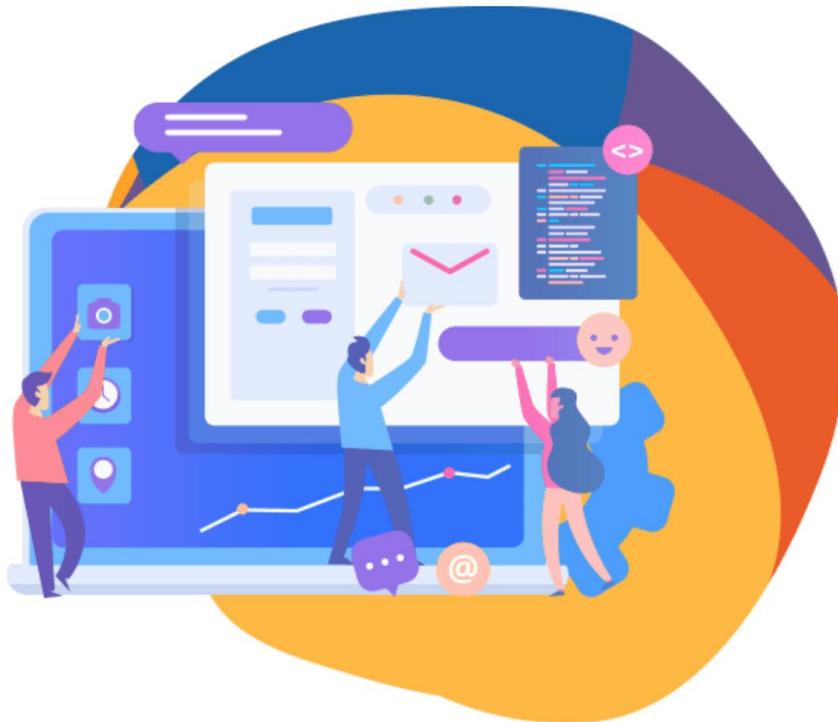




# HR should have a data strategy



**Playbook to help the nontechnical HR executive create strategic value through an effective HR Data Strategy**

## **Contributors:**

Sunil Vatave - CEO , Canopy Workforce Solutions, Atlanta, USA.

Jake Terry - CTO , Canopy Workforce Solutions, Atlanta, USA.

Vikas Pandey - CTO , DevopsInternational, Amsterdam, NL.

March, 2021

In 2015 the Harvard Business Review printed on its front page an article entitled “It’s Time to Blow Up HR and Build Something New.” Since then there have been various articles all talking about the need for a new kind of HR. What is all this talk about?

It’s about **digital transformation** of the HR function. Another way you may have heard this is “HR needs to be data driven”. For those who’ve been in HR some time, the importance of data will come as no surprise. HR has **always** been data driven. The problem is not that the function doesn’t recognize the need for data. The problem is that HR data has always been hard to get.



“HR leaders are in the unique position of being able to lead the business conversation on how the world of work is taking shape in the 21st century. But you cannot occupy that space with other business leaders without a deep comprehension of the technology involved,” says Susan Ferrier, Global Head of People for KPMG. She states that the positive business impact of digital transformation is magnified with a strong, digitally savvy and influential HR function.

**Susan Ferrier, Global Head of People for KPMG**

For this to change, you, the HR professional, need to be empowered with technology. No, you don’t have to become an IT person. However, you can’t have data driven HR if you don’t have data. What you need is a way to collect, organize, protect and share data in a way which adds value to your business. In short, you need data strategy. This post will attempt to simplify the concepts into a form you can use to create an effective HR Data Strategy for your company.

We will first define what is a data strategy. Next we’ll talk about the strategic considerations which will pull your data strategy in one direction or another. We will then outline 5 steps that will give you some technical terms but in a practical way that can be used to make a plan for your HR data. Finally we will leave you with a check list of recommendations and

terms for you to incorporate into your consideration of your own HR Data Strategy.

By the end of this post you should be able to effectively communicate as a business professional with your technical teams about the issues that impact your HR function and how data can solve them. This is a long post, but at this time in the transformation of HR we feel it is needed. If you have questions or comments feel free to send them to us, and we'll try to help you as best we can.

## What is a Data Strategy?

At a high level, a data strategy is simply how you will collect and use data to help your company achieve its goals. For most departments this is a straightforward analysis of what data can be collected and analyzed to provide insights for operational improvement. However, in HR a data strategy is more complex.

HR has dual, sometimes conflicting, strategic imperatives. First, HR is concerned with the collection and use of data just like any other department, but there is a second and sometimes more challenging aspect. That is data governance. How is HR going to manage the privacy and other regulatory concerns imposed by factors external to the company.

Our definition of HR Data Strategy takes into account both the need for business information and the obligations to comply with various legal frameworks.

***An HR Data strategy is a set of decisions around policies, technology and processes which governs the collection, use and maintenance of data to support business goals within the context of the applicable legal framework in which the company operates.***

# Groundwork for building HR Strategy

We have a definition of HR Data Strategy that will guide us in making a plan. However, before getting to the steps it is also useful to understand two concepts. These are data *Control* and data *Analysis*. Analysis in some scholarly articles is referred to as Flexibility, but we think Analysis is a better concept when applied to HR. We will prescribe specific meanings to these terms because it will help you better analyze the specific HR data elements and how they should be managed.

## The Elements of Data Strategy

	DEFENSE	OFFENSE
KEY OBJECTIVES	Ensure data security, privacy, integrity, quality, regulatory compliance, and governance	Improve competitive position and profitability
CORE ACTIVITIES	Optimize data extraction, standardization, storage, and access	Optimize data analytics, modeling, visualization, transformation, and enrichment
DATA-MANAGEMENT ORIENTATION	Control	Flexibility
ENABLING ARCHITECTURE	SSOT (Single source of truth)	MVOTs (Multiple versions of the truth)

“What’s your data strategy”, Leandro Dallemule and Thomas Davenport, *Harvard Business Review*, 2017

# Difference between Control and Analysis

Control of data refers to processes and technology that ensure the accuracy, integrity and security of data. Accuracy means that the data is correct at a given point in time. Integrity means the data has not been changed; it is trustworthy. Security means that only those within the parameters of a given legal and policy framework can access the data.

In HR, we know that control requires an analysis of individual data items because we also know certain pieces of data have bigger control implications than others. For example, Social Security Number would be at the high end of the control spectrum whereas job title would not be subject to as much control. How you make these distinctions is critical to your HR data strategy.

Analysis refers to the use of data. Use initially involves viewing of data in a report or other format, but it goes further. Embedded within the notion of use of data are three questions.

- Can this data be used at all?
- If so, who can use it?
- For a user otherwise authorized to use data, to what extent and for what purpose can it be used?

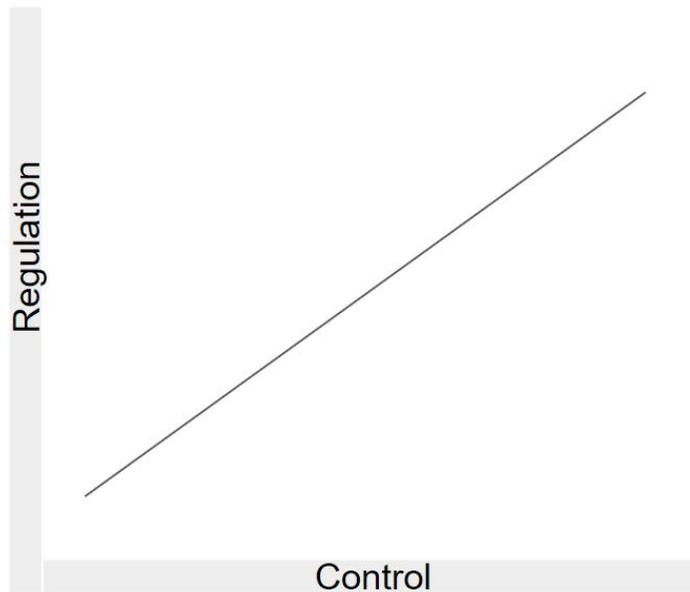
In HR, the simple word “use” can raise complicated issues. Some data we can collect, such as a person’s age, but we are not allowed to use that data to make employment decisions? Other data, such as prior salary in some states, cannot even be used. A second layer of complexity is introduced by who may use data. A complaint of sexual harassment is a data point, but even in the case of HR personnel not everyone should see every detail. Defining what data can be used, how it can be used and who can use it will be important components of your HR data strategy.

## *Define the What, Who and How*

Control and Analysis can often work in opposite directions. Analysis of data at the extreme would favor unlimited access to all data. Control, at a similar but opposing extreme, would lock down data to the smallest subset of users possible. Somewhere in the middle is where most companies find themselves. Where your company lands in the spectrum is what we'll discuss next.

## **How to choose between Control and Analysis**

Now that you know a bit more about Control and Analysis, how do you determine how much of each is appropriate for your company? The natural reaction of most in HR is to control everything - lock it all down. However, taking this approach can put you out of alignment with the business leaders. Instead, take a more nuanced approach by evaluating the regulatory environment in which you operate. You will have data that must be tightly controlled because of regulation, but you will also have data that if you can make it available to the business users will elevate the strategic importance of the HR function.



In highly regulated contexts such as hospitals, local governments, and law enforcement control will outweigh analysis. License your records which may be in multiple locations must have one reliable source that can be relied on when for example scheduling a nurse on a floor. You have to be sure that you can show disciplinary records were never unaltered. Similarly sensitive information such as police officer addresses need to be kept strictly confidential. In these situations the need for accuracy of data, integrity of data and maintenance of confidentiality are paramount.

Employment data will always have some level of control because by definition employment is regulated by laws. However, there are cases where the legal ramifications are not so big, and HR can add a lot of business value by becoming a source of useful information to the business units.

What might such data look like? Time worked data is one example. Attendance data is another one. Prevailing wage data where there are Davis-Bacon requirements is yet another. The point is where there is not

an overriding regulatory concern, HR's Data Strategy should consider what data might be useful to share with those outside of the HR department.

Now it's time to map out a strategy

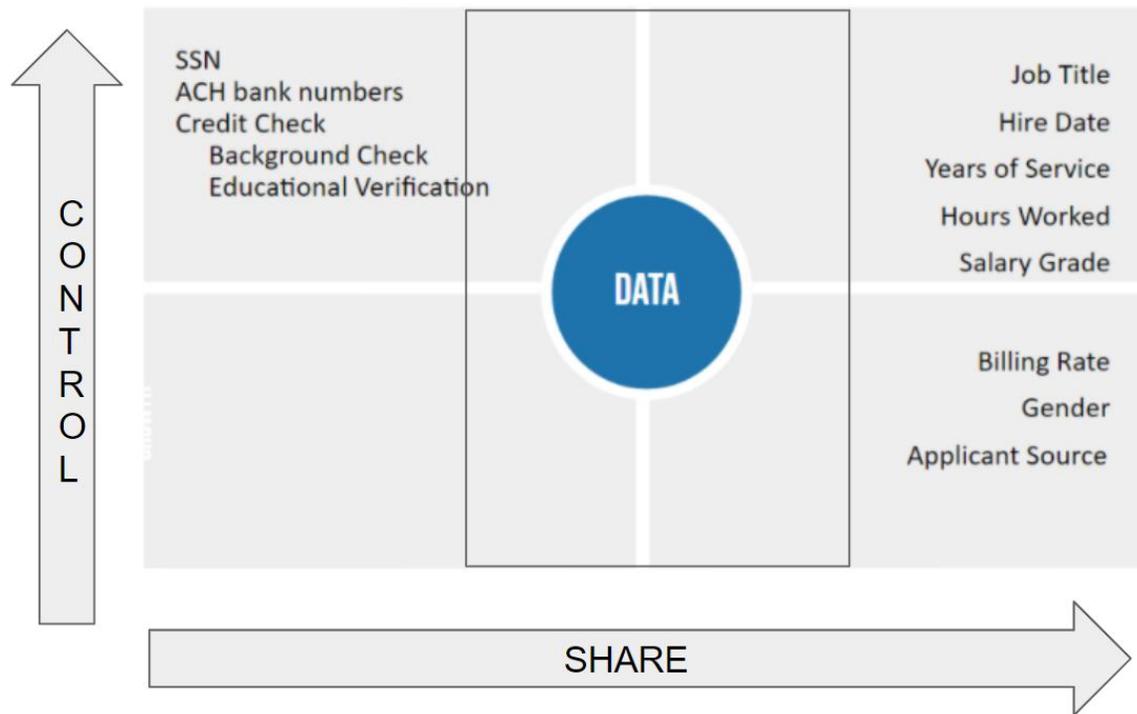
## **5 STEPS TO BUILD HR DATA STRATEGY**

### **Step 1**

**Classify the data over which you are responsible as either Control, Analysis or something in the middle.**

There are three types of data. Data which should never be shared, e.g. individual credit check information. Data which can almost always be shared, e.g. Job Title. Data which might be OK to share if you do it carefully, e.g. age. In order to figure out the later parts of the strategy which deals with how data should be controlled and analyzed, you first need to put the data into one of these three buckets.

We recommend going to a field level. Identify the fields you have and in some manner categorize them by those which you need to exercise a lot of control and those which are less sensitive and can be used by you or others for analysis. In doing this exercise you will find some data points which are useful for analysis but have control concerns. We call these the "use carefully" fields and we'll discuss those in a bit.



Fields in the upper left quadrant contain highly sensitive information. This data needs to be strictly controlled. Your strategy needs to contain plans to legally collect, safeguard, retain and remove this information.

*“Pay close attention to retention policies”*

Retention and removal are two topics that must be addressed in HR’s data strategy. The EEOC regulation requiring records of a terminated employee be kept one year from termination is a good example of how these issues come into play. Holding data unnecessarily has a cost. It also carries a potential liability if there is a data breach and someone gets access to the confidential information of a former employee. We’ll discuss retention and removal policies in more detail in another post.

Fields on the right hand side can usually be shared, at least within the company, with little problem. This data can have a lot of value to other departments. A common example of this is the turn over report which lets

management know how well they are doing at retaining talent. If you add additional data to a traditional turnover report such as turnover by seniority or turnover by termination reason, you can start to provide a lot of useful information. For example, if you see in one office you have 15% turnover and 75% of the reason for termination of employment is voluntary and 80% of that is because of the work environment, you know that something is going on with the workplace that is causing employees to leave.

That gets us to all the data in the middle of our diagram. That is data which can be useful but has to be shared carefully. Here you have information about a person which when used in the aggregate could be useful, but it comes with individual privacy concerns. A person's age or medical condition are good examples. Here you have to think about **Data Minimization** which means presentation of statistical information which does not involve personally identifiable information and can, therefore, not be traced back to a given individual. Another tactic that can be used if your HR strategy involves sharing information which involves individual privacy concerns is **Data Obfuscation**. Here you share data with others but the content is modified so that you can't know who the data belongs to. For example, John Smith may be changed to George Jones.

Once you have categorized the information under your control, the next two steps deal with how best to use it.

### **Step 1 Summary - Key Questions**

1. What data HR data should be strictly controlled?
2. What HR data can be shared with little risk?
3. What potential private data can be aggregated and shared using Data Minimization or Data Obfuscation to protect individual privacy rights.

## Step 2

### Define the big business goals.

*HR's most useful asset is employee data*

First, let's be real about this. HR is not responsible for defining business goals. Our job in HR is to support the strategy. Before you can build your HR Data strategy you need to get from the business leaders the business goals. As a strategic player, they will be happy if you come to them and say "look in HR we have a lot of data. I want to see how that can help you achieve your business goals, but first I need you to define for me those goals."

While business goals can be almost anything, they usually distill to one of two things. Goals designed to support revenue or goals designed to manage costs. It is a useful exercise to create a matrix to analyze the business goals in terms of what HR has within its power to influence

Business Goal	Type	What can HR do to positively impact the business goal?	What data does HR have to support its efforts?
Achieve 18% operating margin	Cost	Reduce recruiting cost	Recruiting source. Turn over report. Recruiting cost.
Achieve 18% operating margin	Cost	Reduce safety claims with more training	OSHA reports Training logs Incidents trends
Achieve 90% customer retention	Revenue	Improve Customer Service Performance	Performance reviews Attendance records Termination record

## **Step 2 Summary - Key Questions**

1. What are the business goals
2. Which of those goals support Cost and which support Revenue
3. What data does HR have to support each of those goals?

## **Step 3**

### **Define how data will be used.**

Key Technical Concepts: Identify and Access Management (“IDAM”)

By this point you know what data you have, and you know how you think that data could support the business goals. So let’s go back to our categorization in step 1 and see how we will use our data. Here is where technical concepts are going to become important.

Data on the left side of the Control/Analysis matrix will generally only be used for compliance purposes. To accomplish this you will need to put in place a system or other controls to ensure that only those with authorized access can view or edit the data.

A special note on Perhal Health Information (“PHI”) and its cousin Personally Identifiable Information (“PII”). These two data types will require enhanced security measures. As part of your strategy you will need to decide whether you will maintain such information and if so, how you will comply laws designed to protect such data from unauthorized disclosure.

Remember as an HR executive we are trying to answer 3 questions about the “use” of data:

1. Can the data be used
2. If yes, then who can use it
3. For authorized users, how can they use it.

Again it's helpful to build a table to analyze the data issues. An example is below.

Data	SSN	Authorized Use
Can it be used	Yes	Not applicable
HR	Yes	Background check, payroll, benefits
Managers	No	Not Applicable
Employees	Yes	Limited to self
Payroll	Yes	Payroll processing
AP Admin	No	None

Your technology executives see the above as a question of Identity and Access Management ("IDAM"). So let's clarify IADM so you can be confident in your discussion.

A full discussion of IDAM as it relates to HR will be in a later post, but for today understand that the main thing you need to be concerned about is "authentication" and "authorization".

Authentication is the process of verifying the digital identity of a user. Username and password represent one such process. Two factor authentication using a phone number or email as a secondary method to validate a user is another authentication method. Another method is to have a centralized repository allowing Single Sign On ("SSO) from one system into multiple systems. When you are discussing authentication with your IT team, you want to make sure that users who come into the system, especially where the system contains data elements with high control concerns such as SSN or PHI, are whom they purport to be.

Authorization is concerned with making sure that a user only gets to see the data he/she is supposed to see. For HR this normally involves role based security where a user is given a specific role. However, if you are sharing data for analysis you need to make sure that those who receive the information are also authorized to receive it. This becomes a particularly big issue if you are exporting files, discussed below. In that case you may have people handling Excel or .CSV files who may not be otherwise authorized to view that information. This is a big problem with benefits files that contain a lot of private information. For this reason, your HR data strategy should minimize data exchanges that involve data landing outside of a control system.

### *Protecting data with a remote workforce*

A special consideration needs to be taken into consideration when a remote workforce is involved. This is especially the case if they will use their personal mobile devices, sometimes known as Bring Your Own Device (“BYOD”). If you have a manager and they can use their cell phone to access HR information how do you stop them from walking off with confidential data if they leave your company’s employ? Mobile Device Management (“MDM”) concerns itself with keeping your company data safe when it is used by a remote worker. There are products like Microsoft’s Intune which create a protected area to view company applications and data on a cell phone, The user cannot make a screen shot of information

shown within that area, and if the employment terminates so does the access to the protected area. With today’s changing workforce it is important to consider all the user devices like computers, cellphones, and tablets when you put together your HR data strategy.

### **Step 3 - Key Questions**

1. For each data item, can it be used?
2. If so, who can use it?
3. For each person who can use a specific piece of data, how can they use it?
4. What are my company's data endpoints, e.g. Laptop, cell phone, tablet, and how will we protect the company's data at each endpoint?

### **Step 4**

#### **Define Sources of Data**

Key Technical Concepts:

- Meta Data
- API
- IPAAS
- ETL

You need to create reports to analyze gender pay equity issues across the enterprise. You have the employee's current rate of pay, but the pay history is over in the accounting system. How are you going to get it? This is an example of a data source that needs to be addressed in your data strategy.

There are five primary sources of data.

1. Data HR captures directly from the employee, e.g. Job Application
2. Data HR creates for the employee, e.g. Performance Reviews
3. Meta Data
4. External sources within the enterprise, e.g. Finance Department
5. External sources outside the enterprise, e.g. Background checking company

Item 1 and 2 are straightforward. You will get and/or create employee information primarily through web and paper based forms. Your data strategy will consider what online and offline process you will use today and in the future. A common example is moving to electronic onboarding which eliminates the need for new hire paper based forms.

Item 3 is **Metadata**. You can think of metadata as being data about data. An easy way to envision data is your playlist. The songs on it are analogous to employment records. Metadata is the categorization of those. This includes simple categories like Rock, Disco and Jazz, but also more complex categorizations like “Most Popular” and “Similar to”. In the HR world, we didn’t used to deal a lot with Metadata because we mostly dealt with data put into fields. However, we now have documents, collaboration tools like Microsoft Teams and Slack, and CRM and Project management systems which allow for commenting and tags. All of these systems generate Metadata, so for example you could see which employees are contacted the most about a problem or what documents are tagged as PHI and required HIPAA compliant control rules. We’ll get into a complete discussion of Metadata in a later post, but for now just be aware of the concept and understand that Metadata can be a powerful source of information for your HR Data Strategy.

Items 4 and 5 in our list of data sources concern data you are going to get from somewhere else. Here we get into the subject of multiple software systems and how they connect. If you have standardized on like SAP or Oracle all of your external sources may be connected to you.

The more common situation is you as the HR person have to deal with multiple systems. These are called disparate systems. You also have to deal with inconsistent spreadsheet formats and even paper documents. What you should be doing in your strategy is defining how you will efficiently connect to the sources of data you need. To do that we need to spend some time discussing how you connect to different data sources.

There are 3 main ways to connect to disparate data sources:

1. Application Programming Interface (API)
2. Integration Platforms (iPAAS)
3. A good old file through Extract, Transform and Load. (ETL)

The technical merits of each of these approaches is beyond the scope of this post, but we'll summarize them for you so you have an idea of what the technical folks are talking about when discussing your HR data strategy.

An **API** can be thought of as a messenger sitting between your software and some other software. Let's use a non-technical example. You go to a diner. You want a burger. The menu tells you what kind of burgers you can order. You read the menu and tell the server you want a No. 2 Special. The server takes your request and gives it to the cook. The cook makes the burger, hands it to the server who hands it to you. In this example, the combination of the menu and the server is the API. You are computer system 1 and the cook is computer system 2. The burger is the data..

APIs are great, but you as the owner of the HR data strategy should know the potential downsides. The first is you have to build them for each data source. Using our example, you cannot just walk into the next diner and say I would like a No. 2 Special. The second thing is not all vendors will have APIs available and, if they do, frequently they will charge you a fairly heavy cost to use them. Last, sometimes you want something that is not on the menu. If that's the case with an API then you won't be able to connect to the data you want. So when you are creating a data strategy, be sure to find out what APIs are available, how much they cost to use or build, and what fields will be available for you.

**Integration Platforms** also known as **IPAAS** at their basic level automate the ETL process discussed above. Using our diner example, with a platform any diner on the platform will know that when you order a No. 2 Special you want a specific type of burger. Where the platforms differ, and

what should be the focus of your inquiry, is cost, how much freedom you have to switch platforms, and whether you can go to any diner you like or do you have a fixed set you can choose from.

From an end user perspective, there are three basic types of IPAAS software. Some act like a master API. Companies like Mulesoft or Dell Boomi fit into this category. They are powerful glue that connects systems to each other, but the data normally sits in the connected systems. Then there are marketplaces also called HR ecosystems from the likes of ADP, Cornerstone, and UKG. In a market place, in theory everything is pre-connected, but again the master data sits inside the marketplace vendor. Finally, there are newer technologies, like my company Canopy Workforce Solutions, which provides a vendor agnostic data platform where you choose what to connect and the master data stays with you.

The last and oldest method of integration of those we've discussed is ***Extract, Transform and Load***, commonly referred to as ETL. The file we are talking about looks like an Excel file, but the format is normally .CSV. One piece of software generates the file to **Extract** the data, then there is

another piece of software which **Transforms** the data into a format the second system will accept. After the formatting is done, a third piece of software **Loads** the data into the second system. Where it all works, the end result is essentially the same as the other two methods.

File feeds have been around a long time, but so have the practical problems with them. They need to be built individually which takes time and money. They also need to be updated. This is particularly a problem with file feed updates for insurance carriers which have an additional formatting standard known as HIPAA 834. File feeds are also more likely to fail than the other two methods. From a control perspective, the other issue is you are generating files which may contain sensitive information. Having those sitting around is an invitation to disaster.

So what does all this mean? It means when you are plotting out your game plan you need to identify the data sources and how you will connect to them. If you make a strategic decision to only use one type of connectivity, let's say a platform, then you need to align your strategy with using an integration platform.

## **Step 5**

### **Define your sources of truth and where you will keep it.**

Key Technical Concepts:

- SSoT
- MVot
- Immutability
- Data Lake/Data Platform

So now you have thought more about sources of data than you ever cared to imagine, but we're not done. The final piece of your strategy defines which piece of data created from multiple sources is the truth at any given point in time.

Let's start our discussion by looking at a field value - the Employer portion of an Employee's medical coverage. In our example the premium is an obviously fictional \$100 for single and \$300 for family. In February, 3 months after open enrollment our employee chats through our broker helpline and tells them he got married to a lovely woman who has two children, and he wants to add them all to his coverage effective March 1.

The original \$100 is entered in all of these systems:

- HRIS
- Benefits Enrollment tool
- Third Party Administrator billing system
- Broker provide Total Compensation Statement
- Payroll System

On February 26 the broker's employee enters a life event in the enrollment tool. On March 3rd our employee takes his new daughter to the doctor at which point he's told "I'm sorry sir your daughter is not covered under your insurance." 2 seconds later the employee calls HR, and to make matters worse this employee is an SVP of the company. You have five places to look to determine the employees coverage level. Which one do you choose?

The above, not too far from reality example, is illustrative of the concept of having a Source of Truth. Where the same data exists in multiple systems, it can get out of sync fast. In order to have an effective data strategy you need a way to know that whenever you are relying on the data it is accurate as of the moment you are relying on it.

Now remember our old friends Control and Analysis because they will complicate the Source of Truth Issue. Source of Truth comes in two flavors - Single Source of Truth ("**SSoT**") and Multiple Versions of Truth ("**MVoT**").

Single Source of Truth means there is only one place from which everyone gets the data. Where control issues are the most important, you want one place that everyone can look to and rely on for a particular piece of data. Let's take a license required by law. If it is critical the the employee have that license in place when doing the job, e.g. Truck Driver, it should be stored and accessed from only one place so that way you never have to worry about data being wrong in some other location.

That brings us to Multiple Versions of Truth. MVOT is not just for politicians (we couldn't resist). MVOT is information which is created from your HR data. For example, finance may have a headcount and aggregate salary number which is connected to your data on active employees by department. To make sure that the MVOT is accurate you need to think about how you are going to link your data to the department with whom you want to share it. The sources of data discussed in section 4 are the means by which you will link HR's SSOT to other departments.

If another department needs real time visibility to information in your SSoT then to add business value you need to have an HR data strategy which supports that need. For example, if you need to get your operations a list of terminated employees prior to the end of the month so that they can terminate a company issued fuel card, then your HR data strategy as it pertains to active employees needs consider how you can get that data to the appropriate people and possibly the credit card issuer before the terminated employees can use the fuel card. In this manner, HR can positively impact the bottom line of the business.

The final piece you need to consider is “**immutability**”. When speaking of immutability of digital records we are simply asking the question “how do you know that the digital information you are relying on wasn’t changed?” With all the concern over hacking of electronics systems immutability is a real issue. There are already laws on the books requiring that electronic records must be preserved in a method which prevents alteration. See SEC Rule-17a-4(f). Similarly 12 CFR Section 1235.4(a)6) requires that

digital records have internal controls to prevent “data alteration”. Arizona and Arkansas have both passed laws pertaining to use of blockchain to create immutable smart records. Thus, it is clear that immutability will be a bigger and bigger concern for companies. As the use of physical means of providing authenticity, e.g. signatures, disappears there will be a more compelling need to demonstrate digital records have not been altered. Therefore, to have a forward looking HR Data Strategy you should consider the issue of immutability in the systems you choose to implement.

### **And last but not least - Location of Data**

When I was running HR, before we moved to a computerized system, everyone one of our 1,000+ employees had a legal sized vanilla file folder full of paper employee documents. We knew exactly where our data resided - in the locked beige cabinets at the back of the second floor. Today it’s a bit more complicated, but the HR issues which caused us to

store records for a long time in locked file cabinets have not really changed much. To the extent there has been change, the changes have made things more not less complicated.

The keystone of your data strategy is your system of record - the SSOT. If you don't have one single system of record, an effective HR data strategy will be difficult if not impossible to execute. How you maintain your system of record will in large part dictate where your data is located.

The most common ways to maintain a system of record, sometimes call the Single Source of Truth (SSOT) are as follows:

1. On premise software application.
2. Cloud vendor application.
3. Cloud data lake or data platform

The on premise HR application is a software application that sits on your company's servers frequently behind your company's firewall but

increasingly on a cloud or hybrid cloud infrastructure managed by your company's IT staff. What's great about on premise, is you control the data. No vendor can take it away from you. What's not so great is that you control the data. You have to spend the money on servers, maintenance personnel, software licenses, software upgrades, security infrastructure and a whole bunch of other things.

Because of that high cost, cloud vendors came along. They have all the servers, security infrastructure and other costs you would have paid, but in the cloud vendor case they can spread that cost out across a bunch of clients which brings the cost down for you. The down side here is they hold your data. If you've ever switched systems, you know it's not particularly easy to take data from one cloud vendor to another. If your strategy depends a lot on Control, the cloud could pose a problem. Even if you are

more on the analysis side, a proprietary cloud ecosystem will normally restrict your choice of tools to report on your data to what they allow.

The third option is the newest, but potentially the wave of the future. In this case, you are separating the data from the various applications which use that data. With an IPaaS or data platform you can collect data from various applications and then keep the data in your control. That's useful because it means you don't have the problem of vendor lock in, and your switching costs are lower if you decide to try a different software application because you already have the data you need.

## **Conclusion**

HR needs to be data driven. However, that's not something anyone needs to tell HR. The function has always been data driven. No matter what you want to do in HR you need data. The problem has never been that HR doesn't know this. The problem has always been that it was difficult for HR to get the data. From paper forms, to employee data existing in other systems, to data being locked away in the cloud - HR has always found

itself without power to harness the data needed for it to make a strategic impact. The good news is that is changing rapidly. We finally have the tools to bring together and share as needed critical data that can be used to help the business achieve its goals. All HR needs now is a little knowledge. We hope this post helps in that regard, and we wish you much success in building your HR data strategy.

## **HR DATA STRATEGY CHECKLIST**

- ✓ Identify all data items over which HR has responsibility.
- ✓ Classify the data as either Control data, Analysis data, or something in between.
- ✓ Identify any data which could be PHI or PII because they have special rules.
- ✓ Identify who has access to each data item.
- ✓ Define the acceptable use of each person who has access to a data item.
- ✓ Identify the business goals that you want to support with your HR Data Strategy.
- ✓ As to each business goal define what data within HR can be used to support that goal.
- ✓ Understand your companies IDAM policies.
- ✓ Decide whether a user name/password, two factor authentication or other authentication method is appropriate for each different aspect of HR data.
- ✓ Establish a method to authorize access to individual data elements, e.g. role based security.
- ✓ Identify an means of data transport, e.g. excel files, paper print outs, that may expose data to unauthorized users.
- ✓ Understand your external sources of data and how you will get that data through API, IPAAS, or ETL (file import)
- ✓ Define what will be HR's Single Source of Truth ("SSoT")
- ✓ Understand if your organization will have Multiple Versions of Truth ("MVoT") and define how you will keep that data in sync.
- ✓ Decide where you will house your SSoT - on premise, cloud in vendor application, cloud in your control or hybrid.

Website:- <https://canopyws.com/>