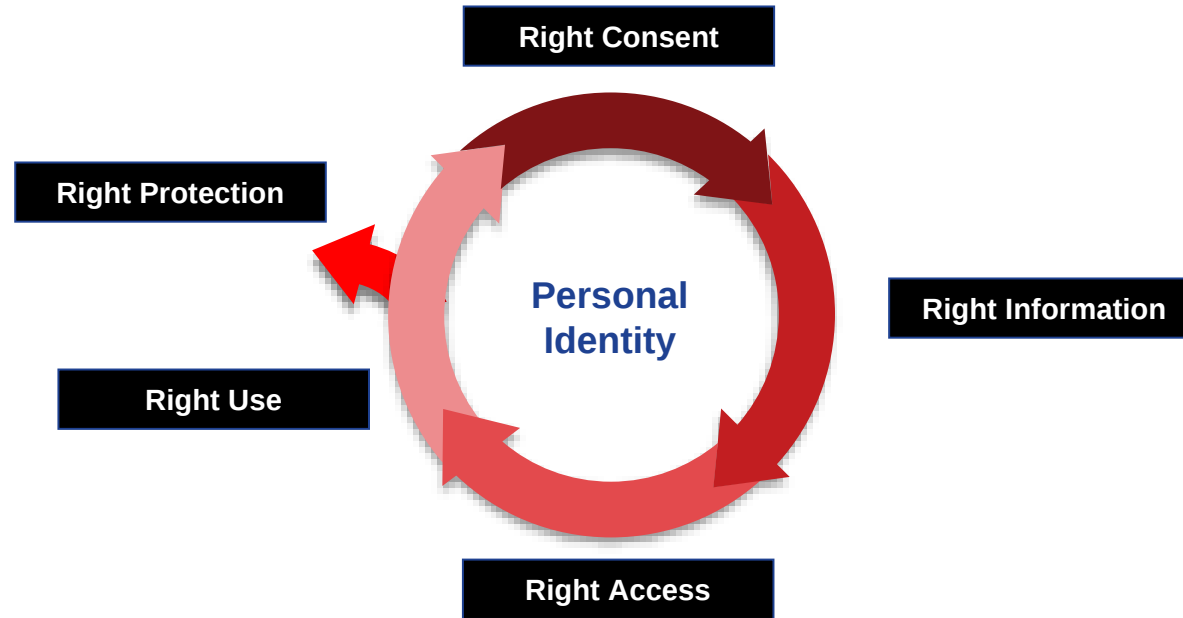


Third-Party Data
Indirect customer relationship
Unknown if it's collected with consent (depends on the data provider)
Aggregate Data
Low accuracy and reliability
Shared with many companies
Examples:- Income – Age- Education- Websites visited- Survey responses

► **Third-Party Data:**

- **Definition:** Third-party data is data that an organization acquires from external sources that are not the organization's own customers or partners. It is data collected and aggregated by other entities, such as data brokers, and is typically purchased or licensed for various purposes, including marketing and analytics.
- **Example:** If a marketing agency buys a dataset of consumer preferences and demographics from a data broker to target advertising campaigns, that dataset is considered third-party data for the marketing agency.

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

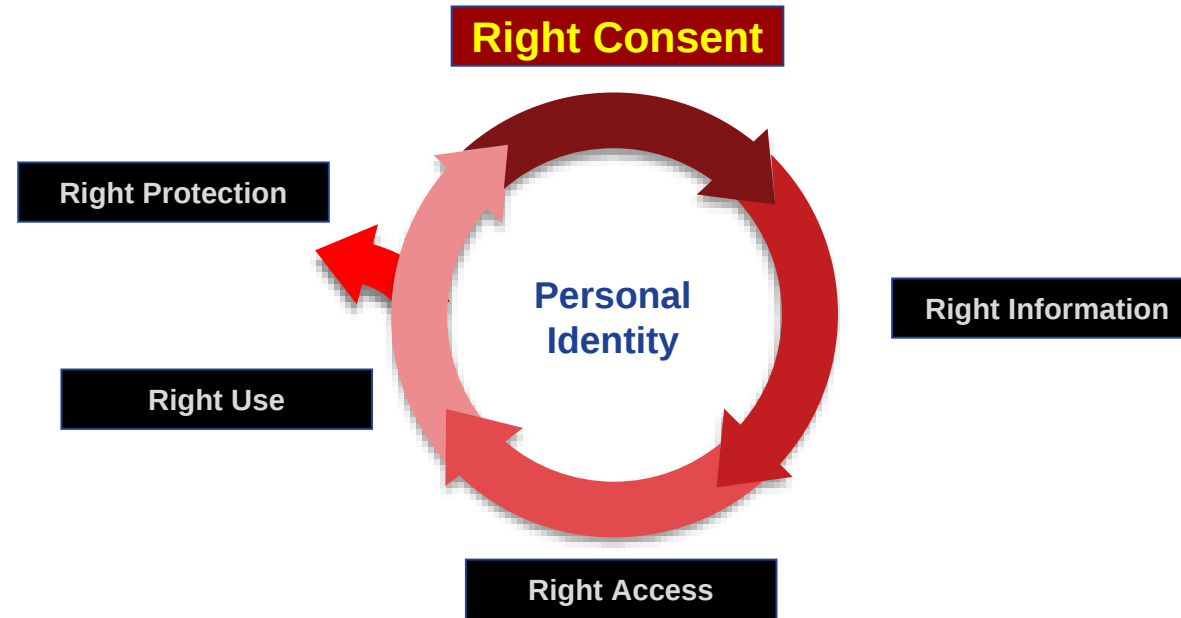
Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

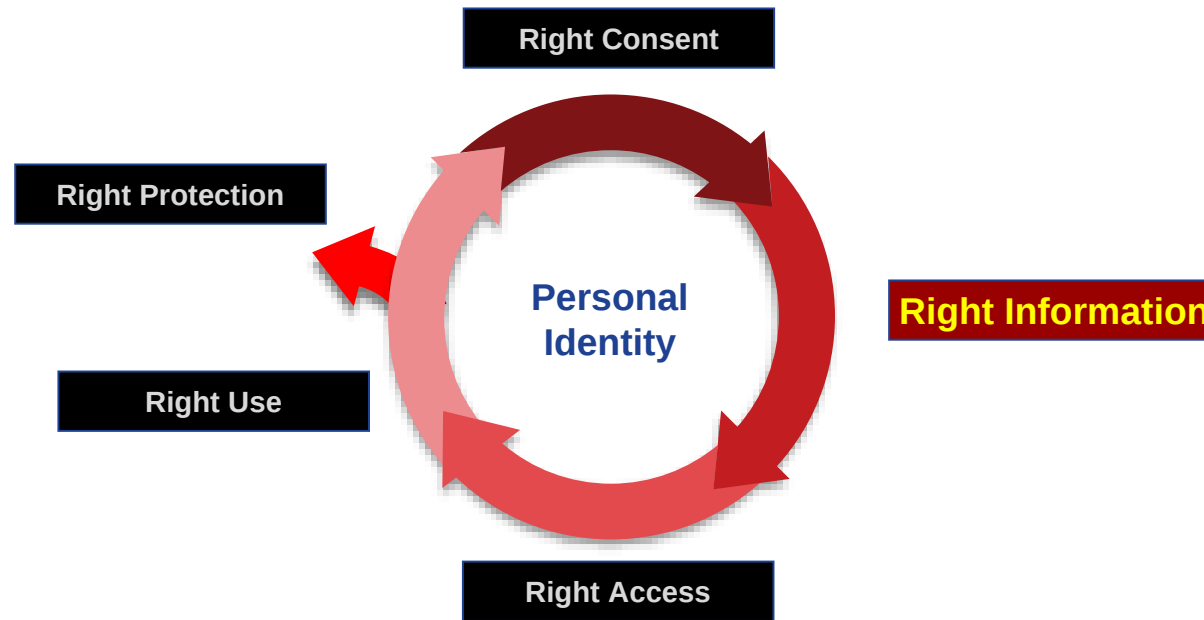
Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

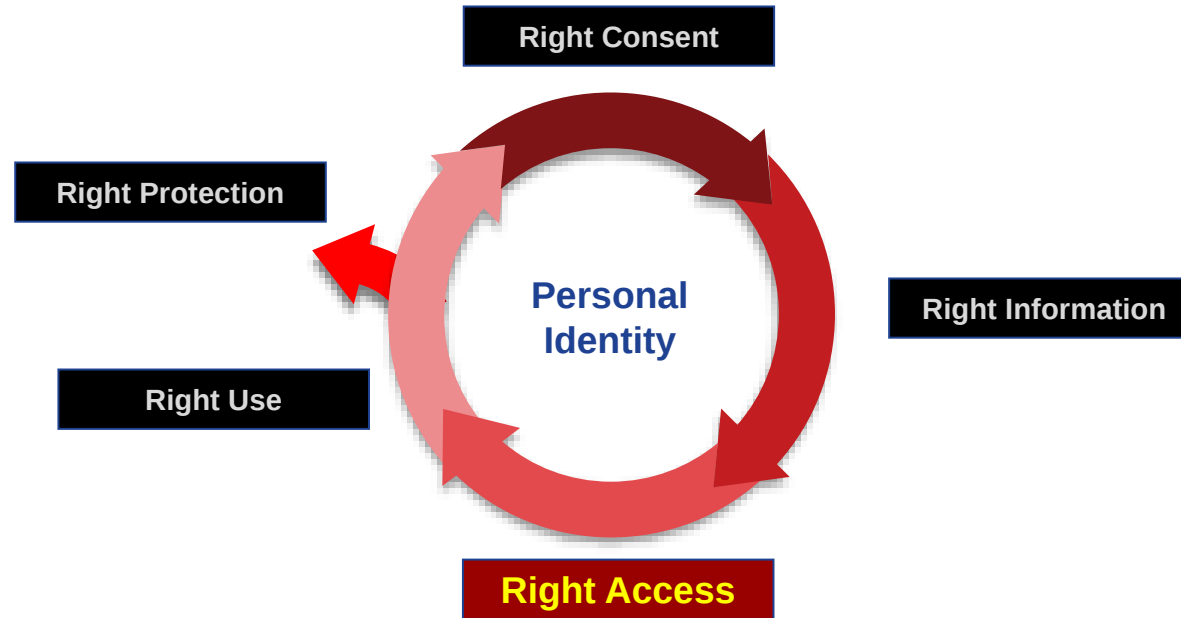
Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

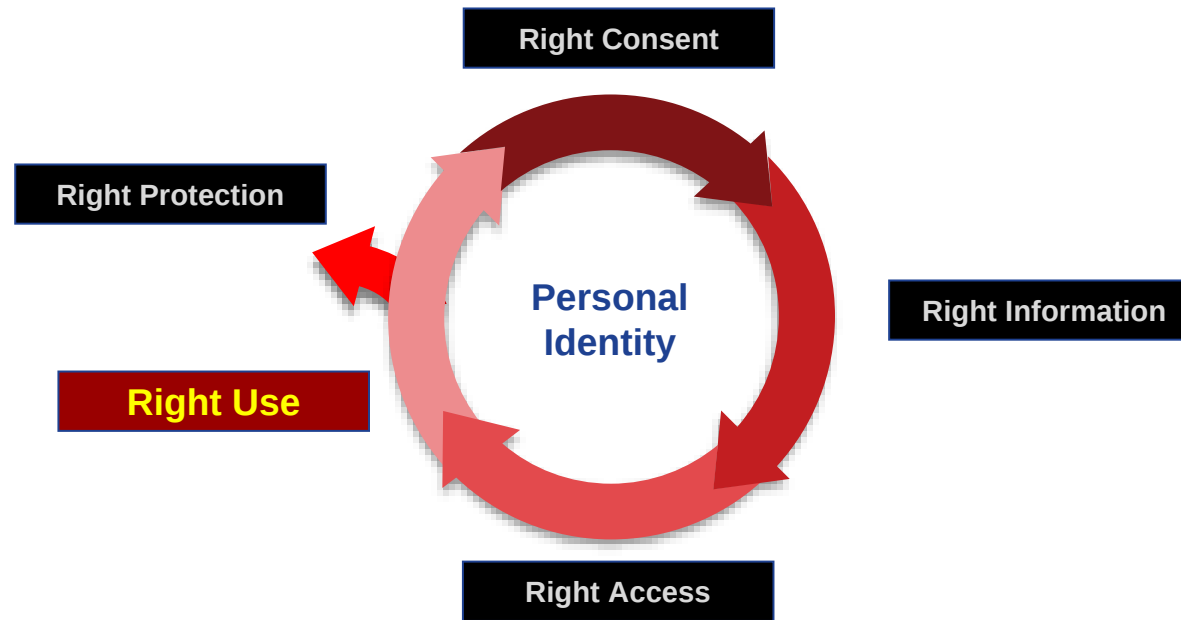
Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

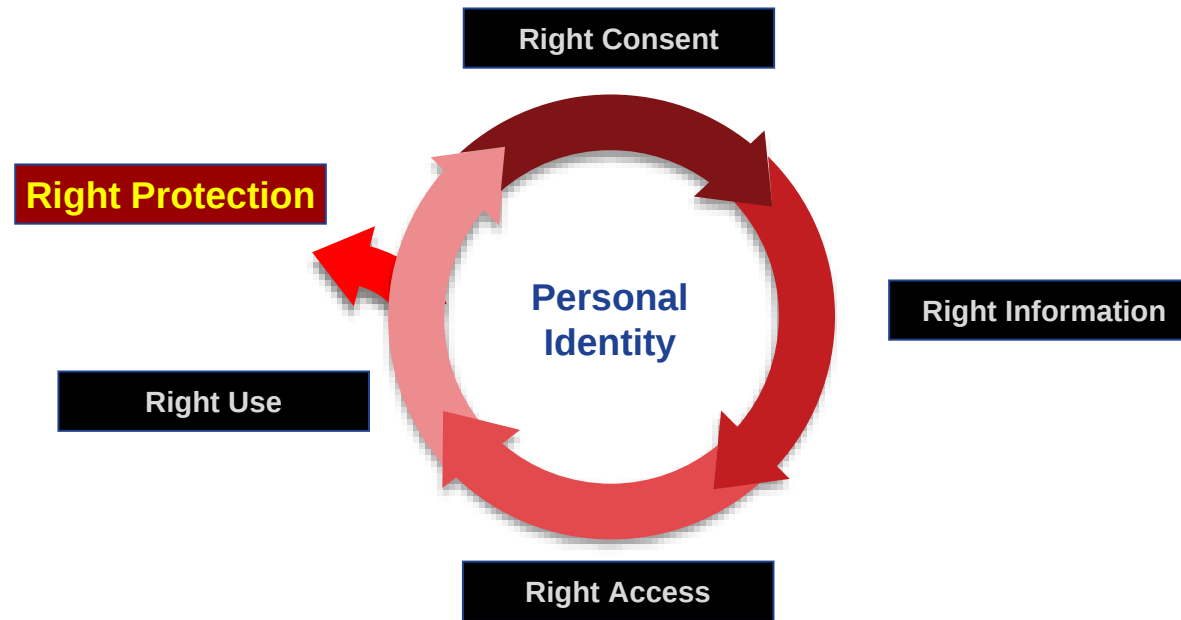
Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

The 5 Rights of My Identity™



Right Consent: Proper consent must include privacy and use preferences and be revocable. The use of tools and methods such as cookies can track user's online behavior such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles which may infringe on user's privacy.

Right Information: The information collected and used may be inaccurate. Third Party Data that is unconsented for access and use which is aggregated and integrated may be inaccurate and violate the privacy of the individual.

Right Access: Historically third -party cookies have led to the data being shared with advertising and analytics companies without the user's full awareness or control. In order to be in full compliance with the evolving regulations, access to personal data must be granted.

Right Use: Individuals should have the right to privacy and use preferences that may be revocable and granted regularly.

Right Protection: It is critical that the personal identity information that is collected and stored is protected from breach, misuse, fraud, and potential harm to individuals and their families.

Sources: HCC Global

What is “Consent”?



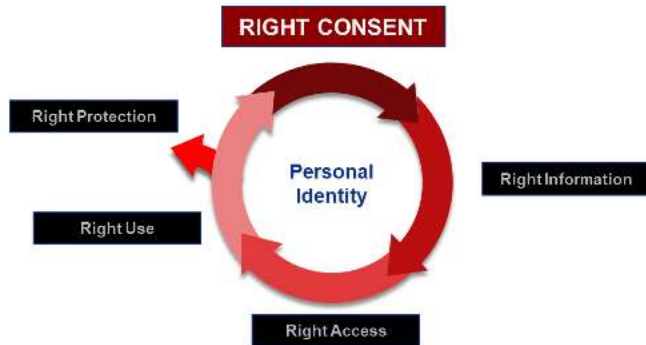
The definition of consent typically involves the following key elements:

- 1. Voluntary Agreement:** Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.
- 2. Informed:** Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is collected, and who the data will be shared with, among other relevant details.
- 3. Specific and Granular:** Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).
- 4. Affirmative Action:** Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.
- 5. Easily Withdrawn:** Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.
- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

The definition of consent typically involves the following key elements:

1. Voluntary Agreement: Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.

The 5 Rights of My Identity™



collected, and who the data will be shared with, among other relevant details.

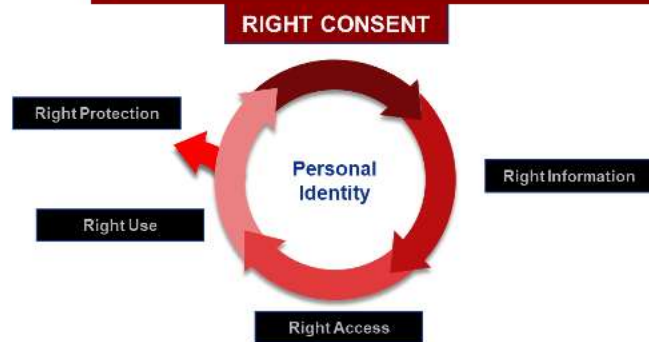
- 3. Specific and Granular:** Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).
- 4. Affirmative Action:** Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.
- 5. Easily Withdrawn:** Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.
- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

What is “Consent”?

The definition of consent typically involves the following key elements:

1. Voluntary Agreement: Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users

2. Informed: Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is collected, and who the data will be shared with, among other relevant details.



Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).

- 4. Affirmative Action:** Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.
- 5. Easily Withdrawn:** Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.
- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

What is “Consent”?

The definition of consent typically involves the following key elements:

- 1. Voluntary Agreement:** Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.
- 2. Informed:** Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is

3. Specific and Granular: Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).

button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.

- 5. Easily Withdrawn:** Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.
- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

What is “Consent”?

The 5 Rights of My Identity™

RIGHT CONSENT

The definition of consent typically involves the following key elements:

- 1. Voluntary Agreement:** Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.
- 2. Informed:** Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is collected, and who the data will be shared with, among other relevant details.
- 3. Specific and Granular:** Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising

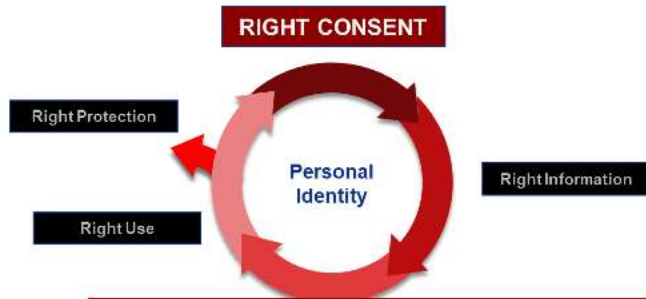
4. Affirmative Action: Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.

level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.

- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

What is “Consent”?

The 5 Rights of My Identity™



The definition of consent typically involves the following key elements:

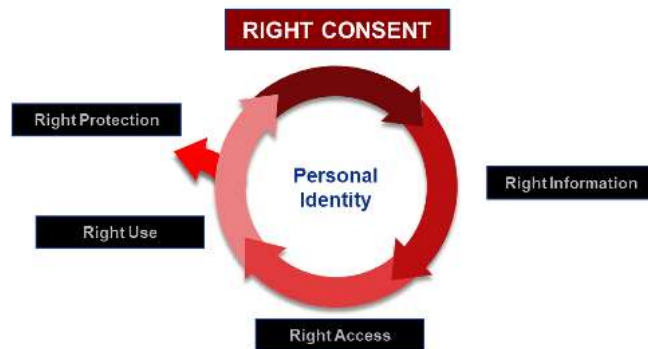
- 1. Voluntary Agreement:** Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.
- 2. Informed:** Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is collected, and who the data will be shared with, among other relevant details.
- 3. Specific and Granular:** Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).
- 4. Affirmative Action:** Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or

5. Easily Withdrawn: Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to change their cookie preferences and opt out of data collection.

- 6. Child Consent:** In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

What is “Consent”?

The 5 Rights of My Identity™



The definition of consent typically involves the following key elements:

- 1. Voluntary Agreement:** Consent must be freely given, meaning that users should not be subjected to undue pressure, manipulation, or negative consequences if they choose not to provide consent. Users should have a genuine choice in whether or not to allow the use of cookies.
- 2. Informed:** Users must be informed about what they are consenting to. This means they should receive clear and transparent information about the types of cookies being used, the purposes for which data is collected, and who the data will be shared with, among other relevant details.
- 3. Specific and Granular:** Consent should be specific to each purpose for which cookies are used. Websites should not bundle multiple purposes into a single consent request but should instead ask for separate consents for different types of cookies (e.g., necessary cookies, analytics cookies, advertising cookies).
- 4. Affirmative Action:** Consent must be given through an affirmative action, such as clicking an "Accept" button, toggling a switch, or actively selecting options in a cookie settings menu. Pre-ticked boxes or assumed consent (e.g., through the use of pre-checked checkboxes) are generally not considered valid forms of consent.
- 5. Easily Withdrawn:** Users should have the ability to withdraw their consent at any time with the same level of ease with which they gave it. This means that websites should provide users with clear options to

6. Child Consent: In many jurisdictions, obtaining consent from parents or guardians is required when collecting data from children below a certain age (e.g., 13 years in the United States).

6 Ways Your Identity Can Be Stolen



SOURCE: <https://www.youtube.com/watch?v=9ST5cMEXmDU>

The Ethics of Managing People's Data

by Michael Segalla and Dominique Rouziès

From the Magazine (July–August 2023)



SOURCE: <https://hbr.org/2023/07/the-ethics-of-managing-peoples-data>

Netflix published a data set that included 100 million records of its customers' movie ratings and offered \$1 million to any data scientist who could create a better movie-recommendation algorithm for the company.

The data contained no direct identifiers of its customers and included only a sample of each customer's ratings.

Researchers were able to identify 84% of the individuals by comparing their ratings and rating dates with a third-party data set published by IMDb, another platform on which many Netflix customers also post film ratings.



SOURCE: <https://hbr.org/2023/07/the-ethics-of-managing-peoples-data>



The year 2023 witnessed a groundbreaking [GDPR fine surpassing €1.2 billion to Meta](#) (formerly known as Facebook). Of the top 20 GDPR fines recorded, seven were imposed on Meta or Meta-owned companies.

Astonishingly, this single fine alone comes close to eclipsing the combined total of all GDPR fines issued by January 28, 2022, which was approximately €1.64 billion.

Collectively, **GDPR fines have now reached over €4 billion**. These figures demonstrate the ongoing commitment to upholding data protection regulations and highlight the increasing financial consequences of non-compliance.

SOURCE: <https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/>

20 biggest GDPR fines so far [2023]

19/09/2023 in Blog, GDPR



What are the “Personal Identity Threats” to Consumers of Consent to Cookies?

Consenting to cookies on websites can present certain privacy and security threats to consumers, depending on how the collected data is used and shared. It's essential for consumers to be aware of these potential risks when providing consent. Misuse may include examples such as gun ads to children. Here are some common threats associated with cookie consent:

1. Privacy Concerns:

- **Data Collection:** Cookies can track various aspects of a user's online behavior, such as browsing history, preferences, and interactions. This information can be used to create detailed user profiles, which may infringe on users' privacy.
- **User Profiling:** Companies can use the data collected through cookies to create detailed profiles of users, including their interests, demographics, and behaviors. This information can be used for targeted advertising and marketing.

2. Data Sharing and Sale:

- **Third-Party Data Sharing:** Many websites allow third-party cookies, which can lead to data being shared with advertising and analytics companies without the user's full awareness or control.
- **Data Brokerage:** In some cases, the data collected through cookies may be sold or shared with data brokers, who aggregate and sell user data to other businesses, potentially leading to further privacy concerns.

3. Security Risks:

- **Data Breaches:** If a website or the third parties it works with experience a data breach, the information collected through cookies may be exposed to unauthorized individuals, leading to identity theft and other security risks.
- **Cross-Site Scripting (XSS):** Malicious actors can use certain types of cookies, like session cookies, to execute cross-site scripting attacks, which can compromise the security of a user's account and personal information.

4. Tracking and Profiling:

- **Invasive Tracking:** Some cookies are designed for tracking users across websites, creating a comprehensive profile of their online activities. This level of tracking can feel invasive and raise concerns about user autonomy.
- **Filter Bubbles:** Personalized content based on user data can lead to filter bubbles, where users are exposed primarily to information and viewpoints that align with their existing beliefs, potentially limiting their exposure to diverse perspectives.

5. User Consent and Transparency:

- **Lack of Transparency:** Some websites may not provide clear and transparent information about their data collection and use practices, making it challenging for users to give informed consent.
- **Cookie Banner Overload:** Users may encounter numerous cookie consent banners on websites, which can lead to consent fatigue, causing them to accept without fully understanding the implications.

To Mitigate These Threats, Consumers Should:

- Be cautious about the websites they visit and the types of cookies they consent to.
- Review and manage their cookie settings, typically accessible through a website's privacy or cookie policy.
- Use browser privacy features, such as ad blockers and cookie blockers, to control cookie behavior.
- Educate themselves about privacy rights and data protection laws in their region, such as the GDPR in Europe and the CCPA in California.
- Consider using privacy-focused browsers or browser extensions that enhance privacy protection.
- Ultimately, informed consent and active management of cookie preferences are key to safeguarding one's privacy and security while browsing the web.

What are the NEW RISKS Advertisers bear from Consumer Data Use Consent And Preferences?

The GDPR in the European Union and the CCPA in California have introduced several new risks and challenges for advertisers when it comes to collecting and using consumer data. **These regulations prioritize consumer privacy rights and impose strict requirements on how businesses handle personal data.** Here are some of the new risks and challenges face:

1. Consent Requirements:

- **Risk:** Advertisers must obtain clear and specific consent from users before processing their personal data for advertising purposes. This can be challenging as users have the right to opt out or withdraw consent at any time.
- **Challenge:** Advertisers need to develop user-friendly consent mechanisms and maintain records of consents. They also need to ensure that third-party partners they work with are compliant with consent requirements.

2. Data Minimization:

- **Risk:** Advertisers must limit the collection and use of personal data to what is necessary for specific purposes. Collecting excessive data can lead to non-compliance.
- **Challenge:** Advertisers need to review and refine their data collection practices to ensure they are only collecting data that is strictly required for their advertising campaigns.

3. Data Transparency:

- **Risk:** GDPR and CCPA require advertisers to provide clear and concise information about data processing practices to users, including how data is used for ad targeting.
- **Challenge:** Advertisers need to update their privacy policies and disclosure practices to meet transparency requirements. They should communicate data usage in a language that is easily understandable to the average consumer.

4. User Rights:

- **Risk:** Both regulations grant users rights over their personal data, including the right to access, rectify, delete, or port their data. Advertisers must be prepared to respond to user requests promptly.
- **Challenge:** Advertisers need to establish processes and systems for handling user requests and ensuring compliance with these rights. This can be resource-intensive.

5. Data Security:

- **Risk:** GDPR and CCPA require businesses to implement appropriate security measures to protect user data. Data breaches can result in severe fines and reputational damage.
- **Challenge:** Advertisers need to invest in robust cybersecurity practices and regularly assess and update their security measures to safeguard consumer data.

6. Third-Party Partners:

- **Risk:** Advertisers are responsible for the actions of third-party partners, such as ad networks and data providers, they work with. Non-compliant third parties can lead to regulatory scrutiny.
- **Challenge:** Advertisers must vet and monitor their third-party partners to ensure they comply with GDPR and CCPA requirements. Contracts with third parties should include data protection clauses.

7. International Data Transfers:

- **Risk:** GDPR restricts the transfer of personal data outside the European Economic Area (EEA) unless specific safeguards are in place. CCPA also has provisions related to international data transfers.
- **Challenge:** Advertisers operating internationally need to assess their data transfer practices and implement mechanisms such as Standard Contractual Clauses (SCCs) to ensure compliance with GDPR.

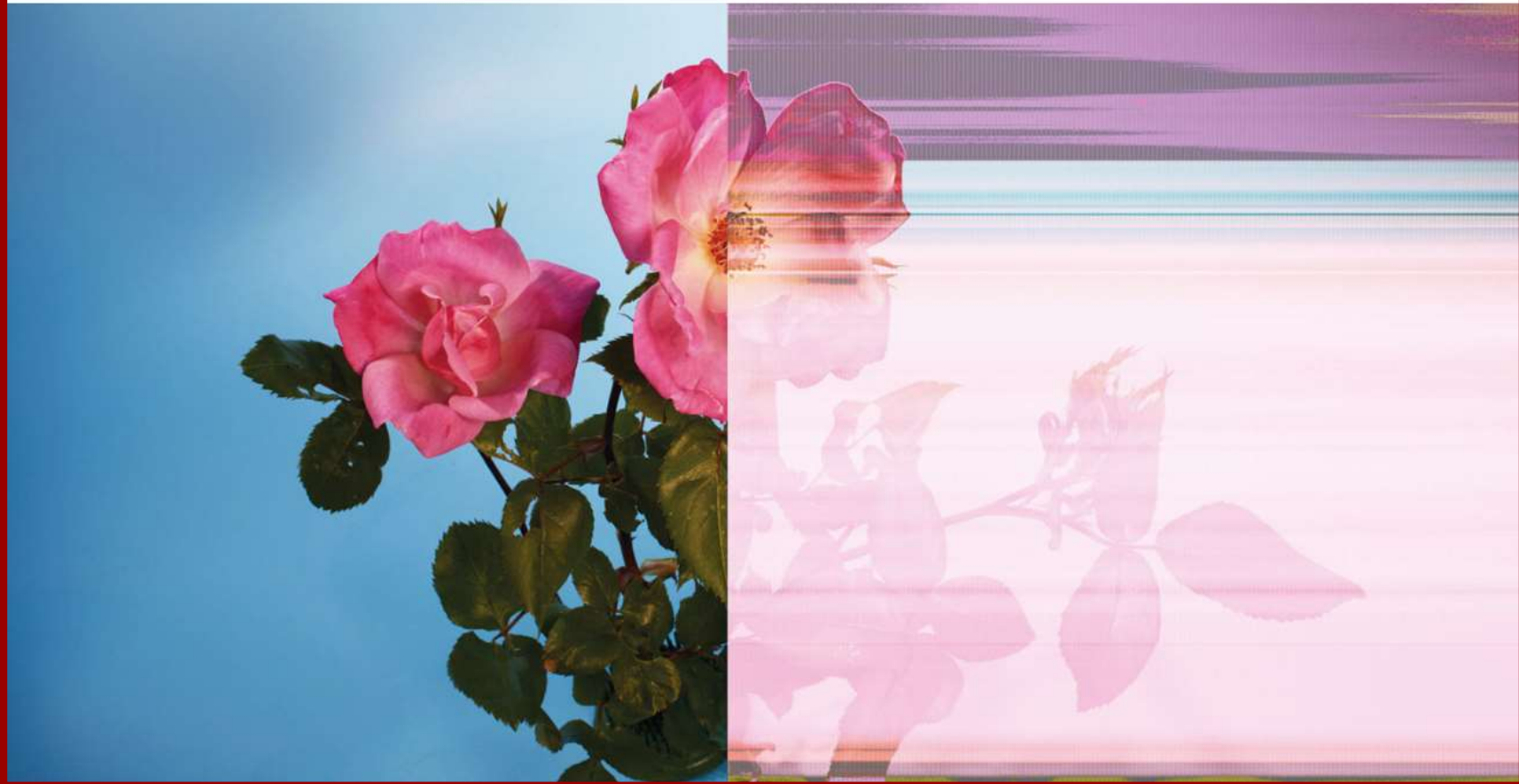
8. Fines and Penalties:

- **Risk:** Both GDPR and CCPA have the authority to impose significant fines and penalties for non-compliance, which can be financially burdensome for advertisers.
- **Challenge:** Advertisers need to allocate resources for compliance efforts and be prepared to respond to regulatory investigations or enforcement actions.

Why You Need an AI Ethics Committee

by Reid Blackman

From the Magazine (July–August 2022)



SOURCE: <https://hbr.org/2022/07/why-you-need-an-ai-ethics-committee>



Key Patient Safety Issues



Gregory H. Botz, MD, FCCM

**Professor of Anesthesiology and Critical Care
UT MD Anderson Cancer Center, Houston, TX
Adjunct Clinical Professor, Department of
Anesthesiology
Stanford University School of Medicine,
Stanford, CA**



**Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine**

“TRANQ is a street name for a drug Xylazine. Xylazine is a sedative agent that's been used in veterinary practice for some time. But even though it underwent testing, it has never been approved for use in humans.”



**Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine**

“But now our friendly drug dealers have figured out that by adding that to drugs like fentanyl, they can get a different or a better high.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“The spread of fentanyl in our community has continued and perhaps accelerated despite things like the COVID pandemic and other issues that are on the front page of the news.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“There's a huge market for counterfeit pills especially coming from Mexico.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“In 2022, the Drug Enforcement Administration seized 15 million counterfeit pills over the year from a variety of sources.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“In 2022, the Drug Enforcement Administration seized 15 million counterfeit pills over the year from a variety of sources. And when tested about 60 % of those counterfeit pills had a lethal dose of fentanyl incorporated into that pill.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“Narcan or the generic name, Naloxone, is a drug that reverses opiates. And Fentanyl, and Morphine, Oxycodone are opiate drugs. That's the only thing that Narcan does. It doesn't have any other effects on the body. So, if you give it to someone, and they don't have opiates in their system, it won't cause them any harm.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“But now there's a threat to a medical record, and people can take over our identity, or create a new identity with your aggregated information that they gather over the internet, to exploit your medical record to get medical services, either to obtain services to get prescriptions for narcotic, or get curable medical equipment that can be resold.”



**Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine**

“To get that false information or that false activity off your medical record is extraordinarily difficult to do.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“Having an accurate version of your medical record including your medical problems, your allergies, your medications, and other things that are particular to you, available to first responders allows them to better understand you and make better choices about your treatment.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“We have found that there is a gap in care between the time of the medical emergency and the response of the first responders. And in that gap, we can train bystanders to provide life-saving care and provide it until first responders get there.”



Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine

“And we have lots of data showing that in people with sudden cardiac arrest, doing CPR is the best instrument until first responders can get there.”



**Gregory H. Botz, MD, FCCM
UT MD Anderson Cancer Center
Stanford University School of Medicine**

“I think we recognize that providing care to our community members makes them safe. And my focus, and I know your focus in patient safety has always been on providing safe care to our patients.”

Workplace Violence & Fraud Series 2023 Speakers and Reactors



Jennifer Dingman



David Morris PhD JD



Vicki King



John Nance JD



Randy Styner



Ann Rhoades



C. Clements MD PhD



Chief William Adcox



Gregory Botz MD



Charles Denham MD

Voice of Patient and Family



Jennifer Dingman

Founder, Persons United Limiting
Substandard and Errors in Healthcare
(PULSE), Colorado Division
Co-founder, PULSE American Division
TMIT Patient Advocate Team Member
Pueblo, CO

Fight the Good Fight...

Finish the Race...

Keep the Faith...

Everyone is a Patient

and

Everyone CAN BE a Caregiver



ADDITIONAL RESOURCES



INFORMATION
DISORDER
MACHINES

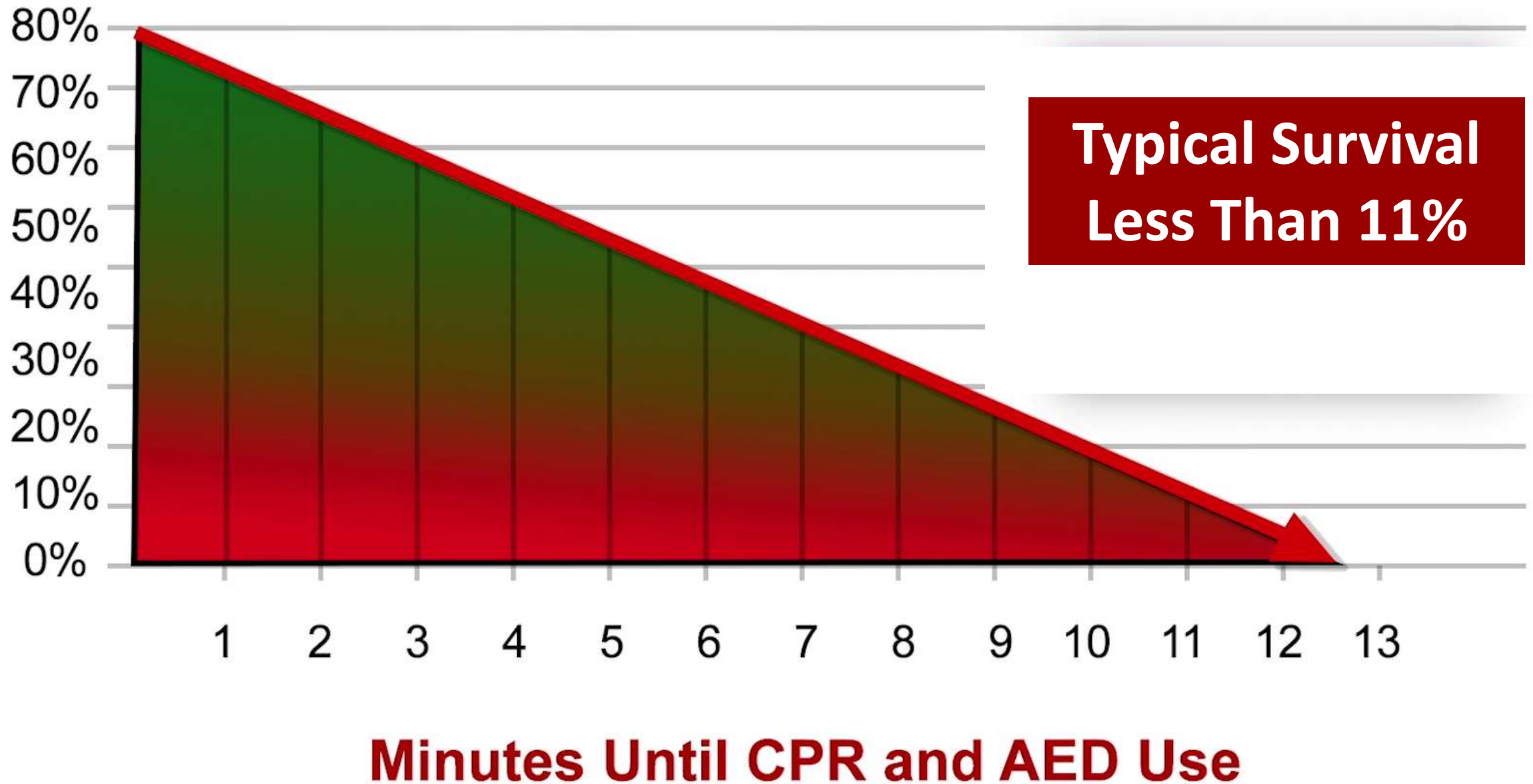


False Narratives & Weaponizing Information

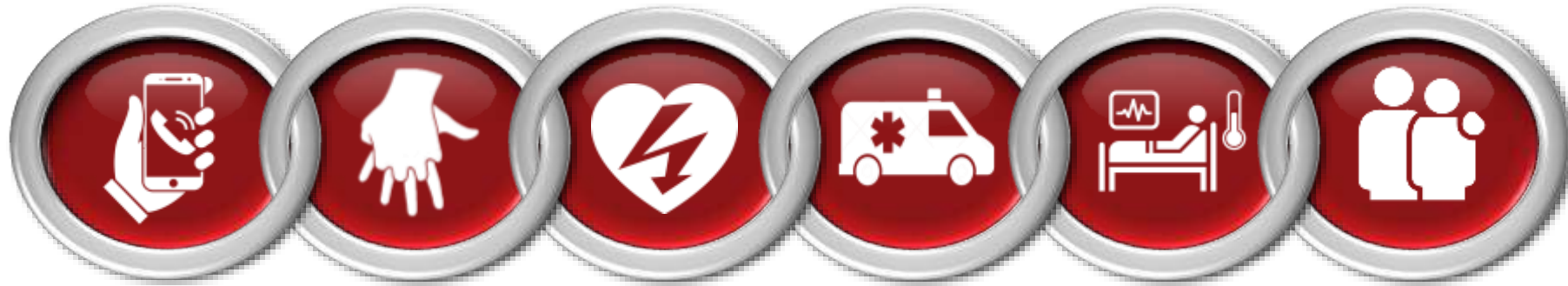
- **Mis-information:** when false information is shared, but no harm is meant.
- **Dis-information:** when false information is knowingly shared to cause harm.
- **Mal-information:** when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.

Source: Claire Wardle and Hossein Derakhshan “Information Disorder”

Survival Loss Over Time for Sudden Cardiac Arrest



Cardiac Arrest Chain of Survival



Recognition and
Activation of Emergency
Response System

Immediate High-
Quality CPR

Rapid
Defibrillation

Basic & Advanced
Emergency
Medical Services

Advanced Life Support
& Post-arrest Care

Recovery

Bystander Care



3 Minutes from Drop to Shock

Trauma Chain of Survival



Bystander Care



3 Minutes from Gun Shot to Stop the Bleed

Freshmen Survive & Thrive™ Checklists

High School Freshmen:

Basic Actions:

- ❑ Phone 911 – Automatically call ICE Parents
- ❑ Know Local Hospitals – Level 1 Trauma Centers
- ❑ Review Family FEMA Checklist for Disasters

Sudden Cardiac Arrest:

- ❑ Consider Cardiac Screening – EKG & Ultrasound
- ❑ Get CPR-AED Certified

Choking & Drowning

- ❑ Learn Heimlich Maneuver & Rescue Position

Life Threatening Allergies

- ❑ Venom, Meds, Food Allergies and Epinephrine Auto-injectors

Opioids and Poisoning

- ❑ Counterfeit Pills, Fentanyl, THC, and Nicotine Poisoning
- ❑ Vaping Dangers
- ❑ Narcan and Rescue Skills

Major Trauma

- ❑ Stop the Bleed Training
- ❑ Understanding Concussions

Infections

- ❑ Clean a Cut Save a Life
- ❑ COVID, Flu, and Pandemics

Transportation Accidents

- ❑ Non-traffic Drive-over Accidents
- ❑ Traffic Accidents, Risk Taking, and Substance Impairment

Bullying & Suicide

- ❑ Physical, Emotional, and Cyber-bullying
- ❑ Suicide Risk and Rescue

College Freshmen:

Basic Actions:

- ❑ Medical Power of Attorney – college, home, and recreation US States
- ❑ Phone 911 – Automatically call ICE – Parents or Another Adult
- ❑ Know Local Hospitals – Level 1 Trauma Centers near College

Sudden Cardiac Arrest:

- ❑ Consider Cardiac Screening – EKG & Ultrasound
- ❑ Get CPR-AED Certified

Choking & Drowning

- ❑ Learn Heimlich Maneuver & Rescue Position

Life Threatening Allergies

- ❑ Venom, Meds, Food Allergies and Epinephrine Auto-injectors

Opioids and Poisoning

- ❑ Counterfeit Pills, Fentanyl, THC, and Nicotine Poisoning
- ❑ Vaping Dangers
- ❑ Narcan and Rescue Skills

Major Trauma

- ❑ Stop the Bleed Training
- ❑ Understanding Concussions

Infections

- ❑ Clean a Cut Save a Life
- ❑ COVID, Flu, and Pandemics

Transportation Accidents

- ❑ Non-traffic Drive-over Accidents
- ❑ Traffic Accidents, Risk Taking, and Substance Impairment

Bullying & Suicide

- ❑ Physical, Emotional, and Cyber-bullying
- ❑ Suicide Risk and Rescue



High School Freshmen:

Basic Actions:

- ❑ Phone 911 – Automatically call ICE Parents
- ❑ Know Local Hospitals – Level 1 Trauma Centers
- ❑ Review Family FEMA Checklist for Disasters

Sudden Cardiac Arrest:

- ❑ Consider Cardiac Screening – EKG & Ultrasound
- ❑ Get CPR-AED Certified

Choking & Drowning

- ❑ Learn Heimlich Maneuver & Rescue Position

Life Threatening Allergies

- ❑ Venom, Meds, Food Allergies and Epinephrine Auto-injectors

Opioids and Poisoning

- ❑ Counterfeit Pills, Fentanyl, THC, and Nicotine Poisoning
- ❑ Vaping Dangers
- ❑ Narcan and Rescue Skills

Major Trauma

- ❑ Stop the Bleed Training
- ❑ Understanding Concussions

Infections

- ❑ Clean a Cut Save a Life
- ❑ COVID, Flu, and Pandemics

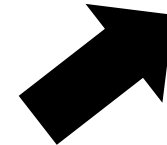
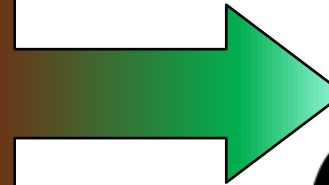
Transportation Accidents

- ❑ Non-traffic Drive-over Accidents
- ❑ Traffic Accidents, Risk Taking, and Substance Impairment

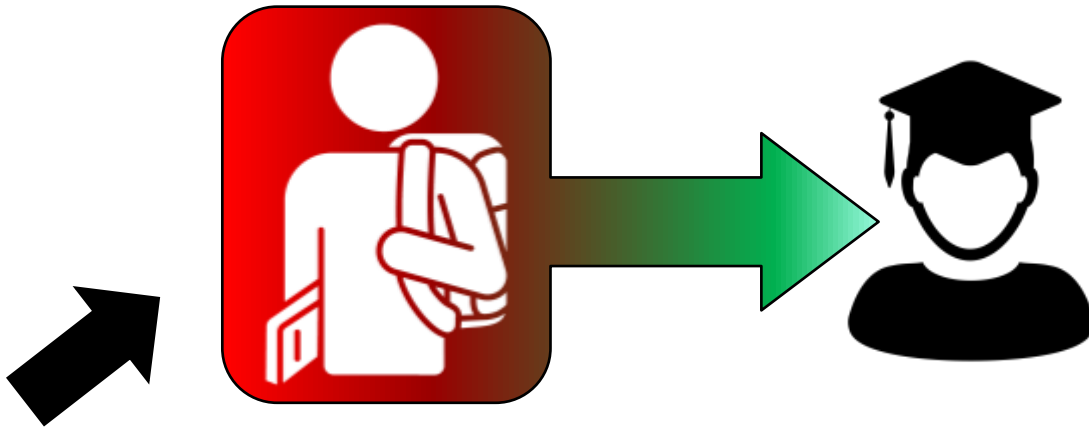
Bullying & Suicide

- ❑ Physical, Emotional, and Cyber-bullying
- ❑ Suicide Risk and Rescue

High School Freshmen



College Freshmen



College Freshmen:

Basic Actions:

- ❑ Medical Power of Attorney – college, home, and recreation US States
- ❑ Phone 911 – Automatically call ICE – Parents or Another Adult
- ❑ Know Local Hospitals – Level 1 Trauma Centers near College

Sudden Cardiac Arrest:

- ❑ Consider Cardiac Screening – EKG & Ultrasound
- ❑ Get CPR-AED Certified

Choking & Drowning

- ❑ Learn Heimlich Maneuver & Rescue Position

Life Threatening Allergies

- ❑ Venom, Meds, Food Allergies and Epinephrine Auto-injectors

Opioids and Poisoning

- ❑ Counterfeit Pills, Fentanyl, THC, and Nicotine Poisoning
- ❑ Vaping Dangers
- ❑ Narcan and Rescue Skills

Major Trauma

- ❑ Stop the Bleed Training
- ❑ Understanding Concussions

Infections

- ❑ Clean a Cut Save a Life
- ❑ COVID, Flu, and Pandemics

Transportation Accidents

- ❑ Non-traffic Drive-over Accidents
- ❑ Traffic Accidents, Risk Taking, and Substance Impairment

Bullying & Suicide

- ❑ Physical, Emotional, and Cyber-bullying
- ❑ Suicide Risk and Rescue