HR Process for Handling Sensitive Data

In HR we have access to Personal Identity Information (PII) and often get requests for ad hoc reports or queries with PII

Personal Identity Information includes:

- Birth Date
- Home Address
- Social Security
- Bank account numbers
- Passport information
- Healthcare related information
- Medical insurance information
- Driver's license and State ID information

Other sensitive data:

- Gender
- Race/Ethnicity
- Disability
- Veteran Status
- Performance Review
- Pay/Compensation

In order to manage the release of PII and other confidential data with the greatest of discretion and integrity, follow this process:

1. The business case for the request must be established. This should be handled by personal contact via in person or phone. If that is not possible then a new email requesting the business case should be sent to the requestor with Director of HR Technology and CLO in copy.

2. Approval for the business case and release of PII must be given by: CLO

3. File should be password protected and zipped.

    - If it is an internal request, place password protected file in secure folder on the shared drive temporarily.

    - If this is an external request, information should be sent via SFTP with key

4. Password to the protected file should be delivered by separate communication.

5. Where possible use summary-level data vs. detailed – row level data

6. **REMEMBER**: The safest place for sensitive data is in the system

5455 E. High St., Suite 111 • Phoenix, AZ 85054 • 480-814-8016 • Fax 480-814-8017