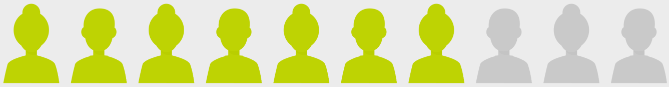
DATA PROTECTION

SHARING DATA RESPONSIBLY

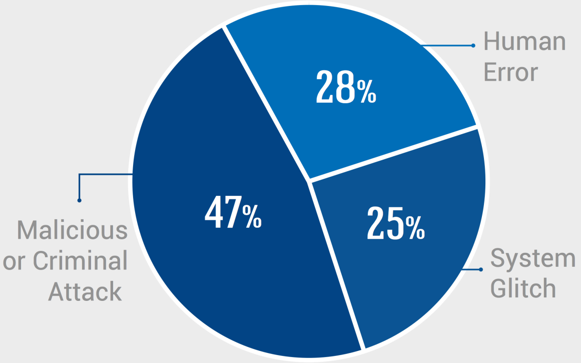
Sharing sensitive information requires a robust privacy infrastructure. How does your organization stack up?

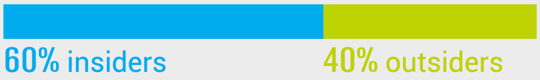
TRADITIONAL ENCRYPTION, ACCESS CONTROLS AND FIREWALLS ARE INSUFFICIENT



70% of employees have access to data they shouldn't

Breaches come from all sides





Breaches are hard to detect and contain

214 Days to identify

77 Days to contain

45% of organizations have had at least 1 breach in the past year

28% probability of another breach in the next 24 months.

Breaches are expensive with lasting impact on brands and careers

$7.35 Million avg cost of a data breach

PRIVACY AND SECURITY HAVE TO COOPERATE TO REDUCE THE RISK OF A BREACH

SECURITY

Keeps unauthorized users out

AND ~~VERSUS~~

PRIVACY

Shares data responsibly

Many regulations and best practices

GDPR	ISO 29100
HIPAA	FIPPA
NIST	PCI
Safe Harbor	COPPA
PIPEDA	FACTA
HITRUST	CASL

Masking Direct De-Identification

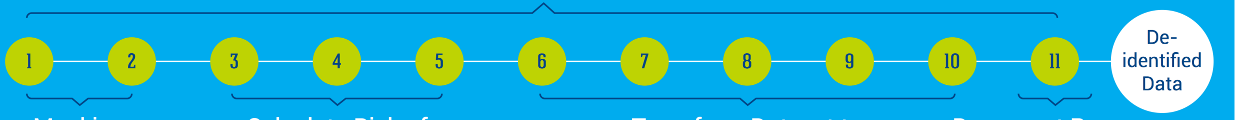
NAME	****
ADDRESS	****
DATE OF BIRTH	MM/DD/YY

Safe Harbor de-identification removes 18 direct identifiers

Risk-Based De-Identification

Attack vector leaves **25 OUT OF 10,000 PEOPLE** exposed to re-identification

11-STEP DE-IDENTIFICATION PROCESS



Masking Direct Identifiers

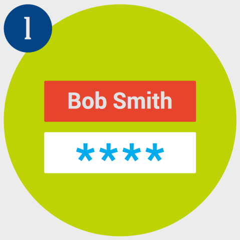
Calculate Risk of Re-Identification

Transform Dataset to Meet Risk Threshold

Document Process and Results

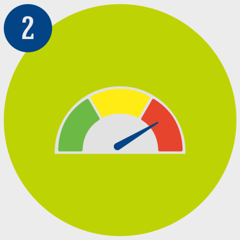
RISK-BASED DE-IDENTIFICATION

5 COMPONENTS
OF A TRUSTED DATA-SHARING INFRASTRUCTURE



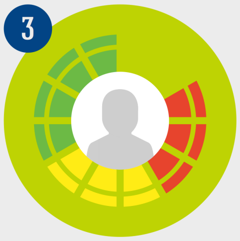
Mask Direct Identifiers with Dynamic Privacy Controls

Real-time access to identified or masked data based on policy-driven user authentication.



Apply Risk-Based De-Identification with Persistent Access Controls

Build de-identified datasets where the risk of re-identification is calculated and data is transformed to meet risk threshold.



Enforce Zones of Trust to Control Data Proliferation

Ensure sensitive data doesn't leak to uncontrolled environments such as portable devices.

Generate Detailed Compliance Reports to Track Sensitive Assets

Document de-identification process and inventory data proliferation including right to be forgotten and personal information retention.

Maintain Fine-Grained Audit Logs to Identify Unauthorized Access

Log user activity and access to sensitive data, alerting anomalous patterns.

www.phemi.com | info@phemi.com | www.twitter.com/PHEMIsystems | www.linkedin.com/company/phemi

PHEMI