DIRTY DATA EXPERT

Structure Before Intelligence™

INFORMATION HAS CURRENCY

Executive Brief

Gary Segal
www.dirtydataexpert.com
gary@dirtydataexpert.com

The cold calls you get from marketing agencies — have you ever asked where they bought your number?

Somebody sold it. It passed through hands you never met, under labels you never approved, and arrived at a call centre as a row in a list. You were not asked. You were not told. That is the trade, and it runs on something most people never realise they own.

The €7 million label

In October 2026, Italy's data protection authority, the Garante, fined IQVIA Solutions Italy €7 million (decision n. 710). IQVIA — a global health-data company — held a database of longitudinal patient data drawn from around 800 family doctors, covering an estimated one million patients. The company called the data anonymous.

It was not. Every record carried a persistent patient code — a stable identifier tying years of diagnoses, prescriptions, test results and location data to the same individual. Records reached back to 2001, with no retention schedule and no deletion plan. Separately, a breach exposed the direct identifiers — names and contact details — of 3,370 patients.

The Garante's finding was simple: replacing a name with a code does not make data anonymous where re-identification remains reasonably possible. Pseudonymised is not anonymised. And nobody inside the chain had questioned the label before the regulator did.

Note the numbers honestly: the 3,370 exposed patients are substantiated in the decision's breach analysis. The million-patient total is an estimate — treat it as one until the decision itself is read.

The middlemen

I once needed a list of properties with owners. I approached a company that bought lists from companies that did credit checks. These, in my opinion, are the middlemen. Debt collection agencies can make the details available to credit rating agencies.

Follow the chain: the check is done for one purpose, the list is sold for another, and the details surface somewhere nobody in the chain will admit to. Every handoff has a label — legitimate, anonymised, aggregated — and every label is asserted by the party selling, not verified by anyone buying.

The brief on IQVIA does not say the information would not be sold to marketing companies. Read that again. Nobody asked, so nobody knows.

The man in the street

The man in the street is unaware of the trading of information. He does not realise information has currency.

That is the whole of it. Most people think that divulging their personal, intimate information to a medical professional is safe. They trust the medical professional because they trust his diagnosis. And that trust — in the diagnosis — is exactly what the trade runs on. The information leaves the consulting room and enters a market the patient never knew existed, traded by people he will never

meet, under labels nobody verified.

"The Questioner" — the person who asks whether "anonymous" is true before the regulator does — was missing at every step. Not because the question is hard. Because the people with standing to ask it didn't know there was a market.

Who benefits from acquiring it

There is value in information. You just need to understand who benefits from acquiring it.

Before you hand a dataset to an AI model, before you buy a list, before you accept a column labelled "anonymous" — ask who verified the label, and who profits if it is wrong. Structure before intelligence: the check belongs outside the loop that made the claim, because the loop that made the claim will never question it.

Gary Segal is the author of *Dirty Data — The Hidden Threat to Transactional and Segmented Integrity*, and *Switching ERP for Embedded AI — The Hidden Cost of Changing the Backbone of Your Business*. He writes the weekly *Structure Before Intelligence™* executive brief at dirtydataexpert.com.