|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Barrier relevance to technology innovation deployment process** | | | | | | | |
|  |  | Initiation (pre-adoption) | | | | Implementation (post-adoption) | | | |
|  |  | Barrier | Cause | Effect | Source | Barrier | Cause | Effect | Source |
| **Owner of deployment barrier** | Individual | Privacy and security:   * *For many people (many rugged individuals) in the US data movement and data ubiquity is not a good thing (CS1\_DI, Pos. 18/370-384)* * *Digital trust of patients starts to be compromised (PYV1\_DI, Pos. 32-34)  “You just shadow me; you just didn’t know that I actually did sip a little bit more of wine there or had a smoke here and all that and then you go and crack my premium up and all that. No, no, you guys just surveil me. I don’t want to have anything to do with it. I’ll come to you, and I need to come to you, and that’s it, and make a phone call to schedule and all this [quote].”* * *Willingness to share personal health information depends on what information is requested (P1\_DI, Q13)* * *Frequency of data leaks (P21\_DI, Q16\_9)* * *Worried about data leaks (P5\_DI, Q17\_3; P5\_DI, Q18)* * *Feels most vulnerable to fraud in the area of medical information security (P4\_DI, Q23)* | * *Patients feel shadowed (PYV1\_DI, Pos. 32-34)* * *Heard a lot about data leaks in the news (P5\_DI, Q18)* * *Person that feels most vulnerable to fraud in the area of medical information security was victim of an identity theft (P4\_DI, Q23)* | * *Patient stop participating in patient engagement programs (PYV1\_DI, Pos. 32-34)* * *Patients move away from digital medium increasingly and go back to the old-school way of making phone calls to schedule a meeting (PYV1\_DI, Pos. 32-34)* * *Lower willingness to share personal health information with primary care physicians (data leak worry) (P21\_DI, Q16\_9)* * *Person that feels most vulnerable to fraud in the area of medical information is afraid that is information is used by someone else and he would be liable for someone else’s medical expenses (P4\_DI, Q23)* | CS1\_DI, Pos. 18/370-384  PYV1\_DI, Pos. 32-34  P1\_DI, Q13  P21\_DI, Q16\_9  P5\_DI, Q17\_3  P19\_DI, Q17\_4  P5\_DI, Q18  P4\_DI, Q23 | Privacy and security:   * *For many people (many rugged individuals) in the US data movement and data ubiquity is not a good thing (CS1\_DI, Pos. 18/370-384)* * *Digital trust of patients starts to be compromised (PYV1\_DI, Pos. 32-34)*  *“You just shadow me; you just didn’t know that I actually did sip a little bit more of wine there or had a smoke here and all that and then you go and crack my premium up and all that. No, no, you guys just surveil me. I don’t want to have anything to do with it. I’ll come to you, and I need to come to you, and that’s it, and make a phone call to schedule and all this [quote].”* * Many physicians do not accept emails of clinical data, but they’ll take anything via fax (CS2\_A2\_DI, Pos. 34) * Many patients do not want their health data to be recorded in the EMR and to be shared with other HC stakeholders, e.g., payers (PV3\_ETC2\_DI, Pos. 35) * Patients lie to the physicians about their conditions or causes of why something happened (PV3\_ETC2\_DI, Pos. 35) * *Willingness to share personal health information depends on what information is requested (P1\_DI, Q13)* * *Frequency of data leaks (P21\_DI, Q16\_9)* * *Worried about data leaks (P5\_DI, Q17\_3; P5\_DI, Q18)* * *Feels most vulnerable to fraud in the area of medical information security (P4\_DI, Q23)* | * *Patients feel shadowed (PYV1\_DI, Pos. 32-34)* * On the EMR data analytics used for decision-making on reimbursement of treatment and future access to treatment (PV3\_ETC2\_DI, Pos. 35) * *Heard a lot about data leaks in the news (P5\_DI, Q18)* * *Person that feels most vulnerable to fraud in the area of medical information security was victim of an identity theft (P4\_DI, Q23)* | * *Patient stop participating in patient engagement programs (PYV1\_DI, Pos. 32-34)* * *Patients move away from digital medium increasingly and go back to the old-school way of making phone calls to schedule a meeting (PYV1\_DI, Pos. 32-34)* * *Patients lie to the physicians about their conditions or causes of why something happened (PV3\_ETC2\_DI, Pos. 35)* * *Patients do not receive the adequate care (if they lie about their conditions) (PV3\_ETC2\_DI, Pos. 35)* * *Lower willingness to share personal health information with primary care physicians (data leak worry) (P21\_DI, Q16\_9)* * *Trusts organization that only care about the bottom line less (P1\_DI, Q18)* * *Person that feels most vulnerable to fraud in the area of medical information is afraid that is information is used by someone else and he would be liable for someone else’s medical expenses (P4\_DI, Q23)* | CS1\_DI, Pos. 18/370-384  PYV1\_DI, Pos. 32-34  CS2\_A2\_DI, Pos. 34  PV3\_ETC2\_DI, Pos. 35  P1\_DI, Q13  P5\_DI, Q17\_3  P19\_DI, Q17\_4  P5\_DI, Q18  P4\_DI, Q23 |
|  |  |  |  | Emotions:   * Physicians do not trust the EMR systems (HITV1\_DI, Pos. 22) | * It did not work as it was supposed to work (HITV1\_DI, Pos. 22) | * They write it off | HITV1\_DI, Pos. 22 |
| Requesting stakeholder:   * *Trust providers most with personal health information (P16\_DI, Q18)* * *Higher trust in primary care physician than payers with shared personal health information (P1\_DI, Q16\_9)* * *Higher trust in primary care physician than pharmaceutical companies with shared personal health information (P1\_DI, Q16\_9)* * *Higher trust in primary care provider than hospitals with shared personal health information (P19\_DI, Q17\_3)* * *Higher trust in primary care physician than federal agencies (P4\_DI, Q17\_7)* * *Higher trust in payers than federal agencies (P4\_DI, Q17\_7)* * *No trust in hospitals with personal health information shared (P5\_DI, Q17\_3; P17\_DI, Q17\_3-Q17\_8)* * *No trust in payer with personal health information shared (P19\_DI, Q17\_4; P5\_DI, Q17\_4; P7\_DI, Q17\_4; P9\_DI, Q17\_4; P10\_DI, Q17\_4; P12\_DI, Q17\_4)* * *No trust in health apps with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P5\_DI, Q17\_5; P7\_DI, Q17\_5; P9\_DI, Q17\_5; P10\_DI, Q17\_5; P11\_DI, Q17\_5; (P19\_DI, Q17\_5; P19\_DI, Q18))* * *No trust in manufacturers with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P1\_DI, Q17\_6; P5\_DI, Q17\_6; P7\_DI, Q17\_6; P7\_DI, Q18; P9\_DI, Q17\_6; P12\_DI, Q17\_6; P14\_DI, Q17\_6)* * *No trust in pharmacies with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P5\_DI, Q17\_7; P9\_DI, Q17\_7)* * *No trust in federal agencies with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P10\_DI, Q17\_7; P18\_DI, Q17\_7; P24\_DI, Q17\_7; P25\_DI, Q17\_7)* * *No trust in any organization, no matter which stakeholder group (P15\_DI, Q18)* * *Little trust in an organization if it has controversial public image (P11\_DI, Q18; P14\_DI, Q18)* * *No trust if the requesting stakeholder has no authority (P20\_DI, Q18)* * *Trust with personal health information is higher in organizations individuals are familiar with / have a long-standing relationship with (P12\_DI, Q17\_2; P20\_DI, Q23)* * *Many organizations care just about their bottom line (P1\_DI, Q18)* | * *Payers are just out for their own interest, i.e., profit generation (P19\_DI, Q17\_4; P5\_DI, Q17\_4; P7\_DI, Q17\_4; P12\_DI, Q17\_4)* * *Health apps are just out for their own interest, i.e., profit generation and collecting data (P19\_DI, Q17\_5; P19\_DI, Q18)* * *Manufacturers are just out for their own interest, i.e., profit generation (P5\_DI, Q17\_6; P12\_DI, Q17\_6)* * *Might be using old systems that are easy to get compromised (P17\_DI, Q17\_3-Q17\_8)* * *Hospitals can be vulnerable to cyber-attacks (more than primary care providers) (P19\_DI, Q17\_3)* * *Payers have never been able to provide patient with adequate care (P10\_DI, Q17\_4)* * *Controversial public image of health apps (P11\_DI, Q17\_5)* * *Controversial public image of manufacturers (P7\_DI, Q17\_6; P7\_DI, Q18)* * *Data leaks (in context of pharmacies) (P5\_DI, Q17\_7)* * *Found out that CVC kept her credit card info on file and makes her wonder what other information they gather without (P9\_DI, Q17\_7)* * *Federal agencies are notoriously inefficient (P4\_DI, Q17\_7)* * *Federal agencies have never been able to approve good healthcare for her (P10\_DI, Q17\_7)* * *Government workers do not care about other people’s problems (P18\_DI, Q17\_7)* * *Does not know what is done with the information (in the context of federal agencies) (P24\_DI, Q17\_7)* * *No familiarity (with federal agencies) (P25\_DI, Q17\_7)* | * *Keep data provided to health apps to a bare minimum (P5\_DI, Q17\_5; P9\_DI, Q17\_5)* * *Do not provide data if information requested is too sensitive (in context of health apps) (P9\_DI, Q17\_5)* * *No usage (in context of health apps) (P10\_DI, Q17\_5)* * *Does not trust manufacturers but still provides the information if necessary (P9\_DI, Q17\_6)* * *Does not trust pharmacies but still provides the information if necessary (P9\_DI, Q17\_7)* * *Trusts organization that only care about the bottom line less (P1\_DI, Q18)* | P16\_DI, Q18  P1\_DI, Q16\_9  P17\_DI, Q17\_3-Q17\_8  P19\_DI, Q17\_3  P5\_DI, Q17\_4  P7\_DI, Q17\_4  P9\_DI, Q17\_4  P10\_DI, Q17\_4  P12\_DI, Q17\_4  P5\_DI, Q17\_5  P7\_DI, Q17\_5  P9\_DI, Q17\_5  P10\_DI, Q17\_5  P11\_DI, Q17\_5P19\_DI, Q17\_5;  P19\_DI, Q18  P1\_DI, Q17\_6  P5\_DI, Q17\_6  P7\_DI, Q17\_6;  P7\_DI, Q18  P9\_DI, Q17\_6  P12\_DI, Q17\_6  P14\_DI, Q17\_6  P5\_DI, Q17\_7  P9\_DI, Q17\_7  P4\_DI, Q17\_7  P10\_DI, Q17\_7  P18\_DI, Q17\_7  P24\_DI, Q17\_7  P25\_DI, Q17\_7  P15\_DI, Q18  P11\_DI, Q18; P14\_DI, Q18  P20\_DI, Q18  P12\_DI, Q17\_2; P20\_DI, Q23  P1\_DI, Q18 | Requesting stakeholder:   * *Trust providers most with personal health information (P16\_DI, Q18)* * *Higher trust in primary care physician than payers with shared personal health information (P1\_DI, Q16\_9)* * *Higher trust in primary care physician than pharmaceutical companies with shared personal health information (P1\_DI, Q16\_9)* * *Higher trust in primary care provider than hospitals with shared personal health information (P19\_DI, Q17\_3)* * *Higher trust in primary care physician than federal agencies (P4\_DI, Q17\_7)* * *Higher trust in payers than federal agencies (P4\_DI, Q17\_7)* * *No trust in hospitals with personal health information shared (P5\_DI, Q17\_3; P17\_DI, Q17\_3-Q17\_8)* * *No trust in payer with personal health information shared (P19\_DI, Q17\_4; P5\_DI, Q17\_4; P7\_DI, Q17\_4; P9\_DI, Q17\_4; P10\_DI, Q17\_4; P12\_DI, Q17\_4)* * *No trust in health apps with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P5\_DI, Q17\_5; P7\_DI, Q17\_5; P9\_DI, Q17\_5; P10\_DI, Q17\_5; P11\_DI, Q17\_5; (P19\_DI, Q17\_5; P19\_DI, Q18))* * *No trust in manufacturers with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P1\_DI, Q17\_6; P5\_DI, Q17\_6; P7\_DI, Q17\_6; P7\_DI, Q18; P9\_DI, Q17\_6; P12\_DI, Q17\_6; P14\_DI, Q17\_6)* * *No trust in pharmacies with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P5\_DI, Q17\_7; P9\_DI, Q17\_7)* * *No trust in federal agencies with personal health information shared (P17\_DI, Q17\_3-Q17\_8; P10\_DI, Q17\_7; P18\_DI, Q17\_7; P24\_DI, Q17\_7; P25\_DI, Q17\_7)* * *No trust in any organization, no matter which stakeholder group (P15\_DI, Q18)* * *Little trust in an organization if it has controversial public image (P11\_DI, Q18; P14\_DI, Q18)* * *No trust if the requesting stakeholder has no authority (P20\_DI, Q18)* * *Trust with personal health information is higher in organizations individuals are familiar with / have a long-standing relationship with (P12\_DI, Q17\_2; P20\_DI, Q23)* * *Many organizations care just about their bottom line (P1\_DI, Q18)* | * *Payers are just out for their own interest, i.e., profit generation (P19\_DI, Q17\_4; P5\_DI, Q17\_4; P7\_DI, Q17\_4; P12\_DI, Q17\_4)* * *Health apps are just out for their own interest, i.e., profit generation and collecting data (P19\_DI, Q17\_5; P19\_DI, Q18)* * *Manufacturers are just out for their own interest, i.e., profit generation (P5\_DI, Q17\_6; P12\_DI, Q17\_6)* * *Might be using old systems that are easy to get compromised (P17\_DI, Q17\_3-Q17\_8)* * *Hospitals can be vulnerable to cyber-attacks (more than primary care providers) (P19\_DI, Q17\_3)* * *Payers have never been able to provide patient with adequate care (P10\_DI, Q17\_4)* * *Controversial public image of health apps (P11\_DI, Q17\_5)* * *Controversial public image of manufacturers (P7\_DI, Q17\_6; P7\_DI, Q18)* * *Data leaks (in context of pharmacies) (P5\_DI, Q17\_7)* * *Found out that CVC kept her credit card info on file and makes her wonder what other information they gather without (P9\_DI, Q17\_7)* * *Federal agencies are notoriously inefficient (P4\_DI, Q17\_7)* * *Federal agencies have never been able to approve good healthcare for her (P10\_DI, Q17\_7)* * *Government workers do not care about other people’s problems (P18\_DI, Q17\_7)* * *Does not know what is done with the information (in the context of federal agencies) (P24\_DI, Q17\_7)* * *No familiarity (with federal agencies) (P25\_DI, Q17\_7)* | * *Keep data provided to health apps to a bare minimum (P5\_DI, Q17\_5; P9\_DI, Q17\_5)* * *Do not provide data if information requested is too sensitive (in context of health apps) (P9\_DI, Q17\_5)* * *No usage (in context of health apps) (P10\_DI, Q17\_5)* * *Does not trust manufacturers but still provides the information if necessary (P9\_DI, Q17\_6)* * *Does not trust pharmacies but still provides the information if necessary (P9\_DI, Q17\_7)* * *Trusts organization that only care about the bottom line less (P1\_DI, Q18)* | P16\_DI, Q18  P1\_DI, Q16\_9 P17\_DI, Q17\_3-Q17\_8  P19\_DI, Q17\_3  P5\_DI, Q17\_4  P7\_DI, Q17\_4  P9\_DI, Q17\_4  P10\_DI, Q17\_4  P12\_DI, Q17\_4  P5\_DI, Q17\_5  P7\_DI, Q17\_5  P9\_DI, Q17\_5  P10\_DI, Q17\_5  P11\_DI, Q17\_5P19\_DI, Q17\_5;  P19\_DI, Q18  P1\_DI, Q17\_6  P5\_DI, Q17\_6  P7\_DI, Q17\_6;  P7\_DI, Q18  P9\_DI, Q17\_6  P12\_DI, Q17\_6  P14\_DI, Q17\_6  P5\_DI, Q17\_7  P9\_DI, Q17\_7  P4\_DI, Q17\_7  P10\_DI, Q17\_7  P18\_DI, Q17\_7  P24\_DI, Q17\_7  P25\_DI, Q17\_7  P15\_DI, Q18  P11\_DI, Q18; P14\_DI, Q18  P20\_DI, Q18  P12\_DI, Q17\_2; P20\_DI, Q23  P1\_DI, Q18 |
|  | Trust in electronic medium:   * *There is often no choice of whether to trust a certain electronic medium if one cannot get the service required* *otherwise (P3\_DI, Q21; P16\_DI, Q21; P18\_DI, Q21)* * *Trusts in electronic medium if the website provides data security information (P3\_DI, Q21)* * *Trusts in electronic medium if complex security measures are required e.g., complex passwords or two-factor authentication (P4\_DI, Q21; P5\_DI, Q21; P6\_DI, Q21; P7\_DI, Q21; P25\_DI, Q21)* * *Trusts in electronic medium if she heard anything about the technology (P5\_DI, Q21)* * *Trusts in electronic medium if she previously used the technology (P5\_DI, Q21)* * *Trusts in electronic medium if she previously used the technology and had a good experience (P11\_DI, Q21; P13\_DI, Q21)* * *Trusts in electronic medium if it has it clearly connected to the office facility she is trying to use (P6\_DI, Q21)* * *Trusts in electronic medium if the staff handling it seems qualified/capable (P7\_DI, Q21)* * *Trusts in electronic medium if the terms and conditions are appropriate (P8\_DI, Q21)* * *Trusts in electronic medium if it has no negative public reputation / has not been covered in the news negatively (P9\_DI, Q21; P10\_DI, Q21; P11\_DI, Q21)* * *Trusts in electronic medium if it has no negative reputation within his family (P9\_DI, Q21; P20\_DI, Q21)* * *Trusts in electronic medium if others had a good experience with it (P10\_DI, Q21; P21\_DI, Q21)* * *Does not trust in a legacy electronic medium (P17\_DI, Q21)* * *Trusts in an electronic medium if the track history of those in charge of said technology is fine (P19\_DI, Q21)* * *Trusts in an electronic medium depending on the company’s business model and goals (P19\_DI, Q21)* * *Trusts in an electronic medium if he gets to select that his data cannot be sold to anyone (P24\_DI, Q21)* |  |  | P3\_DI, Q21  P4\_DI, Q21  P5\_DI, Q21  P6\_DI, Q21  P7\_DI, Q21  P7\_DI, Q21  P8\_DI, Q21  P9\_DI, Q21  P10\_DI, Q21  P11\_DI, Q21  P13\_DI, Q21  P16\_DI, Q21  P17\_DI, Q21  P18\_DI, Q21  P19\_DI, Q21  P20\_DI, Q21  P21\_DI, Q21  P24\_DI, Q21  P25\_DI, Q21 | Trust in electronic medium:   * *There is often no choice of whether to trust a certain electronic medium if one cannot get the service required* *otherwise (P3\_DI, Q21; P16\_DI, Q21; P18\_DI, Q21)* * *Trusts in electronic medium if the website provides data security information (P3\_DI, Q21)* * *Trusts in electronic medium if complex security measures are required e.g., complex passwords or two-factor authentication (P4\_DI, Q21; P5\_DI, Q21; P6\_DI, Q21; P7\_DI, Q21; P25\_DI, Q21)* * *Trusts in electronic medium if she heard anything about the technology (P5\_DI, Q21)* * *Trusts in electronic medium if she previously used the technology (P5\_DI, Q21)* * *Trusts in electronic medium if she previously used the technology and had a good experience (P11\_DI, Q21; P13\_DI, Q21)* * *Trusts in electronic medium if it has it clearly connected to the office facility she is trying to use (P6\_DI, Q21)* * *Trusts in electronic medium if the staff handling it seems qualified/capable (P7\_DI, Q21)* * *Trusts in electronic medium if the terms and conditions are appropriate (P8\_DI, Q21)* * *Trusts in electronic medium if it has no negative public reputation / has not been covered in the news negatively (P9\_DI, Q21; P10\_DI, Q21; P11\_DI, Q21)* * *Trusts in electronic medium if it has no negative reputation within his family (P9\_DI, Q21; P20\_DI, Q21)* * *Trusts in electronic medium if others had a good experience with it (P10\_DI, Q21; P21\_DI, Q21)* * *Does not trust in a legacy electronic medium (P17\_DI, Q21)* * *Trusts in an electronic medium if the track history of those in charge of said technology is fine (P19\_DI, Q21)* * *Trusts in an electronic medium depending on the company’s business model and goals (P19\_DI, Q21)* * *Trusts in an electronic medium if he gets to select that his data cannot be sold to anyone (P24\_DI, Q21)* |  |  | P3\_DI, Q21  P4\_DI, Q21  P5\_DI, Q21  P6\_DI, Q21  P7\_DI, Q21  P7\_DI, Q21  P8\_DI, Q21  P9\_DI, Q21  P10\_DI, Q21  P11\_DI, Q21  P13\_DI, Q21  P16\_DI, Q21  P17\_DI, Q21  P18\_DI, Q21  P19\_DI, Q21  P20\_DI, Q21  P21\_DI, Q21  P24\_DI, Q21  P25\_DI, Q21 |
| Organization | Privacy and security:   * *Strong belief that they have built knowledge internally that gives them a competitive advantage (CS2\_A2\_DI, Pos. 8)* * Hospitals are apprehensive about letting new applications be part of their system (PV1\_DI, Pos. 4) * *People are petrified of HIPAA penalties and violating the law (CS1\_DI, Pos. 45, 1085-1116)  “And so, my analogy of the game of bowling is there’s a penalty for the ball going in the gutter on the right there is no penalty for the ball going in the gutter on the left. So, everybody just constantly throws the ball to the left gutter to make sure that they avoid the penalty. Until there’s a mandate to say avoid both gutters equally, get the ball down the middle. We can’t expect people to try to get the ball down in the middle [quote].” (CS1\_DI, Pos. 45, 1085-1116)* | * *Development of medical Centers of Excellence (CS2\_A2\_DI, Pos. 8)* | * *Providers loose the competitive advantage of how things are done when engaging in data sharing (CS2\_A2\_DI, Pos. 8) [see Ex\_Fin]* * *People do everything to avoid these penalties, such as under-matching identity data (CS1\_DI, Pos. 45, 1085-1116)* | CS2\_A2\_DI, Pos. 8  PV1\_DI, Pos. 4  CS1\_DI, Pos. 45, 1085-1116 | Privacy and security:   * Over-interpretation of the application of HIPAA to the movement of data to treat healthcare, despite government and legislature stating repeatedly that the payment and treatment of healthcare are safe harbors around the movement of healthcare data (CS1\_DI, Pos. 18/411-428) * *Strong belief that they have built knowledge internally that gives them a competitive advantage (CS2\_A2\_DI, Pos. 8)* * Providers, in particular the front office staff, see a risk of being sued for improperly sharing clinical data (CS2\_A2\_DI, Pos. 34) * *People are petrified of HIPAA penalties and violating the law (CS1\_DI, Pos. 45, 1085-1116)  “And so, my analogy of the game of bowling is there’s a penalty for the ball going in the gutter on the right there is no penalty for the ball going in the gutter on the left. So, everybody just constantly throws the ball to the left gutter to make sure that they avoid the penalty. Until there’s a mandate to say avoid both gutters equally, get the ball down the middle. We can’t expect people to try to get the ball down in the middle [quote].” (CS1\_DI, Pos. 45, 1085-1116)* | * *Development of medical Centers of Excellence (CS2\_A2\_DI, Pos. 8)* * The US has a very litigious society (CS2\_A2\_DI, Pos. 34) [see Pr\_SystemChar] | * Data for the treatment of healthcare is not shared (CS1\_DI, Pos. 18/411-428) * *Providers loose the competitive advantage of how things are done when engaging in data sharing (CS2\_A2\_DI, Pos. 8) [see Ex\_Fin]* * *People do everything to avoid these penalties, such as under-matching identity data (CS1\_DI, Pos. 45, 1085-1116)* | CS1\_DI, Pos. 18/411-428  CS2\_A2\_DI, Pos. 8  CS2\_A2\_DI, Pos. 26  CS2\_A2\_DI, Pos. 34  CS1\_DI, Pos. 45, 1085-1116 |
| System |  |  |  |  | Privacy and security concerns:   * The feeling that the core business model is threatened (VRS providers) (ETC1\_DI, Pos. 34) * Fear of losing business intelligence (ETC1\_DI, Pos. 48; CS2\_A2\_DI, Pos. 8) |  | * Involved parties (VRS providers) fell back on the old-school relational model, with everyone building their own look-up directory and keeping it in synch via APIs [they wanted to go with the tried and tested] (ETC1\_DI, Pos. 14; ETC1\_DI, Pos. 34) [see Pr\_FacilCon] * VRS providers felt anxiety that the maintainers of the look-up directory could be compromised (ETC1\_DI, Pos. 14; ETC1\_DI, Pos. 34) * [[Success factor[Need to solve a problem that requires consensus, that everyone involved/affected shares equally, and that no one really wants to own internally]] (ETC1\_DI, Pos. 48) | ETC1\_DI, Pos. 14; ETC1\_DI, Pos. 34  ETC1\_DI, Pos. 34  ETC1\_DI, Pos. 48  CS2\_A2\_DI, Pos. 8  CS1\_DI, Pos. 45, 1085-1116 |
|  |  |  |  | Emotions:   * The industry has a tremendous mistrust of any data that they didn’t originate (CS1\_DI, Pos. 45, 1035-1085) | * Clinical data does not flow (CS1\_DI, Pos. 45, 1035-1085) | * Even if the data flows, externally generated data but quarantined in a special holding place (CS1\_DI, Pos. 45, 1035-1085) | CS1\_DI, Pos. 45, 1035-1085 |